

ESO - Security Trends Report

02/09

McAfee Warns of Economy-Based Threats

Computer Business Review (01/20/09) ; Evans, Steve

Cybercriminals will use the current economic crisis to heighten attacks on unemployed individuals or those concerned about the economy, according to the 2009 Threat Prediction Report released by the security vendor McAfee. The report draws attention to increased threats of malware attacks through USB drives and other removable devices. McAfee's Greg Day told reporters that attackers will use economic fears to their advantage. "Unemployed people or those worried about their job may be tempted by an offer to upload their CV to a job site; if that site is fake then they've opened themselves up to data theft," the security analyst warned. "People may also be tempted by offers of low-interest loans." As businesses transition to Web 2.0, or cloud computing, and attackers increasingly rely on single-use binary files to launch malware, investigators face many challenges this year in the war on cybercriminals and theft, the report states.

Misconceptions About Laptop Encryption May Put Data at Risk

Dark Reading (01/15/09) ; Wilson, Tim

Users with encryption protection on their laptops may be overconfident about the capabilities of such protection when working remotely, according to a recent study conducted by the Ponemon Institute. The study of roughly 700 IT security experts and more than 800 non-IT users found that laptops with encryption security account for nearly six in 10 machines. The 66 percent of users who say they are not concerned about losing their laptops because the information is encrypted may be taking more risks with their machines, experts say. Approximately 30 percent of non-IT users say they will use their machine in an unsecured location or leave it with another person while traveling. Fewer than 30 percent of users use a privacy shield to deter prying eyes, the study found, while only 31 percent of users physically secure their laptops to their desks. A majority of respondents do not use a difficult password, and 36 percent admit to using Post-It notes to remember their passwords. "We believe that the primary conclusion that can be drawn from this study is that business managers are either negligent in the protection of sensitive and confidential information on their laptops, or they may be overly dependent on encryption to keep this information secure," the study concludes.

Guarding Data

SC Magazine (01/09) Vol. 20, No. 1, P. 26 ; Armstrong, Illena

Many organizations are likely to cut their information technology security budgets this year to deal with the slumping economy, despite the fact that they see the risks posed by the threat of data breaches, concludes a recent SC Magazine survey. According to the survey, 80.6 percent of 217 respondents said the threat of data breaches is having a significant influence on their organizations' current security initiatives. Of the 368 IT security professionals who took part in last year's survey, 81.3 percent said such threats were influencing their organizations' security initiatives. However, about 11 percent of the respondents to this year's survey said their organizations were planning to make moderate or dramatic cuts to their budgets for IT security projects and data loss prevention efforts over the next year, compared with about 5 percent in last year's survey. Forty-five percent of respondents said their organizations were launching risk management or data protection initiatives because their executive boards were demanding that they do so. BT chief security technology officer Bruce Schneier says the drop in executive board demand indicates that some boards likely feel that reports of data breaches are becoming old news, or that the risk of data breaches is lower since there have not been significant prosecutions for data theft or congressional hearings into why data was exposed in a breach.

What the Web knows about you

What information is available about you in cyberspace? Where does it come from, and what risks does it present? Computerworld's Robert L. Mitchell set out to see just how much he could find about himself online. What he discovered is frightening.

<http://cwflyris.computerworld.com/t/4265345/101582/165136/0/>

(This is a long and interesting article -- so I just provided the link.)

12 tips for managing your information footprint

Take an active role in controlling your personal data.

By Robert L. Mitchell

January 27, 2009 (Computerworld) When it comes to managing personal information online, most people are their own worst enemies. Many of us fail to adequately protect our personal data before it gets online, but once information makes its way to the Internet, it can be quickly replicated and is often [difficult, if not impossible, to remove](#).

For example, in four weeks of on-and-off reporting and online searches using publicly available online records and tools, I was able to find my current and past addresses and phone numbers, date of birth, Social Security number, employment history, identifying photographs, a digital image of my signature and much more. See ["What the Web knows about you"](#) for all the gory details.

You can take an active role in managing data about you, whether it resides in marketing lists, government databases, telephone directories or credit reports. Here are some tips.

1. Think before you disclose personal information about yourself online on business networking sites such as [LinkedIn](#), job listing sites such as Monster.com, and social networking sites such as [MySpace](#) and [Twitter](#).

How much do you want to disclose about your employment history, likes and dislikes, and where you are at any given time? Do you really want everyone to know when you're not at home, how long you'll be out and when you'll be back?

2. Don't give out your Social Security number -- anywhere -- unless absolutely required.

3. Don't use real information about yourself for authentication, recommends private investigator Steve Rambam. Instead, he suggests making up answers to commonly asked security questions such as a mother's maiden name.

4. Know what's out there about you. Do a search online using search engines, government Web sites and other resources cited in ["What the Web knows about you"](#) to get an idea of what information about you is available online today. If your Social Security number appears in a public records database, ask the agency in charge of the database if they will redact it from the record on your behalf. You can also ask Web site owners to have sensitive information redacted and any potentially damaging inaccuracies corrected.

5. Keep up with new data about you as it is published on the Web. Alert services such as [Google Alerts](#) are designed to continuously search the Web to track topics you're interested in, but you can also use them to find out what information about you is being published on the Web. Configure the service to search the Web for instances of personally identifying information such as your name, address, phone number, Social Security number, and so on. When [Google](#) finds matches, it will send you an e-mail with links.

6. Consider requesting a fraud alert from one of the three major credit reporting agencies ([Experian fraud alert](#), [TransUnion fraud alert](#) or [Equifax fraud alert](#)) if you discover sensitive data such as your Social Security

number on a public Web site or service. If you request a fraud alert with any of the three agencies, it will notify the others on your behalf.

7. Also consider requesting a security freeze, which takes a fraud alert one step further. It means that no one can access your credit report without your explicit consent, which makes it difficult for fraudsters to open up new accounts in your name.

This is a new option that has only become broadly available in the past year. A freeze must be placed with each of the three major credit reporting agencies, and you must unlock access to your credit report (for a fee) when a lender, insurance company or other party requests the information.

True, it's inconvenient. You pay a small fee to freeze your credit report at each of the three reporting agencies. Then you pay another fee each time you unlock it. But you'll have the security of knowing exactly who is trying to access your credit report -- and for what reasons -- every time.

8. Request a copy of your credit report at AnnualCreditReport.com and review it for errors.

Ignore the sales pitches for credit monitoring products. Identity fraud monitoring services, including those sold by the three credit reporting agencies and others, can provide peace of mind, but they're pricey for what you get and most tell you only after someone has compromised your identity.

9. Opt out of the marketing databases at the big data aggregators such as ChoicePoint and Acxiom. Unfortunately, the companies usually won't take requests from third-party services like Reputation Defender, which attempt to do this on your behalf; you have to contact each one yourself. You can also ask to see the profile they have of you and ask for changes if the data is incorrect. They won't, however, pull information about you that's used for "risk purposes," such as for insurance underwriting or litigation.

