

Security Trends Report

11/16/07

Gartner: Most security threats can be addressed without additional investment

Throwing money at problems is no substitute for thinking them through

Jaikumar Vijayan

October 15, 2007 ([Computerworld](#)) -- IT managers trying to figure out how much money to budget for information security purposes each year might want to take note of some recent advice from [Gartner Inc.](#): Despite the growth in targeted attacks and the continuing discovery of new vulnerabilities, almost 90% of the threats companies face today can be handled without any extra investment in security.

Instead, companies need to reduce some of the money they've spent over the past few years protecting against mass attacks -- redirecting those freed-up resources to confront more narrowly directed emerging threats.

A lot of companies spend too much money on security controls such as firewalls, antivirus software and other desktop protection tools designed to defend against traditional mass attacks, said Gartner analyst [John Pescatore](#).

According to Pescatore, over the years such products have become highly commoditized and can be deployed for far less than many companies currently shell out for such protection.

"A lot of it is just inertia," he said. For instance, companies that signed up with one vendor years ago simply continue to do business with that vendor without exploring any of the cheaper and equally functional options available for desktop protection. Those who might be inclined to make the switch to cheaper technologies often mistakenly assume that such migrations are either prohibitively expensive or too complex.

The same is true for the multitude of remote access technologies that companies continue to support with very little reason to do so.

According to Pescatore, such inefficiencies have resulted in average organizations spending more than 5% of their IT security budget on security, and close to 12% if disaster recovery is included. However, he said, Gartner has seen little evidence to suggest that the more you spend on security the better your security gets. In fact, companies with really mature security practices rarely average more than 4% of their total IT budget on security.

"Security strategies must reduce the cost of dealing with mass attacks to free up investment and personnel resources" for dealing with today's more complex targeted attacks, Pescatore said.

"Being aware of 'inside out' communications and being able to block those as effectively as 'outside in' is becoming increasingly important."

Such planning is important at a time when the costs associated with security breaches are going up sharply. Over the next two years in fact, companies can expect breach-related costs to increase on average by 20% each year compared to today, according to Gartner.

That increase, said Pescatore, is fueled by several factors. Increasingly, companies that suffer data breaches are getting sued by victims as well as by other affected parties. Though such suits have gone nowhere so far, companies can expect such costs to become a major factor when calculating data breach costs, he said. Pescatore also points to increased pressure from state lawmakers looking to hold companies fiscally responsible for the costs associated with data breaches.

Gartner Sees Rise in Cost of Data Breaches

Oct 15, 2007

Financially motivated data breaches are set to cost businesses 20 percent more each year until 2009, according to Gartner.

John Pescatore, VP at Gartner, said the biggest risk to organizations came from targeted attacks. He said that "phishing and identity theft attacks have caused the rise of 'credentialed' attacks, in which the attacker uses the credentials of a legitimate user."

Malicious software attacks allowed internal executables to be used to forward information to an external attacker, Pescatore warned. "Being aware of 'inside out' communications and being able to block those as effectively as 'outside in' is becoming increasingly important," he said.

It was important to make sure that security strategies reduced the cost of dealing with mass attacks, Gartner advised, in order to free up budgets for the next generation of security attacks.

The analyst group reckons the average business is spending more than 5 percent of its IT budget on security, and another 7 percent on disaster recovery.

But it said 90 percent of targeted attacks could be avoided without an increase in firms' security budgets, and said the investments that enterprises had made in intrusion prevention, vulnerability management and network access control had largely paid off.

At the same time, however, it warned that there was currently little or no correlation between organizations that spent the most on security and those that are most protected, it said.

It said the most effective way to become increase the efficiency of security spending was to avoid vulnerabilities by ensuring that security was a top requirement for every new application, process and product

"Privacy, Security Depend on Program Managers, Experts Say"

Federal Computer Week (10/12/07) ; Mosquera, Mary

To effectively manage risk, project managers must adopt security and privacy best practices early on in the development of systems, according to Robert Wright, former chief of the plans and program management unit in the FBI's Cyber Division. The Privacy Act and the Office of Management and Budget's requirements for security and privacy are helpful resources for program managers determining which practices to implement, says Sally Wallace of the Veterans Affairs department. Agency executives who are accountable for the organization's adherence to such laws and regulations typically delegate those compliance duties to program managers to carry out in daily operations. For instance, OMB has ordered agencies to decrease their use of Social Security numbers and to utilize personally identifiable data only when essential. As a result, when program managers develop systems that collect or use sensitive information, the managers must also generate privacy impact assessments. The appraisals are a means for guaranteeing that privacy is attended to throughout each IT system; the evaluations also detect risks in gathering data, Wallace says. The Privacy Act also requires information from agencies regarding their standards for using personal information.

"Desktop Users Remain Biggest Security Threat"

ZDNet Australia (10/11/07) ; Browne, Marcus

Businesses have greater concern about desktop users than outsourced labor and remote users, reveals a new Sophos survey. Forty-four percent of respondents said that vulnerabilities were more likely via desktop usage, while 11 percent reported guests as potential threats. Users logging onto to remote networks were cited by 31 percent of respondents as the most likely security liability. Although the number of mobile users has grown considerably in businesses, Sophos' Paul Ducklin says the results underscore the fact that administrators have not grown complacent about securing desktop networks. With increasing usage of external storage devices such as USB drives and factoring in inevitable risks such as damages or loss via mobile usage, Ducklin says "administrators are realizing that the risks exist wherever you use your computer."

"What Are Your Weaknesses?"

