

Security Trends Report

06/08

Security pros focused on internal threat, training

By Marcia Savage, *Information Security* magazine
05 May 2008

Organizations are shifting their focus to the threat posed by insiders and turning their attention to training and data protection, according to a recently released survey of information security professionals.

The 2008 [Global Information Security Workforce Study](#), conducted by analyst firm Frost and Sullivan for certification organization (ISC)2, surveyed 7,548 information security pros worldwide.

Fifty-one percent of the respondents said internal employees pose the biggest threat to their organizations. The finding represents an ongoing trend in the past two to three years, as the numbers of remote workers and portable storage devices have jumped in the enterprise, said Rob Ayoub, Frost & Sullivan network security industry manager.

"That increases the chance of something happening, whether it's malicious employees or just someone with good intentions but walks out of the building with data so they can work at home," he said.

The survey's findings are supported by [Information Security's Priorities 2008 survey](#), in which 70% of participants said they're worried about [detecting and thwarting internal attacks](#).

Along with the focus on internal threats, respondents in the (ISC)2 survey view security awareness as critical for effective security management. Forty-eight percent said users following information security policy was the top factor in their ability to protect an organization.

More and more, security teams are being tasked with running [security awareness training](#) for end users, from safe password practices to corporate policies, Ayoub said. "Industry-wide, security awareness training is becoming more important," he said.

Regulatory requirements and a stream of data breaches are leading more businesses to place more emphasis on security awareness, Winn Schwartau, founder of SCIPP International, a nonprofit provider of end-user security awareness training and certification, said in an interview in March. Still, some companies rely on technology to address behavioral problems while others do just the bare minimum when it comes to training their rank and file about security, he said.

"In the cyber world, we've been very neglectful about teaching people when something is not right," he said, adding that security awareness is critical for reducing risk in an organization.

(ISC)2's survey also indicated a growing need for professional training in certain security domains, with participants ranking security administration and secure application development as the top areas they want to increase their skills.

Security professionals also are optimistic that their organizations will increase spending for training this year. Nearly 60% of respondents in the Americas and Asia-Pacific reported that they expect training and education to increase in 2008.

"The upper levels of management are realizing they can't expect a security professional to do their job properly without continued training," Ayoub said. "As a result, folks are seeing more money going into the training while in

other areas, we might see training cutbacks. Security is one area where respondents are reporting healthy increases."

The survey also found that, as an increasingly mobile workforce punches holes in the traditional network perimeter, companies are becoming more focused on data protection. Wireless security, cryptography, storage security and biometrics were the top five technologies that respondents said their organizations were planning to deploy. Ayoub said companies are implementing more security measures for their wireless networks because they "are a real path to the data."

The interest in [biometrics](#), researchers said, shows the continued need for organizations to improve access controls to protect sensitive data.

Information Security's Priorities 2008 survey also showed heightened interest in protecting sensitive and confidential data. About 68% of readers surveyed said they will be spending more time on data protection this year. Some 66% said database security is important while 58% viewed creation of a data deletion and retention process as vital.

Despite a slow economy, Frost & Sullivan estimates the number of information security professionals to increase to almost 2.7 million by 2012, up from approximately 1.66 million today.

Report says C-level execs more involved with security

[Jim Carr](#)

May 09, 2008

The major data breaches that have received mass media coverage are driving so-called "C-level" executives to become actively involved in their organization's security policies, according to a new report from the (ISC)2.

There are several key "take-aways" from the report, titled "[2008 \(ISC\)2 Global Information Security Workforce](#)" and authored by Rob Ayoub, Frost & Sullivan's network security industry manager.

Ayoub told SCMagazineUS.com that these include the fact that C-level executives are paying attention to security, the overall optimism of security professionals is increasing and organizations are focusing more on business continuity and disaster recovery.

"CEOs are asking their security professionals important questions about how they're prepared to not become another [TJX](#)," Ayoub explained. "We've heard a lot in the past about upper management taking a role in security; this time it is validated."

Nearly three-quarters (73 percent) of the survey of 7,548 security professionals reported that they're concerned about the impact of service downtime and damage to the organization's reputation.

"Public reputation was very important, and these are issues we haven't seen concern in before," Ayoub said.

"The study confirms for me that security is becoming a broader issue and is moving up the stack into the priorities of business folks as well," Howard A. Schmidt, the ISC2's security strategist, told SCMagazineUS.com. "Executives are seeing that breaches can have far-reaching consequences throughout their business, impacting corporate reputation, the privacy of customer data, identity theft and of course legal and regulatory compliance."

In addition, 70 percent said customer issues related to privacy violations were high priority, as were customer identity theft issues (67 percent). Other top-of-mind issues included concern about viruses and worms and insider threats.