While you can opt out of Web people search and background checking services such as Intelius and US Search, there are simply too many to contact. Intelius will honor your request, but Ed Petersen, co-founder and executive vice president, says it's not worth the effort. "You're tilting at windmills. I'm not the original source of the data, [and] there's a lot of companies like Intelius out there." This is one reason why it's so important not to let these data bits get out there in the first place.

10. Protect your cell phone number. If you don't want it in public database records, don't give it out for business transactions. "If you never put it down anywhere, then it is not going to be in the public records," says Petersen.

Using an unlisted phone number reduces, but does not eliminate, the number of places where your telephone number will appear online. Every time you give out the number, as may be requested for purchases, registrations and other business transactions, it goes into databases that may be sold to aggregators.

11. Don't participate in surveys or fill our product registration cards. It's not required for warranty service (all you need is your receipt), and the information you submit goes right into marketing databases.

12. Think twice before signing up for retail store loyalty cards -- and read the privacy policy. Are the incentives worth it if the business is tracking your every purchase? In many cases, the business will keep that information for its own use. In other cases, some or all of that data may be shared with business partners, marketing companies or data aggregators.

VA Will Settle Data Security Breach Lawsuit for US \$20 Million

(January 27 & 28, 2009) The US Department of Veterans Affairs (VA) will pay US \$20 million to settle a lawsuit brought on behalf of 26.5 million individuals whose personal data were on a laptop and external storage device stolen in a May 2006 robbery. The computer and drive were recovered and investigators determined that the information had not been accessed.

Nonetheless, the suit proceeded to collect damages for emotional distress and expenses incurred while affected individuals monitored their credit reports. The VA agreed to settle to avoid any further litigation. The settlement must be approved by a judge before it becomes final.

[Editor's Note (Pescatore): Getting off for \$20M is cheap compared to other incidents of large scale, but just think: they could have bought and installed laptop encryption on about 100,000 laptops for that amount.

P2P networks rife with sensitive health care data, researcher warns

Data leaks could be significant threat to patients, providers, Dartmouth study finds

By Jaikumar Vijayan

January 30, 2009 (Computerworld) Eric Johnson didn't have to break into a computer to gain access to a 1,718-page document containing Social Security numbers, dates of birth, insurance information, treatment codes and other health care data belonging to about 9,000 patients at a medical testing laboratory.

Nor did he need to ransack a health care facility to lay his hands on more than 350MB of sensitive patient data for a group of anesthesiologists or to get a spreadsheet with 82 fields of information on more than 20,000 patients belonging to a health system.

In all instances, Johnson was able to find and freely download the sensitive data from a [peer-to-peer file-sharing network](#) using some basic search terms.

Johnson, a professor of operations management at the Dartmouth College Tuck School of Business, did the searches last year as part of a study looking at the inadvertent hemorrhaging of sensitive health care data on Internet file-sharing networks.

The results of that study, which are scheduled to be published in the next few days, show that [data leaks over P2P networks](#) involving the health care sector pose a significant threat to patients, providers and payers, Johnson said.

"When you start thinking about the nature of these disclosures, it's far more worrisome" than compromises such as those involving payment card data, he said.

"Here you are leaking not just detailed personally identifiable information but also very personal medical information related to patients," Johnson said. Such data can be readily used by hospital employees, the uninsured, organized crime rings, illegal aliens and drug abusers for medical identity theft, and to fraudulently obtain costly medical services and prescription drugs, he said. And while such fraud can cost millions, there is less monitoring for such fraud in the health care industry than there is in the financial sector.

P2P networks allow Internet users to share music, video and data files with others on the network. Normally, popular P2P clients -- such as [Kazaa](#), [LimeWire](#), BearShare, Morpheus and FastTrack -- let users download files and share items from a particular folder. But if proper care isn't taken to control the access that these clients have on a system, it is easy to expose far more data than intended.

For example, [Dartmouth](#) conducted a [similar study](#) about 18 months ago and found volumes of sensitive financial data on P2P networks as a result of inadvertent data leakage. At a [congressional hearing](#) in July 2007, security experts testified that millions of documents, including sensitive military and government documents, were being leaked on P2P networks. Even pharmaceutical giant [Pfizer Inc.](#) became a victim when an [employee illegally installed a P2P client](#) on a company computer and exposed personal data belonging to 17,000 employees.

Hospitals and other health care providers need to be aware of the dangers posed by inadvertent data leakage and implement better controls to monitor, detect and stop them, Johnson said. Stricter access control measures also need to be adopted across the health care industry to minimize access to sensitive patient data, he said. This is especially critical because of the growing portability of sensitive data, he said.

Dartmouth began its search for medical data on P2P networks in January 2008. Over a two-week period, researchers examined health care data disclosures and health-related searches on file-sharing networks such as Gnutella, FastTrack, Aries and e-Donkey.

The search focused on finding information related to the top 10 publicly traded health care organizations in the country, representing nearly \$70 billion in spending. Dartmouth researchers used search terms related to each of the companies, such as the names of affiliated hospitals, clinics and brands, to see what information it could find on P2P networks.

The university conducted the searches with the help of a firm called Tiversa Inc., which sells P2P network-monitoring services to government agencies and private companies. The searches yielded an astonishing range of information floating over P2P networks, Johnson said.

The information found on the networks originated from health care companies, suppliers and patients, and included sensitive patient health and identity information, insurance and billing data, and business documents. The data found on P2P networks included medical diagnoses and psychiatric evaluations, and even blank, signed prescription forms that anyone could have easily copied and filled out.

What was probably the most interesting finding "was the sheer amount of unstructured data that is floating around," Johnson said. The range of health care information floating on P2P networks and the variety of sources from which it is being leaked highlight the disorganized and decentralized manner in which health care data is being collected, stored, used and shared, he said.

With economic slump, concerns rise over data theft

Security breaches will go up as a result of the downturn, McAfee says

By Robert McMillan

January 29, 2009 (IDG News Service) Is the worsening economic situation going to turn some employees into data thieves?

That's a top concern amongst IT decision-makers, many of whom say that laid-off employees are the biggest security threat created by the economic downturn. In a [McAfee Inc.](#)-sponsored [worldwide survey](#) (registration required) of 1,000 IT decision-makers, the company found that 42% of respondents felt that laid-off employees represented the biggest IT security threat caused by the recession. That's more than were worried about outside intruders. And 36% said that they were worried about security problems caused by employees in financial stress.

Crime rates spike during hard times, and with thousands of workers being laid off each week lately, there may be an added incentive for laid-off employees to take intellectual property with them to bolster their chances of getting hired with a competitor, to use with a start-up company of their own, or maybe even to sell.