Security Management (10/07) Vol. 51, No. 10, P. 62 ; Wagley, John

Growing concern over data loss and theft, coupled with increasingly stringent regulations, is prompting a rising number of organizations to run formal assessments of their IT infrastructures. Retailers and card processors are strongly encouraged to adhere to the Payment Card Industry Data Security Standard, though compliance is technically voluntary. An assessment's first step entails conducting an inventory of the technological assets to be inspected. Secondly, multiple vulnerability

scanners are used to search for network weaknesses such as misconfigured servers and missing patches. More and more, such scans are scrutinizing applications as well, as applications are highly targeted by modern hackers. The majority of vulnerabilities are located in Web-based applications, including exploits like cross-site scripting and SQL injections. Penetration tests are also an effective way to demonstrate the actual impact of network flaws. Modern security assessments are examining a company's workers, processes, and policies in addition to technology, as many security breaches are caused by company personnel, whether intentionally or inadvertently. The results of security assessments are also increasingly being viewed through the lens of a company's overall business risks in order to eliminate inefficient IT spending and encourage a proactive approach to security. Khalid Kark of Forrester Research explains that information risk management is what is important today and that assessments should "take into account how businesses use information, who has access to information, how data needs to be secured and what the risk is of losing data."

By Means of a Network By Means of a Human – Accountability and Responsibility is Still the Same

Submitted by [Jeff Bardin](#) on Fri, 2007-09-21

Connecticut attorney general Richard Blumenthal announced he is suing the company for illegal negligence, unauthorized use of state property, and breach of contract. According to an advisory from the attorney general's office, the lawsuit alleges that Accenture converted state property to its own use without permission, acted negligently, and violated its contract by allowing the sensitive data to be placed on a state of Ohio backup computer tape that was later stolen.

I couldn't agree more. All too often I have seen companies like Accenture (Big 4r types) use interns and college students (as standard practice) to mine data during external audits. They are untrained; they are housed on sight in veal pens; they leave sensitive data around the pen area; and their laptops are largely not encrypted. These outside firms object when we require them to demonstrate their controls over our data prior to their removing it from the premises. The uproar over a CISO's actions by these firms in these cases can be heard all the way to New Zealand. It is much like the cop breaking the law in order to enforce it.

"Accenture deserves censure -- to be held accountable for allowing valuable secret data to be stolen and putting at risk state taxpayers, bank accounts, and purchasing cards," Blumenthal said in a statement. "Accenture acted unconscionably and illegally. It breached its commitment to keep confidential this highly sensitive financial information. The company broke its contractual promises and duty of care to safeguard the secrecy of sensitive data. It misappropriated state property -- taking significant valuable data for its own use without permission or authority."

Accenture released a statement saying the company is reviewing the matter basing the mistake on human error.

Regardless of whether it was advertent or inadvertent loss, destruction, disclosure and/or modification of the information, it is an egregious breach. Their controls did not work and obviously, they do not have the right controls in the right places to ensure such an action cannot happen. It is the same type of pressure CISO's get from outside auditors when reviewing controls. Does it work all the time every time or does it only work 90 times out of 100. At the least that is a deficiency and depending upon the sensitivity of the data and impact the loss of the data can have, is it then seen as material?

"Based on what we know today, we believe that our policies were inadvertently not followed," the statement read. "We intend to take appropriate actions with any individuals involved and to reinforce with all of our employees, as we do on a regular basis, the importance of following our privacy and data protection policies."

Who audits their practices? Who audits the auditors?

The company also asserted that there is no evidence that the Connecticut data has been accessed or misused by an unauthorized third party. In this day and age, I don't know any criminal who acts like a script kiddie and posts his boastful winnings online.

"As the Ohio inspector general determined, the technical complexity of retrieving the data from the backup tape storage device makes the possibility that it will be used for improper purposes remote," the company noted. "We invest heavily in training our employees so they understand how to appropriately handle sensitive data and we impress on them the importance of following our policies. Accenture regrets this unfortunate incident, which was clearly caused by human error, and remains committed to working with our client in this matter."

Accenture should just stand up and admit the issues and errors; accept the fine and become the poster child for corrective action. When I grew up, we were taught that when you make a mistake, you admit it and take the heat.

Phishers (almost) scam grocery giant out of \$10 million

Social engineers come close to reeling in a big one

Jaikumar Vijayan

October 22, 2007 ([Computerworld](#)) -- Apparently it's not just unwary individuals that fall victim to online scammers. Even large corporations, it seems, can get suckered into parting with their money by devious phishers.

Case in point: Eden Prairie, MN.-based grocery chain Supervalu Inc., which earlier this year got conned into depositing more than \$10 million into two fraudulent bank accounts before recognizing the ruse. Details of the case are contained in court documents filed in connection with two forfeiture cases stemming from the incident.

According to federal court filings in the U.S. District Court for the District of Idaho, the fraudulent activity took place in late February and early March this year. In the court filings, Stephen Kilgoff, Supervalu's vice president of legal affairs, said that on February 26 and 28 the company received two separate e-mails, one purporting to be from an employee at American Greetings Corp. and the second from an employee at Frito-Lay, both company-approved vendors.

Both e-mails told Supervalu to send future payments for each vendor to new bank account numbers. In the case of the e-mail that purported to be from American Greetings Corp., Supervalu was advised to send payments to an HSBC account in Miami. The other e-mail advised Supervalu to send Frito-Lay payments to an account at First Security Bank in Rogers, Arkansas.

Between Feb 28 and March 3, Supervalu deposited just over \$6.5 million via multiple wire-transfers to the HSBC account, thinking that it was sending the money to American Greetings Corp. Similarly, on March 2 it made eight separate wire-transfers to the bank in Arkansas, depositing a total of \$3.6 million to an account it thought belonged to Frito-Lay.

In addition to the \$6.5 million deposited by Supervalu into the HSBC account, an additional amount of \$500,000 had been deposited into the same account by a second company, identified as "ROHM" on court documents. No information has been available concerning the second company, and it is not a party to subsequent litigation.

Around March 6, according to the filings made by Kilgoff, Supervalu discovered that it had been "induced" into making the transfers to the bogus accounts. Following the discovery of the fraud, Supervalu quickly notified the appropriate law enforcement authorities, who managed to recover nearly all of the money before it could be withdrawn from the accounts.