The top five new security technologies enterprises are deploying now are biometrics, wireless, disaster recovery, intrusion prevention and cryptography, the report indicated. Ayoub said he was surprised that disaster recovery climbed into the "top five" realm this year.

Disaster recovery has become a key issue "because companies rely so heavily on the internet for employee communications and to react with customers," Ayoub said. "They realize they need to have a solid disaster-recovery plan."

"Public incidents are driving an awareness in disaster-recovery technologies," he added. "Company executives are seeing events on the news and want to know how they're prepared to deal with a fire or a hurricane."

Ayoub also said the report indicated companies planned to spend more money on security training, and that security professionals are "optimistic" about their job.

All this points to the conclusion that more C-level executives are "showing actual concern about what their security professionals are doing and not just paying lip service," Ayoub said.

Non-tech criminals can now 'rent a botnet'

Everybody wants to get in on the act

By Andrew Hendry

• May 15, 2008 (Computerworld Australia) Online fraudsters that aren't highly skilled in the art of cybercrime can now rent a service that offers an all-in-one hosting server with a built-in Zeus Trojan administration panel and infecting tools, allowing them to create their own botnets.

EMC Corp.'s security division, the RSA Anti-Fraud Command Center (AFCC), cited an increase in the use of the Zeus Trojan in attacks against financial institutions in its April online fraud report, claiming the Trojan is "extremely user-friendly and easy to operate."

"Fraudsters who execute Zeus attacks simply need to take control of a compromised server or have their own back-end servers; once they have a server in place, they merely need to install the Zeus administration panel, create a username and password, and start launching their attacks," the report stated.

But the AFCC recently traced a new service that does all of the above for would-be botnet barons. The service offers access to a "bullet-proof hosting server with a built-in Zeus trojan administration panel and infection tools. ... The service includes all of the required stages in a single package, meaning that all the fraudster now has to do is pay for the service, access the newly-hired Zeus trojan server, create infection points and start collecting data."

RSA's banking and finance specialist, Geoff Noble, said that those offering the Zeus package are mirroring what legitimate security vendors are offering — security as a service — but in their case, they are slinging malware as a service.

"Phase 1 of online threats was stealing credit card numbers, buying stuff on the Internet and selling it somewhere else to make a profit. Phase 2 is this grabbing of usernames and passwords online. Phase 2b is productizing that solution, and Phase 2c is offering that solution as a service," Noble said.

"What Zeus means is that you are buying a service with traditional software support and maintenance, so you can go about your business without updating and patching," he said.

RSA said that the exploit package allows fraudsters to easily infect users and grow a botnet of compromised machines, and boasts an easy-to-use Web-hosting control panel that can be used by virtually anyone.

"The bottom line is that with such services, creating the infrastructure for Zeus attacks and actually implementing these attacks is now easier than ever before," the report said.

"It makes it markedly easier because you don't need to bring together the three components. The challenge still remains how to get the cash out — and that will likely be the constriction point getting in the [fraudsters'] way," Noble said. "It will be a lot easier to do on the attack front, but the cash still needs to come out of the channel."

Victims receiving e-mails at home or work offering amazing deals to become the local financial outpost for a multinational company is just one of the ways the fraudsters are getting the cash out.

"People still get sucked into that, and that's one of the variants of getting the cash out. The fact that it's too good to be true doesn't always sink into everyone, and people still become mules," Noble said. "And we're seeing a lot more specific approaches to people to become mules in tandem with the ease of use for non-tech spooks and fraudsters."

The Zeus Trojan is designed to perform advanced keylogging when infected users access specific Web pages. The information it collects is encrypted when it is sent to the collection point and can be communicated over SSL encryption.

The monthly AFCC report found that U.S. banks continued to be the dominant target of cybercriminals, with 62% of attacks, followed by the U.K. with 11%. Australia and New Zealand made it into the list for the second month in a row as phishing in the Asia-Pacific region continues to grow.

The U.S. also topped the AFCC's April list of top hosting countries, with 51% of phishing attacks originating from there — a 12% decrease from the previous month. China came in second with 19% of attacks, while Australia was responsible for 2% of threats.

Phishing botnet expands by hacking legit sites

Plants SQL injection attack tool on bots, hacks business, education sites

By Gregg Keizer

- May 14, 2008 (Computerworld) A botnet is now using a SQL injection attack tool designed to hack legitimate Web sites, a move meant to add more hijacked PCs to its collection, according to a security researcher.

The Asprox botnet, which specializes in sending phishing spam, is pushing an update to the infected PCs it controls, [Joe Stewart](#), the director of malware research at Atlanta-based [SecureWorks Inc.](#), said today. The update is an executable file -- "msscncr32.exe" -- that installs as a Windows service dubbed "Microsoft Security Center Extension."

But the executable actually installs an SQL injection attack tool, said Stewart.