"The economic downturn across the board is going to provide additional motivation for people who would want to do harm," said [Seth Bromberger](#), an information security manager at PG&E in San Francisco. "It's on a lot of people's radar right now."

According to Bromberger, companies that have their employee exit processes in order have less to fear from laid-off workers. It's just that with the current economic squeeze, people's motivation may be changing.

Layoffs can fray employee loyalty, and there certainly is money to be made selling all kinds of corporate data.

Last August, the [FBI](#) arrested [Rene Rebollo](#), a financial analyst at subprime mortgage broker Countrywide, for allegedly selling Excel spreadsheets containing customer information for about two-and-a-half cents per record. Over a two-year period, he may have made \$70,000 from the scam, the FBI said. His annual salary was \$65,000.

According to court filings, Countrywide had security software that disabled the use of USB drives on its PCs. But Rebollo found one PC that didn't have the software and was able to download about 20,000 records each week onto his personal thumb drive, which he'd later e-mail to a buyer, the FBI said.

USB drives are one of the most underestimated sources of data leaks, says McAfee [CEO Dave DeWalt](#). "For \$100, you can buy a 100GB drive," he said. "100GB can be the entire customer base for an entire large company."

An economic slowdown can create other computer security problems too. As businesses fail and are bought, that churn can lead to management chaos within IT groups. Workers aren't sure how to report security concerns, or to whom, and existing controls may not be monitored as roles are switched and jobs are lost. In addition, workers may not want to report security issues for fear of jeopardizing a co-worker's job or drawing unwanted attention to themselves.

Ignoring security problems can be costly. The average security breach results in a loss of \$4.6 million in intellectual property and costs about \$600,000 to clean up, DeWalt said.

"We don't have the good risk models and as a result people are taking risks," said Eugene Spafford, a professor of computer science at Purdue University who contributed to McAfee's report on its survey data.

Security breaches will go up as a result of the downturn, especially as companies try to trim information security costs, although "it's not clear that we will see a lot of them attributed back directly to security issues," he said.

Still, not everyone sees the downturn as a game-changer.

"I'm not sure I recognize a greater threat to this company because of the downturn in terms of cyberthreats," said Jim Klotz, CIO at the PMA Insurance Group in Blue Bell, Pa. Increasing cybercrime is just a fact of life, and it would be growing with or without the slump, he said. "More people are capable and more people are finding profit in it."

Russian 'cybermilitia' knocks Kyrgyzstan offline

Same tactics used in '08 attack against Georgia, but hackers getting faster, says researcher

By Gregg Keizer

January 28, 2009 (Computerworld) A Russian "cybermilitia" has knocked the central Asian country of Kyrgyzstan off the Internet, a security researcher said today, demonstrating that the hackers are able to respond even faster than last year, when they waged a digital war against another former Soviet republic, Georgia.

Since Jan. 18, the two biggest Internet service providers in Kyrgyzstan have been under a "massive, sustained distributed denial-of-service attack," said [Don Jackson](#), the director of threat intelligence at [SecureWorks Inc.](#)

The attacks, which are ongoing, have knocked most of the country offline and disrupted e-mail to and from a U.S. air base there, Jackson said. The public affairs officer at Manas Air Base in Kyrgyzstan was not immediately available to answer questions about whether the attacks have disrupted operations or other activities.

According to Jackson, the distributed denial-of-service (DDoS) attacks -- essentially a flood of requests that overwhelm servers and effectively knock them off the Internet -- can be traced to the same groups of Russian and ethnic Russian hackers who assembled in militia-like fashion last August to [launch similar attacks against Georgia](#).

"The traffic we've collected has all the hallmarks of the tools that were used in the Georgia attacks," said Jackson. "And they're from the same network [of IP addresses] that we associated with the cybermilitia last year." Researchers have also found two groups, led by "two specific players," in common with the 2008 attacks against Georgia, he added.

Speculation about why Kyrgyzstan's Internet infrastructure was attacked center around an investment deal that Russia is negotiating the country. Russia has indicated that it wants Kyrgyzstan to oust foreign air forces, including those of the U.S., before it will agree to loan the country \$300 million and invest another \$1.7 billion in its energy industry.

Opposition to the current administration in Kyrgyzstan has relied heavily on the Internet, while President Bakiyev's government has ignored the Web, said Jackson. "Any attack by Russians would do no collateral damage to their ally in the area, and would only impact the opposition," he explained.

Beyond the immediate effect on Kyrgyzstan, what's worrisome to Jackson is the speed with which this attack was mounted. "To put some perspective on this, it's been an escalating pattern from [Estonia](#) to Georgia to here," he said, referring to the 2007 and 2008 attacks against other former Soviet republics. "The attacks are more closely coinciding with events that are core to the Russian interest, with increasingly fast response and quick mobilization.

"When it once took days or weeks, now we're seeing it within hours," Jackson said.

In fact, the attacks on Kyrgyzstan were mobilized in much the same way that the so-called militia was formed last year to cripple Georgia. "It was the same kind of mobilization, where word is put out by a few and then other [hackers] respond," he said. One difference: The attacks against Kyrgyzstan lacked the kind of wide support that the Georgian DDoS attacks gained. At one point, Russian social network were involved in the latter, something not yet seen in the attacks against Kyrgyzstan.

"We haven't seen a broad base of support by Russian citizens," said Jackson. "It's more the core of the militia group."

Researchers have not found any direct connection between the attacks -- which originate on botnets and servers that send more mundane pharmaceutical spam or conduct phishing campaigns -- and the Russian government. But to Jackson, that hardly matters.

"People who once were in the KGB, or other parts of the government, and who now are in computer security, have in the past said, 'We will rely on this capability because there is no risk for us doing so,'" said Jackson. "Using cybermilitias shelters the Russian government from culpability."

Coming Soon: Full-disk Encryption for all Computer Drives

Computerworld (01/27/09) ; Mearian, Lucas

Six of the world's largest computer drive makers have published three specifications for a single, full-disk encryption standard that can be used in all hard drives, solid state drives, and encryption key management applications. The specifications call for the use of either the 128-bit or 256-bit key Advanced Encryption Standard, depending on the level of security the vendor wants. The standard will require users to enter a password before Windows boots up in order to access any disk equipped with the encryption technology. In addition, the password will have to be entered whenever a USB drive is unplugged or an administrator removes a drive from a server. The technology will offer a number of benefits for drive manufacturers and enterprises alike. Since the specification is a single, full-disk encryption specification, drive manufacturers will be able to integrate security into their products' firmware, which in turn will help reduce the cost of production and increase the efficiency of the security technology. Enterprise users, meanwhile, will not experience a slowdown when an operating system or application writes data to the encrypted drive. The encryption standard will eventually be included on all new computer drives. It is already available on some drives made by several manufacturers.