The recovered money is now being claimed by Frito-Lay, American Greetings *and* Supervalu. In making the claim to the recovered money, Frito-Lay said that it believes the money belongs to Supervalu and said supported that company's claim to ownership of the misdirected funds.

"However to the extent there is any determination that the ownership of these funds changed from [Albertsons](#) / Supervalu [*the Albertsons grocery chain was recently [acquired](#) by Supervalu -- eds.*] to Frito-Lay (as a result of the attempted transfer, the misdirection, or any other development) Frito-Lay makes this claim to these funds in the alternative and subject to any claim of ownership by Albertsons / Supervalu" the company said in an affidavit.

A federal judge is expected to rule sometime in November on which firm should receive the recovered funds.

A spokeswoman from Supervalu responded via e-mail to a request for comment. "As indicated by the forfeiture complaint filed by the U.S. Attorney's Office in Boise, Supervalu was the target of attempted financial fraud," spokeswoman Haley Meyer said. "Due to our internal controls and processes, we were able to quickly discover and report this to the [FBI](#). As a result of the quick work of the Boise FBI Office and the U.S. Attorney, any funds lost are minimal."

Get Serious About Info Integrity

Mark Hall

October 29, 2007 ([Computerworld](#)) -- Madhavan Nayar isn't surprised that 58% of the 653 members of Financial Executives International who responded to its 2007 survey said their "most pervasive critical technology concern" is information integrity. The CEO of Infogix Inc. in Naperville, Ill., says the top financial executives at large companies understand that "the integrity of information cannot be taken for granted." You'd think IT would have assuaged that concern years ago with sleek systems that run 24/7 and track every cent, incoming and outgoing. But you'd be wrong. Nayar points to several areas where IT puts data integrity at risk, such as ill-conceived or widely ignored change policies for equipment and software. Plus, he notes, many companies have islands of incomplete or isolated information and use lousy data-conversion techniques. Add in IT complexity and security concerns, and it's little wonder that CFOs are worried despite the armies of auditors they command. As Nayar notes, "Auditing is obsolete." He wants the entire industry to go beyond it to address the problem. He suggests formulating rigorous standards to manage information, teaching information integrity strategies in schools and offering

certification in that area. And of course, CIOs need to make information integrity their highest priority. Nayar thinks that if they do, they'll have strong support from their CFOs.

Secure All Code

Most modern software development shops use sophisticated methods and products to discover security holes in their code. For some time, Fortify Software Inc.'s Source Code Analyzer has been one of those tools, helping all manner of programmers who use a variety of integrated development environments, operating systems and languages. The next version, due the first week of December, looks forward by adding ultrahip PHP and JavaScript support, but it also looks backward at the antiquated source code running in your data center. According to Barmak Meftah, senior vice president of products and services at Palo Alto, Calif.-based Fortify, Source Code Analyzer 5.0 will include support for Cobol, Visual Basic and Active Server Pages. He notes that while .Net (which Fortify supports) is tops today among Microsoft users for development, most companies still have plenty of Visual Basic scripts running in their data centers, and some organizations continue to write Visual Basic programs. Meanwhile, Active Server Pages remain littered on Web servers throughout the Internet. And we all know that Cobol programs will never, ever disappear. Fortify's tool starts at \$1,200 per developer.

Cozy Up to Your ISP

Corporate networks must fend for themselves against malware attacks. But Steve Bannerman, vice president of marketing and product management at Narus Inc. in Mountain View, Calif., believes that in the near future, you'll work hand in glove with your Internet service provider on security issues. He says this, in part, because his company's Insight Secure Suite, now used by ISPs to analyze traffic behavior on massive global networks, may soon have hooks behind your firewall to correlate potential malware activity on LANs with similar behavior elsewhere online. By combining the data from companies and ISPs, Bannerman suggests, IT departments could vastly improve their security posture. Though Bannerman thinks it's inevitable that this confluence of security systems will take place, he's vague as to how and when it will happen.

TJX violated nine of 12 PCI controls at time of breach, court filings say

More than 80GB of cardholder data was stolen; company had no clue

Jaikumar Vijayan

October 26, 2007 ([Computerworld](#)) -- New documents filed in a Boston federal court Thursday by banks suing The TJX Companies Inc. over its data breach claim that the Framingham, Mass.-based retailer had not complied with nine of the 12 security controls mandated by the Payment Card Industry (PCI) data security standards when the breach occurred.

Among the deficiencies that contributed to the breach were a failure to properly configure its wireless network, a failure to segment networks carrying cardholder data from the rest of TJX's network and the storage of prohibited data. A forensics expert hired by the company to probe the incident, which exposed data on some 94 million accounts, also identified other deficiencies such as improper patching practices and a failure to maintain adequate logs.

According to the court documents filed yesterday, more than 80GB of cardholder data was illegally transferred to another site in California between July 2005, when the breach first occurred, and December 2006, when it was finally uncovered. TJX, however, did not notice that any such transfer was occurring during that time frame, the court documents noted.

In May 2006, a "traffic capture program" was apparently installed on TJX's networks by intruders to sniff out and capture sensitive cardholder data as it was transmitted -- unencrypted -- over the company's networks. The data that was illegally transferred included large amounts of so-called Track 2 information from the magnetic stripes on the back of payment cards. The storage of such data, which includes personal identification numbers and card verification codes, is explicitly banned under PCI.

The new information from the court documents is being used by the plaintiffs in an attempt to file an amended complaint against TJX. The plaintiffs in the case include the [Massachusetts Bankers Association](#), the Connecticut Bankers Association, the Maine Association of Community Banks and AmeriFirst Banks.

According to the documents, TJX knew before the breach that its wireless networks were insufficiently protected, but took no steps to mitigate the situation. The company also knew that storing Track 2 data was a violation of PCI policies, but it continued to do so anyway.

In addition, the forensic analyst who conducted the investigation, said he had never seen such a "void of monitoring and capturing via logs activity" in a Level 1 merchant like he saw at TJX, the court filings noted.

"As a Level 1 merchant, TJX is subject to the strictest standards related to data security," the plaintiffs noted.

But "these additional facts materially support the claim that TJX's conduct generally" violated laws governing unfair trade practices, they said.

Reports of federal security breaches double in four months

By Jill R. Aitoro jaitoro@govexec.com October 23, 2007

Federal agencies report an average of 30 incidents a day in which Americans' personally identifiable information is exposed, double the number of incidents reported early this summer, according to the top information technology executive in the Bush administration.

The Office of Management and Budget issued a memo in July 2006 requiring agencies to report security incidents that expose personally identifiable information to the U.S. Computer Emergency Readiness Team within one hour of the incident. By June 2007, 40 agencies reported almost 4,000 incidents, an average of about 14 per day. As of this week, the average had increased to 30 a day, said Karen Evans, administrator of the Office of Electronic Government and Information Technology at OMB.

Evans, who spoke Monday at the Executive Leadership Conference in Williamsburg, Va., an annual gathering of government and industry IT executives, attributed the increase to agencies conducting more thorough reporting on security breaches.

"Agencies are erring on the side of [caution], reporting [incidents] first, and then getting more information," Evans said in an interview with *Government Executive*.

She added that only a small percentage of reported incidents pose a significant risk to Americans' personal information.

But the figure of 30 incidents a day concerned a chief information security officer for a large civilian agency attending the conference. "I was surprised by the number," the CISO said. He added that he reports an average of one security incident a week, which is typically caused by an employee who lost a BlackBerry. Since sensitive data is encrypted and handheld devices can be remotely turned off, the agency avoids security breaches that could result in exposure of personally identifiable information, the CISO said.

OMB's 2006 memo states that agencies should report all incidents involving personally identifiable information in electronic or paper form, and agencies should not distinguish between breaches that are suspected to have resulted in exposing personal information and those that agencies can confirm have resulted in exposing personal information.

"An increase in reporting isn't necessarily a bad thing," Evans said. "It means people don't want to end up on the front of the *Washington Post*. High [numbers of] reports reflect increased market awareness."

Visa rolls out new payment application security mandates

Companies accepting payment cards have three years to comply

Jaikumar Vijayan

October 25, 2007 ([Computerworld](#)) -- Amid signs of growing frustration in the retail community over the credit card industry's Payment Card Industry (PCI) data security requirements, Visa on Tuesday quietly rolled out an additional set of Payment Application Security Mandates for all companies that handle credit and debit card transactions.

Under the multiphase initiative, covered entities will have three years to ensure that all their payment applications are compliant with a set of security requirements mandated by Visa ([download PDF](#)). The rules apply to any third-party payment software used by companies for storing, processing or transmitting cardholder data.

For many companies, especially large ones using older payment applications, Visa's mandate could mean "tens of millions of dollars" in upgrades to new technologies over the next few years, said Jim Huguelet, an independent consultant in Bolingbrook, Ill. The mandates will also "by proxy" force vendors of payment applications to finally start implementing security features that have been recommended by Visa and others for some time now, he said.

"This is a really major step forward for the industry in asking payment application vendors to step up and support more directly the compliance efforts of their customers," Huguelet said. Until now, adherence to such standards was an "optional sort of thing" for vendors. "Now it has become clear that payment vendors have to make their software support security standards" or risk being cast aside by their customers, he said.

Visa's mandates have been expected for some time and are designed to address long-standing security weaknesses in the applications merchants use to conduct payment card transactions. The biggest concern has been the fact that many payment applications now in use are designed to store data such as the full magnetic-stripe information from the back of cards, card-

verification code numbers and PIN data. Storing that data has made payment systems an attractive target for hackers and has long been considered a fundamental security weakness. It is a practice that has been explicitly banned under PCI.

However, it has been hard for many companies to comply with this requirement since certain payment applications currently in use -- especially older applications -- are designed to store the prohibited data by default, sometimes without even the knowledge of the companies using them.

Visa has over the last two years or so been pushing the vendors of such payment applications into making their software more secure.

The company has developed a set of so-called Payment Application Best Practices (PABP) to help vendors implement the recommended security features in their software. It maintains a list of [validated payment applications](#) that meet the PABP standards and has been urging companies to start using those applications.

At the same time, Visa has also been circulating a frequently updated list of vulnerable payment applications with instructions to card-issuing banks [to get merchants to stop using such software](#).

Tuesday's announcement formalizes these efforts into a set of standards that companies need to implement with a specific time frame.

The first phase of Visa's payment application security mandates goes into effect on Jan. 1, 2008. After that date, the so-called acquiring banks that authorize companies to accept payment card transactions will be prohibited from authorizing new merchants that use payment applications known to be vulnerable. According to an Oct. 23 Visa bulletin, the goal in the first phase is to deter software vendors from introducing new vulnerable applications into the payment system.

The next two phases, which go into effect on July 1 and Oct. 1, 2008, respectively, are designed to get payment processors, agents and merchants to start using software that is compliant with the new application security standards.

Starting on Oct. 1, 2009, all merchants will be required to start terminating the use of any noncompliant payment applications that they might still have in their environments. The fifth phase, beginning July 1, 2010, mandates the use of only those payment applications that support the new standards, according to Visa.

The application rules complement a separate set of PCI standards that are already in place for all entities handling payment cards. Under PCI, merchants are required to implement a set of 12 security controls such as encryption, transaction logging and access management for protecting cardholder data.

Though the requirements went into effect more than two years ago, a large number of big retailers are still noncompliant because of a variety of issues that include [legacy system challenges, rules interpretation issues and continuously evolving guidelines](#).