Microsoft Study: Users Worry About Privacy But Know Little About Threats

Dark Reading (01/28/09) ; Higgins, Kelly Jackson

Computer users are concerned about protecting their privacy online and use a number of different security technologies, but few of them have a full understanding of the threats that exist on the Web, concludes a new Microsoft study. The study found that many Internet users believe there is little that they can do to protect personal information that is already online. Microsoft's Peter Cullen says that many people are not aware of the steps they can take to protect the privacy of their data online, such as opting out of behaviorally-targeted advertising or downloading new tools for Internet browsers. The study raises the question of whether businesses and governments are giving users who are not informed about security threats too much of the responsibility for protecting the privacy of their personal information. Security researcher Nathan Hamiel says that users "have been left with too much responsibility, mainly because they don't know what data about themselves should be private." Hamiel says that Web sites should not be totally responsible for protecting the privacy of their users' data, but they should do a better job communications the security features available to them. Cullen says that users "must have the right resources from industry, government, and nongovernmental organizations so they can better educate themselves about privacy, threats to personal information, and ways to safely navigate online."

As the Market Tumbles, Cyberthieves Log On

USA Today (01/29/09) P. 1A ; Acohido, Byron; Swartz, Jon

Data thieves and cyberfraudsters are taking advantage of the financial crisis to launch a new wave of Internet-based schemes that prey on confused, fearful, and unwary people. Security experts warn that gangs of data thieves could start exploiting disgruntled employees with inside knowledge about their employers' technology systems. Application Security's recent audits of 179 organizations found that nearly 60 percent had suffered at least one intrusion in the past 12 months. Meanwhile, Panda Security reports that the number of malicious programs circulating on the Internet increased to 31,000 a day in mid September. "The criminal economy is closely interrelated with our own economy," says Panda Security's Ryan Sherstobitoff. "Criminal organizations closely watch market performance and adapt as needed to ensure maximum profit." Data storehouses also have become a more attractive target for hackers, as indicated by the recent breach of the system that Heartland Payment Systems uses to process 100 million payment card transactions a month. Another recent incident involved a hacker obtaining the user name and password for a system administrator at e-bill payment system CheckFree.com. The hacker used it to access the firm's domain name service account and rerouted anyone typing www.mycheckfree.com to a Ukrainian Web server that attempted to install a password-stealing Trojan. Beyond stealing Social Security numbers and user account names and passwords, some cybercriminals are now spreading malware via direct-messaging systems and social networking sites. Routine queries on the major search engines also can have tainted links, and the search firms say there is little they can do to stop it.

Study: Data breaches continue to get more costly for businesses

Average cost of breaches hits \$202 per stolen record, according to Ponemon report

By Jaikumar Vijayan

February 2, 2009 (Computerworld) Companies that are reluctant to invest what it takes on data security better be prepared to pony up a lot more if their systems are ever [breached](#).

That's the main take-away from a new report released by the [Ponemon Institute LLC](#), which shows that the average [cost of a data breach](#) to companies is continuing to increase. Ponemon said the breaches from last year that it studied cost an average of about \$202 for each compromised customer record. That is 46% higher than the \$138 per record that Ponemon cited in its first annual report on breach costs, for 2005. The average cost had previously increased to \$182 in 2006 and \$197 in 2007, according to Ponemon.

The cost-per-record figures include direct expenses for breach detection, mitigation, [notification](#) and response efforts, as well as indirect costs, such as the financial impact of customer defections and lost business opportunities. Ponemon said the average overall cost of the breaches covered in the new report was more than \$6.6 million, with individual companies reporting costs that ranged from \$613,000 to almost \$32 million.

The report was based on a study of breaches at 43 large companies from 17 different industries. The number of customer records that were compromised in the breaches ranged from less than 4,200 to more than 113,000. Those figures are much lower than those associated with the most-publicized breaches, which involve compromised records numbering in the millions, but they're in line with the number of compromised records involved in the types of breaches that companies are typically hit by.

Increasingly, the biggest cost to companies that suffer data breaches is lost business, said [Larry Ponemon](#), chairman of the Elk Rapids, Mich.-based think tank. He added that about \$139 of the average per-record breach cost — or 69% of the total — was in the form of lost business last year, while other costs declined. That statistic indicates that although companies are getting better at detecting and responding to data breaches, customers are becoming [less tolerant of breaches](#) and showing a growing willingness to take their business elsewhere, Ponemon said.

In the wake of breach reports, "we found customer churn rates actually going up," Ponemon said. "People do care deeply about data being stolen."

That concern was especially evident, he noted, in breaches involving financial services firms and health care organizations, because the data involved in such compromises is often more sensitive than the information at other types of companies.

For instance, the customer-defection trend doesn't appear to have manifested itself in a big way in the retail industry. As an example, the massive breach disclosed in January 2007 by [The TJX Companies Inc.](#) was expected to have a dramatic impact on customer trust in the company. But in the quarter immediately after the disclosure, TJX reported one of its strongest-ever financial performances. And in the first year after the breach came to light, the retailer's stock price [remained largely unaffected](#), while its same-store sales increased 4%.

Ponemon said the new study also showed that breaches end up costing significantly more for companies that are experiencing them for the first time than they do for companies that have suffered previous data compromises. The same is also true, he noted, for breaches involving third parties. On average, such breaches ended up costing companies about \$231 per compromised record, based on the study.

[John Pescatore](#), an analyst at [Gartner Inc.](#), said the numbers released in the Ponemon study were somewhat similar to Gartner's own cost estimates for relatively small breaches involving up to 100,000 customer records. "Basically, \$202 per account is right in the ballpark," Pescatore said. "It's a little lower than what we've seen," but not by much.

But, he added, that figure is "way high" for large-scale breaches involving millions of customer records, such as the one at TJX. That's because some of the costs associated with a breach, such as the expense of detecting and mitigating a systems intrusion, may not increase significantly as the number of customer records grows larger and larger.

A number of variables can affect the actual cost of breaches, Pescatore said. For instance, certain kinds of breaches, such as those involving [Social Security numbers](#), may require companies to offer credit monitoring services to affected customers, while others don't. Similarly, if a breached company had encrypted its data, it might not need to spend as much on breach notification costs as businesses with unencrypted information do.

New disk encryption standards could complicate data recovery

So, what do you do if you lose your password?

By Lucas Mearian

February 2, 2009 (Computerworld) When the world's largest disk-makers joined last week to announce a [single standard for encrypting disk drives](#), the move raised questions among users about how to deal with full-disk encryption once it's native on all laptop or desktop computers.

For example, what happens if a user loses a password -- essentially leaving the drive filled with data that can no longer be unencrypted? Or what if a drive becomes corrupted or damaged, the data has to be recovered by a third party -- and your password is on the drive?

"Then you have just killed yourself," said [Dave Hill](#), an analyst at research firm Mesabi Group.