--Payment Card Data System Needs Security Overhaul (October 29, 2007)

Gartner analyst Avivah Litan says that to focus solely on retailers' card data security is to take a narrow view of the situation; instead, efforts should be directed toward revamping the payment system's security as a whole. According to Litan, "the banks and the credit card companies could solve this [data security issue] more easily" than the retailers could. Presently, merchants have to retain cardholder data to protect themselves against charge backs and to manage recurring charges and refunds. Banks already have stronger data security measures in place so perhaps they could store the data. Another option would be to require personal identification numbers (PINs) for each transaction; fraud from signature debit transactions is considerably higher than fraud from PIN debit transactions.

<http://computerworld.com/blogs/node/6446>

[Editor's Note (Ullrich): The focus on retailers seems to be wrong.

While they have a part in the systems security, they didn't design it.

At the very least, the payment card industry should at least assist retailers. PINs seem like a sensible improvement.

(Honan): While experience in the UK reinforces Ms. Litan's argument for the introduction of PIN authorised transactions in reducing certain types of fraud, it also demonstrates that criminals will adapt to changing situations. Since the introduction of Chip and Pin in the UK, card-not-present fraud is increasingly at an annual rate of 16% - see

<http://www.computing.co.uk/computing/analysis/2194859/fraud-squad>

"Identity Theft: Costs More, Tech Less"

Network Computing (10/23/07) ; Claburn, Thomas

A study by Utica College's Center for Identity Management and Information Protection (CIMIP) revealed that the median actual dollar loss for victims of identity theft is \$31,356, a much higher figure than suggested by past studies. However, earlier studies primarily concentrated on consumer losses, whereas Utica's study reviewed 517 cases investigated by the U.S. Secret Service, which tend to be major incidents, not minor scams. Indeed, the CIMIP study is the first to review the Secret Services' closed case files, and as such aims to provide empirical data. The report proved that companies as well as individuals are affected by identity theft. The study also discovered that the Internet is not always an essential tool for identity thieves. Of the 517 cases reviewed, 102 cases involved Internet use and 106 involved non-technological means, such as mail rerouting. In other instances, criminals used mail theft to access sensitive information and then used Internet-related tools to create fake documents. Another unanticipated finding was that in the 274 cases with identifiable points of compromise, businesses were the starting point for half of the breaches. Moreover, one-third of the identity theft cases reviewed implicated insiders. Finally, the study's results challenged the belief that most identity thieves are white males, as roughly 50 percent of the offenders were black and roughly 40 percent were white. CIMIP works with corporate, government, and academic institutions to research identity management, information sharing, and data protection, including the Carnegie Mellon University Software Engineering Institute, Indiana University's Center for Applied Cybersecurity Research, and Syracuse University's CASE Center.

"Portable Security"

Government Computer News (10/22/07) Vol. 26, No. 27, ; Cassel, David

A growing number of systems administrators are opting to secure the data on their mobile devices by implementing full-disk encryption instead of only encrypting sensitive files or selected directories. Systems administrators are choosing full-disk encryption over selected encryption because it is much easier to scramble all the data stored on a device than it is to figure out which files should be encrypted. Several state agencies in California, including the California Department of Insurance and the state's Board of Equalization, are using full-disk encryption on their mobile devices. The Board of Equalization is also beginning to use full-disk encryption on desktop PCs as well, says Anita Grandrath Gore, the board's chief communications officer. There are two types of full-disk encryption systems that organizations can use--hardware-based encryption systems and software-based encryption systems. Each type of system has its advantages, says Gartner analyst John Girard. "There are certain levels of security certification that can't be achieved without hardware," he says. "But even so, the software vendors have made an excellent showing of meeting some rigorous government certification [requirements] for protection." But no matter what type of encryption organizations opt to use, they need to be very careful that their employees do not lose the key that unlocks the encrypted files, says Burton Group analyst Trent Henry.

"Managing Technology Shadow IT"

Government Executive (10/01/07) Vol. 39, No. 17, P. 63 ; Noyes, Andrew

The practice of downloading unauthorized applications from the Internet has grown so prevalent that it is now referred to as "shadow IT," and government employees are no exception to the trend. Instant messaging is one example of an Internet-downloaded application that is widely used by government officials as a key mode of communication. However, whether applications are being used to enhance productivity or as entertainment, they pose numerous risks to IT security. The applications may possess vulnerabilities that hackers could exploit to gain access and install malware or steal data. As a result, some IT managers are striving to block applications with firewalls or prohibit their use via rigorous policies. But, according to Alan Paller of the SANS Institute, "Resistance is futile." Instead of battling the technologies, Paller recommends that IT managers find a secure method to permit them. A "comply and connect" strategy will be more effective than a "scan and block" strategy, says Paller. For example, the Air Force will not let any computer link to the Air Force network until all security software and patches have been updated or installed, along with a common configuration. Another solution is to customize IT constraints to the agency's mission and to the job function's level of sensitivity. Nuclear power plant operators, for example, would not have anything on the computer desktop that does not relate to plant operations, says Carnegie Mellon University's Marty Lindner. Experts also recommend that agencies establish and enforce policies regarding what can be downloaded onto computers. Issuing "white lists" of sanctioned applications will also instruct workers as to what they can safely do, which will help balance the IT department's needs with employee productivity.

Hitachi Replacing Car Keys With Finger-Vein Scanner

Biometric device could also be used to log in to PCs and ATMs

Sharon Gaudin

October 30, 2007 ([Computerworld](#)) -- Tired of hunting for your car keys?

If you are, researchers at [Hitachi Ltd.](#) just might be working on something just for you.

The Tokyo-based company is developing a biometric device that would identify a driver by reading the veins in his fingers. Each finger could authorize something different, according to Hitachi. For instance, one finger could authorize the driver to start the car, another finger could be scanned to adjust the seat or mirror, and yet another finger could authorize the payment for a hamburger at a drive-through.

The company would not divulge how soon the technology might be fitted into automobiles coming off the production line. However a spokesman did say that Hitachi is working to commercialize the biometric technology and that it will start with the automotive industry.

The finger-vein reader, similar to the more well-known fingerprint reader, works by matching up the veins in the driver's finger to corresponding information stored in the device's database. The scanner reads the finger-vein pattern by passing light through the finger.

Hitachi noted in a release that its engineers have been researching ways to use biometric authentication technology to replace traditional keys since 1997. In 2005, researchers developed a finger-vein authentication technology that allowed a door to be opened simply by gripping the handle.

The company is planning on using the same kind of technology for building access, PC log-in and automated teller machine authorization.

IT Managers Claim End Users Are More Stressful Than Hackers – Oct. 29/07

IT managers are more concerned about end-user abuse of IT systems than attacks from hackers and other threats, according to new research.

The 2007 State of Security Report, sponsored by security vendor Websense Inc., surveyed 158 employees and 159 IT managers from Australian companies with more than 50 staff.

Managing end-user online activity is the most frustrating part of the IT manager role, according to the survey, which found 59 percent of surveyed companies do not block peer-to-peer file sharing, while 47 percent do not enforce Internet usage policies through filtering applications.

Budget constraints were the second highest concern reported by 48 percent of IT managers, followed by lax attention to security (25 percent) and ease of deployment (18 percent).

Most organizations (87 percent) deployed multiple URL filters, with phishing scams listed as the biggest threat (58 percent), followed by spyware (56 percent) and instant messaging (51 percent).

Lost banking details (30 percent) and credit card numbers (20 percent) are considered worse than having company data stolen (17 percent), according to end-user responses.

Up to 117 (74 percent) of the non-IT staff surveyed thought they could be sacked for leaking secret company documents or viewing pornography, while 100 (63 percent) considered introducing spyware and viruses a dismissible offense.

IT managers were slightly more relaxed, according to the survey. Employees would be axed if they leaked sensitive documents according to 90 (56 percent) IT managers, letting viruses loose on company networks (52 percent), and downing pornography (34 percent).

IT managers and employees clashed over the time end-users wasted browsing the Internet for personal use. IT staff claimed non-IT users spend 1.5 hours per day visiting banking sites (46 percent), reading news (39 percent), accessing personal e-mail accounts (29 percent) and visiting jobs sites (18 percent).

However users argued the figure is closer to 45 minutes per day, and they spend about 85 minutes surfing the Web as part of their job.

Queensland end users may be Australia's most ardent workers, according to responses which showed they splurge 30 minutes of paid time per day browsing the Internet for personal reasons, compared to the equivalent New South Wales figure of 53 minutes.

However the figure falls short by more than an hour, according to their IT managers who estimated they waste more than 95 minutes a day on the Web.

More than a third (37 percent) of employees do not make up for time wasted on the Internet, while 28 percent work 15 minutes longer, and 17 percent put in an extra 30 minutes.

By Darren Pauli, Computerworld Australia

Internet Researchers Discover New Hacking Service Site

Internet security researchers are warning about a new malware service, apparently based in Eastern Europe, which pursues a business model charging a fee for each PC infected.

By [Scott Berinato](#) **October 29, 2007** —Security researchers studying the latest Internet crime trends have discovered a new Eastern European website that uses a large botnet to infect vulnerable PCs. The operators of the botnet and website charge clients for each successful PC infection.

The site is likely based out of Russia, according to the security researcher's sources who asked to remain anonymous because of their underground intelligence work. While the front-end website, called loads.cc, doesn't appear to contain or deliver malware, readers are strongly urged to avoid visiting the site in case malware is present and because the site likely logs the IP addresses of its visitors. (The ".cc" Internet domain is assigned to the Australian territories of the Cocos and Keeling Islands.)

The sources discovered the site while performing forensics on some servers known to host malware. They say that, when last checked, loads.cc was still in operation.

This service is another example of a service-based hacking product, similar to others recently reported here, that opens up Internet crime to less technically proficient criminals. Rather than compete with some of the other services, it actually complements them.

Whoever is running loads.cc controls a botnet that may include up to several million PCs in its network, according to the sources. The operator of the site provides real-time information on the size and availability of the botnet. The site operator charges clients for using the botnet to infect computers with whatever malware the customer chooses. The going rate at the time of its discovery was about 20 cents per "load," or per successful injection into a vulnerable PC.

A client can ask in advance for a certain number of infections, say 1,000 infections for a \$200 fee. Customers can also pay for loads based on country, IP addresses or other attributes. Once the job is done, the client receives a report—essentially an itemized bill—of the IP addresses where loads were successful. Then the perpetrators can pursue their goals: For example, they could potentially distribute spam, grab PC owners' online banking information, or steal log-in credentials.

This is slightly different than the service model used by the criminal hackers behind the Gozi trojan and 76service, as reported in a [special report](#). With 76service, clients paid for access to a form-grabber that had already infected the machine. This made each infection more expensive, since access was mostly exclusive and the trojan was already installed and operating on behalf of the buyer. With loads.cc, the client is paying to infect the machine in the first place, with whatever malware the buyer chooses. (The Gozi trojan resurfaced this week being distributed via [PDF spam](#).)

The business model behind loads.cc creates several concerns. The botnet is available to anyone, and loads cost only 20 cents each. This could lead to a set of "super-infected" PCs that have several—possibly dozens—of bots loaded onto them. That, in turn, could lead to a proliferation of malware—so much that it could make infected PCs virtual battlegrounds for control over that machine.

The sources also worry about similar services creating a hyper-botnet in which the current botnet is used to load executable files that spread bots to other PCs, which in turn do the same, creating a viral effect.

"Homeland Security Retreats From Facets of 'Read ID'"

Washington Post (11/05/07) P. A7 ; Hsu, Spencer S.