The [Trusted Computing Group \(TCG\)](#), made up of disk hardware and software vendors, last week published three encryption specifications to cover storage devices in consumer laptops and desktop computers as well as enterprise-class drives used in servers and disk storage arrays.

Some industry observers believe that within five years, all disk drive manufacturers will be offering drives -- both hard disk and solid-state disk -- that use the specifications for firmware-based encryption.

While enterprises using drives with full-disk encryption, such as the [Seagate Momentus 5400 FDE.2](#) drive or [Fujitsu's 2.5 7200rpm self-encrypting drive](#), would monitor them through a central access administrator with a master password to unencrypt, consumers purchasing laptops or desktops with drives would face a more daunting scenario: They would need to either back up their data and their passwords, or lose their drives and data.

[Robert Thibadeau](#), chief technologist at [Seagate Technology LLC](#) and chairman of the TCG, said the current disk-encryption specifications allow users to create more than one password to access data, so that if a user were to lose one, he could still access his hard drive with a backup password.

"Furthermore, with some password settings, you can provide a password that allows erasure so you can put the drive back into use, but the data will be gone," Thibadeau said.

If a drive were to become corrupted or the hardware damaged and a data recovery firm needed to retrieve a user's disk, Thibadeau said, the recovery firm could use the password to recover data from the damaged hardware. The TCG is also working with data recovery firms to create a technique that would allow them to recover encrypted data on drives using the standards, without requiring a user password.

Currently, however, if a user loses his password and a drive becomes damaged or corrupted, the data is not recoverable, Thibadeau admitted.

[David Virkler](#), CIO at AdaptaSoft Inc., a payroll systems software and services company, said that administration of drives with hardware-based encryption is easy and that he has seen no I/O slowdown. Virkler installed Seagate's self-encrypting, 2.5-in. Momentus 5400.2 drives in October 2007 on his company's Dell laptops in order to protect customer financial data that his company often deals with in its service capacity. He paid a \$40 premium for each self-encrypting drive, spending about \$120 total for each 80GB drive.

While the rollout was easy, he acknowledges that if a company doesn't already have a group policy in place -- a domain name server and an active directory -- then it would be "painful" to roll out. "You'd have to manage each laptop individually," he said.

At AdaptaSoft, Virkler instituted a policy at the time of the rollout that warned workers not to keep critical data on their laptops; they were told to always use the company's network drive instead for the highest-priority information in case of a drive failure. "If laptop crashes, I'm not going to expend a lot of energy to get it back. I'd also imagine any data recovery options would be nearly impossible," he said.

Virkler said he's now interested in using self-encrypting drives in his data center, but he's not sure how they would work, since he also runs Citrix and virtualization software.

Ken Waring, IT director at CBI Health in Toronto, said his organization needs encryption on its drives to protect sensitive patient information, but he's also concerned about emerging technologies, including the standardization of full-disk encryption and the problems it might create.

But, as Waring put it, "it's still a million times better than having nothing. And, as a business, you can only take what's available to you."

Mesabi Group's Hill agreed, saying that not only is data with full-disk encryption safe if a computer is stolen or lost, but the technology also automatically puts a company using the drives in compliance with state laws such as California's data breach notification mandate. That law requires companies to notify the public when unencrypted drives are lost or stolen.

CBI Health is a national network of more than 135 community and hospital-based rehabilitation, medical and health care facilities. Three years ago, Waring switched from Lenovo to Dell laptops in order to get hardware-based encryption, replacing a software-based encryption product that he found arduous to manage and unreliable. Waring found that drives encrypted with software would sometimes unencrypt themselves -- leaving the data open to theft. And "we've experienced five drive failures due to the encryption software, but none from hardware," he said.

Today, 90 of CBI Health's 200 laptops use Seagate's Momentus drives with native full-disk encryption. The other users will move to Seagate drives as they are replaced at end of life, Waring said.

CBI Health uses [Wave Systems Corp.'s Embassy Suite encryption management software](#) to monitor its encrypted drives, including storing passwords.

Waring understands the concerns about lost passwords and damaged drives but said that Wave's software allows CBI Health to keep a single administrative password to access encrypted drives in case a user loses his password. In addition, Waring backs up all drives, so if one is damaged, the data is not lost.

"Our company as a whole is trying to harden every element of its architecture," he said. "We felt it was prudent to start where we are most vulnerable -- mobile devices that people leave in their cars or have in their homes."

6 Desk Security Mistakes Employees Make Every Day

From passwords on sticky notes to sensitive contracts left in a pile by the printer, many office workers make the same basic security errors. Even our CSO staff is not immune to these common no-nos - but they are easy to fix

By [Joan Goodchild](#), January 23, 2009 — [CSO](#) —

You've checked all of the entry ways in your office building, you have surveillance technology in place and IT assures you that your firewalls are bulletproof. But have you checked your staff's desks? That may be one of the largest holes in a company's security plan. Desks and other work spaces often have items on or around them that contain sensitive information, and that information can be dangerous if it gets into the wrong hands.

Writing passwords on sticky notes

This was probably the biggest offense we noted when we walked around the CSO office after hours. Several employees had sticky notes on their computer monitors with passwords and/or personal ID numbers written on them. While [employees may have a difficult time](#) keeping track of all of their

passwords, writing that information down on a piece of paper and leaving it out for all eyes to see is never a good idea. Keep in mind that after the office closes, many strangers can access the work space. One can never tell when a person might try and use employee passwords to compromise an account.

Writing sensitive information on a white board

Staff often brainstorm together and write down their ideas on a whiteboard. Several offices here at CSO had whiteboards. We found one with client names and billing information written on it. The information would have been very valuable to any potential competitors. After a work session, employees should put information in a less obvious place and put it away after hours. Advise staff to erase all whiteboards regularly.

Leaving sensitive documents on the desk

Also on several desks, we spotted detailed client contracts with billing terms. Like the whiteboard, the information might be valuable to competition. But depending on who views it, the client's information might also be used for ill-gotten gains. Any documents with sensitive data belong in a locked drawer or container.

Leaving a calendar or day planner out on a desk

One day planner we found contained private sales-related information. But a calendar might also contain the agenda or travel itinerary of a member of the staff. Depending on the company, that staff member (an executive, for instance) might be a potential target. All calendars and day planners should be locked up or taken out of the office at the end of the day.

Leaving an access card out

We found one desk with an access card hidden under a keyboard. That's not much better than leaving it in plain sight - it's like putting your house key under the welcome mat, the first place a thief will look. Access cards are used to protect staff from an unwanted intrusion. If an access card gets into the wrong hands, it can allow unauthorized people to roam around freely. Staffers should keep possession of their cards at all times.

Forgetting the printer

The printer in our office had several vendor contracts discarded in a pile of papers. After staff finish with printing jobs, they need to be mindful of any documents that were printed, even the ones that aren't needed, and dispose of them appropriately.

Parking Tickets as Cyber Attack Social Engineering Vector

(February 4 & 5, 2009) Cyber criminals in Grand Forks, North Dakota planted phony parking violation notices on cars. The notices direct the users to a website for more information, which leads the users through a set of links that downloads malware onto their computers. That malware then urges users to download an anti-virus scanner that is worthless. Another scam first uncovered by Internet Storm Center:

[Editor's Note (Ullrich): Fake anti virus software has been an issue in the past, but seems to be gaining some steam lately. The only lucky break we get is that most of these packages are indeed totally fake and do nothing. Of course, once in a while you do hit one that will not clean out a real virus, but it will install its own malicious software.

(Ranum): I've been wondering how long it'd take scammers to figure that out. There are several real-world-based vectors for stealing personal account information offline. I could easily see an underground economy for such a thing. Imagine if kids got an offer of cash payments via paypal to bicycle around and collect financial statements from unsecure mailboxes, scan them, and email the scans to an onion-routed address.

Ultimately, the scammers are going to force financial institutions to rethink how they perform authentication.]

Massive ATM Fraud Linked to WorldPay Breach

February 3, 2009) The FBI is reportedly investigating an international ATM (automatic teller machine) scam in which thieves stole millions of dollars from cash machines in 49 cities in a very brief period of time. The scam is believed to be linked to a data security breach at RBS WorldPay, which offers a service allowing employers to pay employees directly to a payment card that works much like a debit card. The attackers managed to gain access to the system and find a way to clone the cards. The attack was startlingly well-coordinated. In less than one hour on November 8, 2008, 130 ATMs in 49 cities around the world were accessed using the fraudulent cards. The attackers also managed to do away with the limits on cash withdrawals, so the people retrieving the money from the machines were able to use their cards again and again. All told, just 100 cards were used to steal US \$9 million. The people withdrawing the cash are believed to be recruited accomplices who were likely paid small fees.

[Guest Editor Rob Lee, SANS Institute Forensics/IR Faculty Fellow:

Class action lawsuits are encouraging silence among victims due to the high cost of voluntary disclosure. With victims not sharing details, the criminals are becoming more brazen in their crimes as the risk of arrest is low and the payout is extremely high. We have to stop the criminals, not keep blaming the victims.]

Calif. DMV tried to sneak in biometrics for driver's licenses, groups claim

DMV buried plan to use facial recognition, thumbprint technology in a vendor contract, consumer advocates say

By Jaikumar Vijayan

February 5, 2009 (Computerworld) Consumer rights groups in California are protesting what they claim is an attempt by the state [Department of Motor Vehicles](#) to sneak in via the backdoor a fingerprint and [facial-recognition system](#) for issuing driver's licenses in the state.

The groups claim that the use of such [biometric technology](#) has been opposed by state legislators in the past, and that the DMV was trying to do an end-run around opposition by hiding its plans in a seemingly innocuous vendor contract.

If unchallenged, the contract would allow the DMV to establish a new government biometric database containing facial and [fingerprint information](#) on more than 25 million Californians over the age of 16, without first giving legislators and technology experts a chance to vet the proposal.

The DMV did not respond to a request for comment.

Among the groups trying to stop the DMV from going ahead with its plans are the California chapter of the [American Civil Liberties Union](#), the Consumer Federation of California, the [World Privacy Forum](#) and the [Electronic Frontier Foundation \(EFF\)](#). The groups are calling on state legislators to quickly stop the planned vendor contract from moving ahead.

The DMV's proposal to introduce new biometric technologies was contained in an application for a new vendor contract for the production of state driver's licenses and ID cards starting in June. The application, a copy of which was obtained by *Computerworld*, was forwarded to the state's Joint Legislative Budget Committee via the California Department of Finance on Jan. 14.

The application detailed the DMV's plans to implement thumbprint and facial-recognition technology for verifying the identity of applicants for new driver's licenses and state ID cards. During the process of obtaining a license, a driver's thumbprint would be taken at the DMV office to verify the identity of the applicant, according to the document.

In addition, "the facial-recognition software has the ability to compare an individual's new photo against the latest photo for all other records on the database and identify those records that may be the same individual," the DMV application stated.

The automated image-verification process will reduce errors and the number of fraudulent driver's licenses issued by the state, it said. The application noted that more than 1,200 files are matched to the wrong individual every year.

The DMV said that its plan would cost the state roughly \$63 million over the next five years. It also noted that several other states, including Texas, New Mexico, Oregon and Georgia, had implemented facial-recognition technology and were reporting success with it.

Plan raises privacy, security issues

The problem is that the DMV's plan has not been vetted by anyone and no analysis has been made of the potential security and privacy implications, said Richard Holober, executive director of the Consumer Federation of California.

"We believe that important policy changes should be determined by elected officials, but that's not what is happening here," Holober said. "This is an attempt to slip something through that really should have been vetted in a hearing process in the legislature," with the public and technologists given a chance to comment on it, he said.

Although thumbprints and facial-recognition software can be useful in deterring crime and fraud, they also pose serious privacy and security risks, he said.

The information contained in the California DMV databases, for instance, is accessible by law enforcement and other government agencies. Without guidelines for access, there's nothing to prevent the biometric data from being used for other purposes, including surveillance, Holober said.

"What if someone goes to a picket line or a protest rally, and someone were to use the DMV repository to profile and track them down because they spoke out on issues?" he asked. "We are not saying this is the intent of the DMV. We are just saying that there are other uses" for biometric data, he said.

The consequences of a data breach involving biometric information are also significantly higher compared with a breach involving nonbiometric identifiers, said Pam Dixon, executive director of the World Privacy Forum in San Diego. "What happens if the data gets compromised and falls into the wrong hands?" she said.

Unlike other forms of identification, such as a driver's license number, a biometric identifier such as a facial image or thumbprint, cannot be changed in the event of a data breach, potentially resulting in lasting problems for victims, added [Lee Tien](#), a senior staff attorney at the EFF. "Basically, any kind of biometric is a piece of information that is uniquely linked to you and cannot be revoked," he said.

Such issues explain the need for "a robust public debate," Dixon said. Academic and security experts need to first study all of the privacy and security implications involved in the collection, storage, use, sharing and protection of biometric data, she said.

"This was sneaky, there's no other way around it," Dixon said. "California has said no to this type of technology with no proper safeguards in the past," she said. Various bills on the use of biometric technology with driver's licenses have been proposed, including

[California is one of several states that has refused to implement the federal Real ID Act](#) which requires DMVs around the nation to adopt new verification standards for vetting the identities of driver's license applicants.

The act, which also calls for the use of biometric identifiers, was approved by Congress and signed into law by [President Bush](#) in 2005. Since then, it has faced a maelstrom of protest from states that see it as an attempt by the U.S. Department of Homeland Security to force unwanted ID standards down their throats, while also making the states pay for the program.