The Department of Homeland Security announced that it will extend compliance deadlines and ease some security measures for the national Real ID system. After Congress passed legislation in 2005 mandating the creation of a Real ID program to standardize licenses and make it more difficult to forge identification, Homeland Security established a deadline of May 2008. That deadline has already been pushed back once, to 2013, and may be moved again, to 2018, for drivers older than 40 or 50. The delays come in response to complaints from state officials, who say the plan is too costly to implement. Homeland Security has also backed down on several of its demands, including the expensive material that the IDs were to be printed on and the five-year expiration date. Experts say the new deadline and looser security measures illustrate the difficulty that Homeland Security is having with the Real ID program. Eight states have already passed laws that will allow them to opt out of the program, while nine others formally oppose the program. The Real ID program "was flawed in principle from the beginning," says the American Civil Liberties Union's Timothy Sparapani. However, advocates note that almost all of the 9/11 hijackers were able to obtain IDs that let them travel throughout the United States.

"Online Searches May Pose Security Threats"

Washington Technology (11/02/07) ; Lipowicz, Alice

Federal agencies could be placing their organizations at the forefront of major security threats just from searching the Internet, warns a Civitas Group report. Civitas assessed Google Desktop Search and Search Across Computers for their internal network and Web searching capabilities. Researchers noted that while the applications were efficient, the risk for third-party interception was prevalent. For example, Search Across Computers automatically uploaded information from online to the desktop, posing the possibility for unauthorized access. Such actions also leave government agencies susceptible to potential liabilities due to classified information disclosures. The Ponemon Institute's survey of federal IT leaders found that over 60 percent were cognizant of Google Desktop Search's potential security risks. Though Google has implemented controls to abate the risks associated with third-party access, Civitas says that more competent training and operational measures are necessary to prevent system vulnerabilities.

"The Hidden Risk of File-Sharing"

Wall Street Journal (11/07/07) P. D1 ; De Avila, Joseph

File-sharing services such as LimeWire, Kazaa, and BearShare can be an avenue identity thieves can use to steal personal information stored on computers. Users of these file-sharing services often create a folder for the files they will be downloading within their computer's "My Documents" folder, which is where many people also store sensitive documents such as tax returns. Depending on how the user set up the file-sharing program, all of the files in the "My Documents" folder and all of its subfolders are available to others on the peer-to-peer (P2P) network the file-sharing service uses. As a result, identity thieves using a file-sharing application can type in "tax return," for example, to find and download a copy of files with that name off of other users' computers. And if the user has installed a file-sharing application on a company laptop, or has access to company files on a home computer with a file-sharing application, these files can get leaked as well--even from the corporate server. To combat this problem, the Distributed Computer Industry Association is developing a new set of best practices for the file-sharing industry. One of those best practices calls on DCIA members to rework their programs' warnings to make it clearer when users are sharing files that they might not intend to.

"A Global Index to Track Security Fears"

Access Control & Security Systems (10/30/07)

Unisys has initiated a three-part annual survey that will poll consumers internationally about their stance on security issues. For the first survey, Unisys polled consumers in 14 different countries, asking for their views about national, financial, personal, and IT security. The survey revealed that consumers in Hong Kong, Brazil, Singapore, and Malaysia ranked bank card fraud as their top security concern. The survey noted that financial security was a chief concern for all consumers polled, while those in Brazil and Germany were most worried about online data breaches. Those in France and Italy were least concerned with respect to general security issues, while concerns about misappropriation of data were prime concerns for consumers in the United States, Malaysia, and Brazil, among others. The survey found that all consumers, regardless of country, were more troubled by having a virus infect their computers than personal data breaches.

"One in Six PCs Could Be Infected With Malware"

Network World (11/02/07) ; Garretson, Cara

Possibly as many as one in six PCs may have active malware or spyware infections, reveals a Prevx study. Prevx analyzed 300,000 PCs and found that more than 15 percent had at least one active spyware or malware program, including keyloggers and data stealers. The company notes that up to 10,000 malware threats occur daily. The report found that PCs with no installed security software had a 60 percent higher infection rate than those containing antivirus or anti-malware programs.

"No Such Thing as Security 'Best Practices'"

Baseline (10/29/07) ; Violino, Bob

The biggest threat to corporate information and computing centers is the abuse of authorized access to information by employees, customers, business partners, or outsourcing partners, not the unauthorized access to information, according to International Information Integrity Institute (I-4) managing director Linda Stutsman. She notes that while the abuse of authorized access to information is nothing new, there are new ways in which the authorized access of information is being abused. "I've been in this business for a very long time, and 25 years ago we didn't have to worry about employees taking pictures of customer information with their cell phones," Stutsman says. "We didn't have to worry about employees with USB drives on their key chains." Stutsman says organizations can use several tactics to prevent the abuse of authorized access to information, including more carefully limiting the scope of authorized users on the policy implementation side, and on the technology and process side by restricting methods of access via thin clients. She adds that organizations should not get caught up in trying to follow security best practices, since such a thing does not exist. "I don't believe in best practices," Stutsman says. "What is a best practice for one organization may not be a best practice for another." She says information managers should see what others have done and apply what works to their situation. "I believe each company has to take the best of each solution and customize it," Stutsman says.

Survey: With data breaches, less is more (dangerous)

Study finds bigger losses pose less identity-theft risk than smaller ones

Jaikumar Vijayan

November 08, 2007 ([Computerworld](#)) -- When it comes to security incidents involving the compromise of identity data, big breaches may actually be better than smaller ones -- at least from a consumer standpoint.

That's one of the conclusions of a report released this week by [San Diego, Calif.](#)-based risk management firm [ID Analytics Inc.](#) Researchers studied the fallout from 12 security breaches involving the loss of Social Security numbers and other personally identifiable data. In all, the fate of over 10 million records containing identity data was analyzed.

Out of the breaches studied, the research found that the highest rate of organized misuse of data occurred with the smaller breaches. On average, about one in 200 identities were misused in breaches involving 5,000 identities or less. In comparison, the misuse rate was less than 1 in 10,000 for security incidents involving 100,000 or more individuals.

What that means is that a consumer whose identity was exposed in a massive data breach is likely to be less at risk than someone who lost theirs in a small breach, said [Thomas Oscherwitz](#), chief privacy officer at ID Analytics.