New Disk Encryption Standards Could Complicate Data Recovery

So, what do you do if you lose your password?

By Lucas Mearian, Computerworld

February 03, 2009 — [CSO](#) —

When the world's largest disk-makers joined last week to announce a [single standard for encrypting disk drives](#), the move raised questions among users about how to deal with full-disk encryption once it's native on all laptop or desktop computers.

For example, what happens if a user loses a password -- essentially leaving the drive filled with data that can no longer be unencrypted? Or what if a drive becomes corrupted or damaged, the data has to be recovered by a third party -- and your password is on the drive?

"Then you have just killed yourself," said [Dave Hill](#), an analyst at research firm Mesabi Group.

The [Trusted Computing Group \(TCG\)](#), made up of disk hardware and software vendors, last week published three encryption specifications to cover storage devices in consumer laptops and desktop computers as well as enterprise-class drives used in servers and disk storage arrays.

Some industry observers believe that within five years, all disk drive manufacturers will be offering drives, both hard disk and solid-state disk, that use the specifications for firmware-based encryption.

While enterprises using drives with full-disk encryption, such as the Seagate Momentus 5400.2, would monitor them through a central access administrator with a master password to unencrypt, consumers purchasing laptops or desktops with drives would face a more daunting scenario: They would need to either back up their data and their passwords, or lose their drives and data.

[Robert Thibadeau](#), chief technologist at [Seagate Technology LLC](#) and chairman of the [TCG](#), said the current disk-encryption specifications allow users to create more than one password to access data, so that if a user were to lose one, he could still access his hard drive with a backup password.

"Furthermore, with some password settings, you can provide a password that allows erasure so you can put the drive back into use, but the data will be gone," Thibadeau said.

If a drive were to become corrupted or the hardware damaged and a data recovery firm needed to retrieve a user's disk, Thibadeau said, the recovery firm could use the password to recover data from the damaged hardware. The TCG is also working with data recovery firms to create a technique that would allow them to recover encrypted data on drives using the standards, without requiring a user password.

Currently, however, if a user loses his password and a drive becomes damaged or corrupted, the data is not recoverable, Thibadeau admitted.

[David Virkler](#), CIO at AdaptaSoft Inc., a payroll systems software and services company, said that administration of drives with hardware-based encryption is easy and that he has seen no I/O slowdown. Virkler installed [Seagate's](#) self-encrypting, 2.5-in. Momentus 5400.2 drives in October 2007 on his company's Dell laptops in order to protect customer financial data that his company often deals with in its service capacity. He paid a \$40 premium for each self-encrypting drive, spending about \$120 total for each 80GB drive.

While the rollout was easy, he acknowledges that if a company doesn't already have a group policy in place -- a domain name server and an active directory -- then it would be "painful" to roll out. "You'd have to manage each laptop individually," he said.

At AdaptaSoft, Virkler instituted a policy at the time of the rollout that warned workers not to keep critical data on their laptops; they were told to always use the company's network drive instead for the highest-priority

information in case of a drive failure. "If laptop crashes, I'm not going to expend a lot of energy to get it back. I'd also imagine any data recovery options would be nearly impossible," he said.

Virkler said he's now interested in using self-encrypting drives in his data center, but he's not sure how they would work, since he also runs Citrix and virtualization software.

Ken Waring, IT director at CBI Health in Toronto, said his organization needs encryption on its drives to protect sensitive patient information, but he's also concerned about emerging technologies, including the standardization of full-disk encryption and the problems it might create.

But, as Waring put it, "it's still a million times better than having nothing. And, as a business, you can only take what's available to you."

Mesabi Group's Hill agreed, saying that not only is data with full-disk encryption safe if a computer is stolen or lost, but the technology also automatically puts a company using the drives in compliance with state laws such as California's data breach notification mandate. That law requires companies to notify the public when unencrypted drives are lost or stolen.

CBI Health is a national network of more than 135 community and hospital-based rehabilitation, medical and health care facilities. Three years ago, Waring switched from Lenovo to [Dell](#) laptops in order to get hardware-based encryption, replacing a software-based encryption product that he found arduous to manage and unreliable. Waring found that drives encrypted with software would sometimes unencrypt themselves -- leaving the data open to theft. And "we've experienced five drive failures due to the encryption software, but none from hardware," he said.

Today, 90 of CBI Health's 200 laptops use Seagate's Momentus drives with native full-disk encryption. The other users will move to Seagate drives as they are replaced at end of life, Waring said.

CBI Health uses Wave Systems Corp.'s Embassy Suite encryption management software to monitor its encrypted drives, including storing passwords.

Waring understands the concerns about lost passwords and damaged drives but said that Wave's software allows CBI Health to keep a single administrative password to access encrypted drives in case a user loses his password. In addition, Waring backs up all drives, so if one is damaged, the data is not lost.

"Our company as a whole is trying to harden every element of its architecture," he said. "We felt it was prudent to start where we are most vulnerable -- mobile devices that people leave in their cars or have in their homes."

German Magazine Says Armed Forces Establishing Cyber Warfare unit

(February 9, 2009) German magazine Der Spiegel Reports that the country's armed forces are in the process of establishing a unit dedicated to cyber warfare. The unit will take on responsibility for protecting German IT infrastructure from attacks as well as conduct reconnaissance and interventions on foreign and "enemy" computer networks.

[Editor's Note (Skoudis): To me, this seems perfectly natural. Many battles have occurred in the cyber realm already, and will do so increasingly. I also think a nation state should signal its willingness to engage in that arena, lest its adversaries assume weakness leading to potentially tragic miscalculations.]

Costs of a Data Breach: Can You Afford \$6.65 Million?

By Larry Ponemon

February 4, 2009 (CIO) Affixing a dollar cost to a problem has immense benefit, and [The Ponemon Institute](#) goes to great lengths to arrive at the figures for its Annual Cost of a Data Breach Study.

We painstakingly analyzed the financial impact a [data breach](#) has on a company by examining 43 different companies from a cross section of industries, all of which experienced a significant data breach affecting a range of data records representative of the norm. And knowing that a data breach may cost your company \$6.65 million dollars may be all the information that is needed for a company to [assign an appropriate budget to those tasked with information security](#).

In 2008 the average total cost of a data breach was \$6.65 million, up from \$6.35 million last year and \$4.54 in 2005. In 2008, the per-victim cost of a data breach was \$202, up from \$197 in 2007, and from \$138 when the study was launched in 2005. Breaches involving a third party to which data had been outsourced bore a per-victim cost of \$231, whereas self contained breaches bore a per-victim cost of \$179. Breaches that were the result of a malicious act bore a per-victim cost of \$225, whereas breaches that were the result of negligence bore a per-victim cost of \$199. Breaches that were the result of a lost or stolen laptop computer bore a per-victim cost of \$249, whereas breaches that did not involve a lost or stolen laptop computer bore a per-victim cost of \$177. If the data breach was a first-time event for the company the per victim cost was \$243, but if the company had experienced a breach previously the per victim cost was \$192.