Black market not such a lure

"My assessment is that one of the constraints on committing identity fraud is the resources that are available," to the perpetrators for carrying out such fraud, Oscherwitz said. Even in cases where large data files are compromised, he explained, ID thieves rarely have the resources, the time, or the knowledge needed to misuse more than just a fraction of the data they acquire.

The study also found no evidence to suggest that those who had the breached data were broadly disseminating it into the Internet black market, Oscherwitz said -- indicating that the extent to which stolen data is being made available to criminal elements is probably less widespread than most assume.

In most cases, the stolen identity data tended to be used by small clusters of people who used it to apply for new credit cards Oscherwitz said.

For instance, in two of the five instances where data was misused, the fraudsters used one phone to impersonate dozens of real identities when making credit card applications. The addresses used by fraudsters when making such applications also tended to be clustered into small geographic areas, he said.

Interestingly, the abuse of a single compromised identity tended not to last more than two weeks, Oscherwitz said. A fraudster might use a compromised identity to make multiple fraudulent credit cards applications for instance, but after about two weeks he would stop using that identity and move on to another one. The practice appears to be motivated by fears of being detected and by the abundance of compromised identities available.

Don't panic?

An understanding of such distinctions can help inform the debate surrounding data breach disclosures and a companies' responses to it, Oscherwitz said.

"Not all data breaches are the same. There is no one-to-one correspondence between a breach and the harm that results from it," he said. "We feel it's important to focus on the real risks out there" and not treat every breach the same way.

The findings of the ID Analytics study are similar to those contained in a June 2007 report released by the [Government Accountability Office \(PDF format\)](#). The GAO report stated that the extent to which data breaches result in identity theft is hard to determine because of the difficulty of pinning down the source of data used to commit ID fraud.

However, available evidence suggests that despite the number of reported breaches, most breaches do *not* result in identity theft. A GAO review of the 24 largest breaches reported in the media between January 2000 and June 2005 showed that fraud occurred as a result of the breach in only four incidents.

"Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges," that report said. "An expansive requirement could result in [reporting] breaches that present little or no risk, perhaps leading consumers to disregard notices altogether."

Visa's security best practices to become payment industry standard

Aggressively touted guidelines are apparently everywhere you want to be

Jaikumar Vijayan

November 08, 2007 ([Computerworld](#)) -- The PCI Security Standards Council, the body managing the Payment Card Industry data security initiative, on Wednesday announced that it will anoint a set of best practices developed by Visa Inc. as the new security standard for third-party application software in the payment industry.

The new standard is called the Payment Application Data Security Standard (PA-DSS) and is based on Visa's Payment Application Best Practices (PABP).

Over the next few months, the PCI Security Standards Council, together with participating organizations, security auditors, and vulnerability scanning vendors, will offer comments and suggestions relating to the PA-DSS.

The security council will then incorporate this feedback and publish a final version of the application security standards in the first quarter of 2008, said Bob Russo, general manager of the security standards council.

The application security standards are designed to address growing security concerns related to the third-party payment applications used by retailers and other companies accepting credit card transactions. Many of these applications are old and lack many of the security controls mandated by the credit card companies under the PCI data security standard.

For instance, older payment application software products are designed to capture and store certain kinds of cardholder data by default, even though the practice is explicitly banned under PCI guidelines. Similarly, older payment applications seldom have the transaction-logging capabilities that are required by PCI.

Visa, which has been by far the most aggressive of the credit card associations in pushing PCI, has for some time now tried to address such issues by leaning on software vendors to adopt its set of payment application best practices. Though Visa cannot contractually require the software vendors to adopt these best practices, it has been pressuring them into doing so anyway, by making it mandatory for merchants to use only PABP-compliant third-party payment software.

Just two weeks ago, for instance, it [announced](#) formal schedules for companies to ensure that all of their third-party payment applications are PABP-compliant.

With the moved announced yesterday, the PCI council has taken Visa's requirements and forged them into a broader industrywide mandate -- meaning that soon it won't be just Visa that's pressuring payment software vendors to adopt security controls, but MasterCard Inc., Discover Financial Services, American Express Co. and JCB International Credit Card Co. as well.

Survey finds companies clueless about unsecured data costs

A certain amount of ostrich-style thinking observed among respondents

Elana Varon

November 07, 2007 ([CIO](#)) -- When it comes to securing corporate information, many companies are clueless about which content needs protection, and most don't have a handle on the potential costs of not protecting it, according to a survey by AIIM-The ECM Association.

Asked what primarily drives their content security initiatives, survey respondents cited general risk avoidance as the top motivator, followed by regulatory compliance, corporate policies, e-discovery and litigation concerns. But when asked what percentage of their organization's content requires specific controls to ensure their validity and security, 28 percent said they didn't know.

More than 40 percent of respondents said that they had no idea whether any content had been inappropriately accessed within the past two years. And 41 percent said they did not know whether any content had been inappropriately updated or deleted.

"There's almost this reluctance to spend much time and money on [content security] because there's a naive hope that if we never get caught we don't have to worry about it," says Carl Frappaolo, vice president of AIIM Market Intelligence and an author of the report.

AIIM is a professional association that provides market research and education about enterprise content management technologies and practices. Survey respondents included both association members and the general public. The questionnaire, administered online, was designed to provide a general snapshot of corporate knowledge and attitudes about content security issues.

Respondents also reported that making a business case for content security projects is challenging. Though few said they required a formal ROI study to implement content security initiatives, 75 percent of those who did project an ROI did not achieve an acceptable return.

Frappaolo says that's because most companies have a hard time calculating their risks. An exception, he says, is a financial services company with which he worked. "One day an executive happened to notice there was an expense exceeding a million a year for temp services. [The company] was hiring temps to help with e-discovery," Frappaolo recalls. "That's when they decided they could cost-justify bringing in some software. Not everyone is that fortunate to see something like that."