The simple conclusion to these numbers is clear: the financial impact for a company that experiences a data breach is significant and rising. That finding alone may be alarming, but it seems to merely quantify what most people already knew to be true. The "wow" factor comes when you realize that we haven't simply identified the cost of an inevitable outcome, as if to tell the world, "buckle up and brace for impact," but we've shown that companies well have the means to significantly diminish their loss if and when a breach occurs.

Consider the last data point on our list. First-time data breaches cost companies \$51 more per victim than for companies who had already learned the hard lessons of data breach. That means the previous experience resulted in a smarter, more efficient response the second time around. Last year the Ponemon Institute began working with [risk management](#) firm WillisHRH on a [data breach](#) response tracking system called the Privacy Breach Index. We use the PBI to analyze the methods and strategies used by companies when responding to a breach, and the outcome of the response, to create best practices so other organizations don't have to learn from their own experience.

Looking at other data points, given that the per victim cost of a data breach involving outsourced data was \$52 more than when no vendor was involved, it stands to reason that a better vendor management program might help reduce risk and cost. Stricter policies for and better enforcement of [mobile data security](#) might help to reduce the risk and impact of a data breach resulting from a lost or stolen laptop computer or other mobile device. More efficient data governance could go a long way toward reducing the cost of a breach by preventing unauthorized or improper access to data. These are just some of the conclusions we reach based on a superficial look at the study's results, but as we dive deeper into the data and look at other factors, our focus becomes sharper and our reaction more informed, allowing us to apply more specific measures to information management, security, and [compliance](#).

Examples here involve the impact of lost business resulting from a data breach. This year, [lost business costs](#) rose to a level 38 percent higher than in 2005. What's more, healthcare and financial services organizations experienced much higher abnormal customer loss-6.5 percent and 5.5 percent respectively-when compared with retail and consumer products organizations, whose churn rates were found to be 1.5 percent and 3.6 percent respectively. The significant difference in these rates of customer loss can be explained in one word: trust. Violate a consumer's trust and they are more likely to walk, and that likelihood increases when the breach involves an organization in which the consumer has placed a great deal of trust.

What do I mean? When a consumer chooses to do business with a financial services or healthcare organization, they tend to conduct more due diligence than when they walk through the doors of a department store to buy a shirt or a pair of shoes. A retail purchase is a simple transaction, but banking and healthcare requires entrusting an individual or organization with a great deal of highly sensitive information. Violate that trust and the customer may be more inclined to look for a new relationship. This is especially evident when the consumer receives multiple breach notifications from such an organization.

The risk of a data breach incident is real and ever present. The Ponemon Institute agrees with the belief that a data breach is not a matter of if, but when, but we also strongly believe that there is a body of knowledge that can be used to understand the issues and consequences of a [data breach](#), and that forewarned is forearmed. By acting in advance, companies can do much to diminish the likelihood of a data breach, and to lessen the effects should one occur.

[Dr. Larry Ponemon](#) is founder and chairman of the Ponemon Institute, a think tank dedicated to understanding and advancing responsible information and privacy management practices in business and government through independent research. Ponemon Institute research, expertise, and thought leadership is used to educate private and public sector organization on privacy and data protection practices in a variety of industries. The Annual Cost of a Data Breach Study is an independent research report conducted by the Ponemon Institute and underwritten by [PGP Corporation](#), a global provider of email and enterprise data encryption products.

Survey: 40% of hard drives bought on eBay hold personal, corporate data

Buyers found data on everything from corporate spreadsheets to e-mails and photos

By Lucas Mearian

February 10, 2009 (Computerworld) A New York computer forensics firm found that 40% of the hard disk drives it recently purchased in bulk orders on [eBay](#) contained personal, private and sensitive information -- everything from corporate financial data to the Web-surfing history and downloads of a man with a foot fetish.

[Kessler International conducted the study](#) over a six-month period, buying up disk drives ranging in size from 40GB to 300GB from the United States and Canada. The firm, which completed its research about two weeks ago, bought a total of 100 relatively modern drives, the vast majority of them Serial ATA.

"With size of the sample, I guess we were surprised with the percentage of disks that we found data on," said Michael Kessler, CEO of Kessler International. "We expected most of the drives to be wiped -- to find one or two disks with data. But 40 drives out of 100 is a lot."

Kessler believes the drives were likely from computers sold to third-party resellers that disassembled them and sold off the parts.

Kessler's engineers had to use special forensics software to retrieve data from some of the hard drives, but other drives contained sensitive data in the clear, having never been overwritten or erased. The data included personal documents, financial information, e-mails, DNS server information and photographs.

"The average person who knows anything about computers could plug in these disks and just go surfing," Kessler said. "I know they found a guy's foot fetish on one disk. He'd been downloading loads and loads of stuff on feet. With what we got on that disk -- his name, address and all of his contacts -- it would have been extremely embarrassing if we were somebody who wanted to blackmail him."

Kessler said his company specifically avoided buying drives whose sellers indicated that the drives had been erased.

Kessler International offered this breakdown of the kind of data it retrieved: Personal and confidential documents, including financial information, 36%; e-mails, 21%; photos, 13%; corporate documents. 11%; Web browsing histories, 11%; DNS server information, 4%; miscellaneous data, 4%.

"We were more concerned with searching for people's identification, which is what we found, but we were surprised by all the corporate spreadsheets and business finance records we found," Kessler said.

The forensics firm even found one company's "secret" recipe for French fries, Kessler said.

In recent years, hard drives have shown up on eBay that contain all kinds of sensitive data. In April 2006, Idaho Power Co. learned that drives it thought had been recycled had actually [been sold on eBay with the data still intact](#). The Boise, Idaho-based utility had used the drives in servers; when bought on eBay, the drives still contained proprietary corporate information such as memos, customer correspondence and confidential employee information.

And in 2007, a supposedly new hard drive purchased on eBay was found to contain [information from the Arkansas Democratic Party](#).

Charles Kolodgy, an analyst with research firm IDC in Framingham, Mass., said drives from PCs are mostly easily protected even after resale by using a full-disk encryption (FDE) product, but he said prior to selling an old machine, users should still format the drive and use overwrite tools just to be sure. "But if you have FDE you don't need to be as concerned if something falls through the cracks," he said. For larger hard drives, disks should be erased using industrial degaussers. As for the drives Kessler purchased from eBay, the company plans to use a U.S. Department of Defense-grade [degausser and erase the data](#). It will then either throw out the drives or re-use the models with sufficient capacity.