SQL injection attacks have become widespread as criminals increasingly target legitimate Web sites, figure out a way to hack them, then plant iFrames on those sites to redirect users to malicious servers. Those servers silently attack visitors' PCs, often trying multiple exploits, and if one works, they download additional code to the machine to hijack it from its rightful owner and add it to an army of infected systems.

"There are multiple things out there launching similar attacks," said Stewart in explaining why there's confusion about how the tool is being spread. Some analysts have mistakenly concluded that the SQL injection tool is using wormlike tactics, according to Stewart. "The tool does not spread on its own but relies on the Asprox botnet to propagate to new hosts," he said.

It is becoming increasingly difficult to separate the multiple attack vectors that criminals are using to hack legitimate sites, if only because SQL injection attacks have ballooned in scale. Last month, for example, a [massive SQL-injection attack](#) compromised more than a half-million pages, including some on sites run by the [United Nations](#).

After the Asprox botnet seeds its bots with the msscncr32.exe file, the attack tool launches and uses [Google's](#) search engine to find potentially vulnerable pages. It then hits those pages with a SQL-injection attack and, if successful, plants a malicious iFrame on the site.

Visitors are redirected through a series of malware-hosting servers that try one or more exploits to crack the PC. If that works, a Trojan horse is downloaded and installed on the PC, adding it to the Asprox botnet; those compromised PCs are then used to spew more phishing spam.

Stewart has counted 1,000 sites that have been hacked by the SQL injection attack tool since Monday night. The sites include small business sites, domains for several small colleges and universities, and some hosted by law firms. Most are in the U.S.

Other security vendors, including F-Secure Corp. and Symantec Corp., have also uncovered evidence of new waves of SQL-injection attacks. Those firms have been pinning responsibility on Chinese hackers who are compromising legitimate sites to spread malware to steal game passwords.

Separately, the SANS Institute's Internet Storm Center has reported that hackers have [taken to trading](#) various SQL injection attack tools.

Meanwhile, IBM's X-Force, the research arm of the computer giant's Internet Security Systems Inc. subsidiary, has been rooting in the dark corners of the Web to pin down the number of malware-hosting sites linked to the legitimate URLs hacked by SQL-infection attacks. According to [David Dewey](#), the manager of X-Force, his group regularly identifies 20 to 30 new hosting sites each day.

"Some of these are up less than a day," said Dewey. "In one case, the hosting [server] was offline in less than 30 minutes." The majority of the sites X-Force finds appear to be designed as malware hosts, rather than unwitting accomplices.

"SQL injection attacks are rampant," Dewey said. "This latest peak isn't any larger than the previous, but they are very large attacks."

I spy your PC: Researchers find new ways to steal data

By Robert McMillan

- May 19, 2008 (IDG News Service) Researchers have developed two new techniques for stealing data from computers that use some unlikely hacking tools: cameras and telescopes.

In two separate pieces of research, teams at the University of California, Santa Barbara, and [Saarland University](#) in Saarbrücken, Germany, describe attacks that seem ripped from the pages of spy novels. In Saarbrücken, the researchers have read computer screens from their tiny reflections on everyday objects such as glasses, teapots and even the human eye. The Santa Barbara team has worked out a way to analyze a video of hands typing on a keyboard in order to guess what was being written.

Computer security research tends to focus on the software and hardware inside the PC, but this kind of "side-channel" research, which dates back at least 45 years, looks at the physical environment. Side-channel work in the U.S. was kicked off in 1962 when the [National Security Agency](#) discovered strange surveillance equipment in the concrete ceiling of a [U.S. Department of State](#) communications room in Japan and began studying how radiation emitted by communication components could be intercepted.

Much of this work has been top secret, such as the NSA's Tempest program. But side-channel hacking has been in the public eye too.

In fact, if you've seen the movie *Sneakers*, then the University of California's work will have a familiar ring. That's because a minor plot point in this 1992 [Robert Redford](#) film about a group of security geeks was the inspiration for their work.

In the movie, Redford's character, Marty Bishop, tries to steal a password by watching video of his victim, mathematician Gunter Janek, as he enters his password into a computer. "Oh, this is good," Redford says, "He's going to type in his password, and we're going to get a clear shot"

Redford's character never does get his password, but the UC researchers' Clear Shot tool may give others a fighting chance, according to [Marco Cova](#), a graduate student at the school.

Clear Shot can analyze video of hand movements on a computer keyboard and transcribe them into text. It's far from perfect -- Cova says the software is accurate about 40% of the time -- but it's good enough for someone to get the gist of what was being typed.

The software also suggests alternative words that may have been typed, and more often than not, the real word is in the top five suggestions provided by Clear Shot, Cova said.

Clear Shot works with an everyday webcam, but the Saarland University team has taken thing up a notch, training telescopes on a variety of targets that just might happen to catch a computer monitor's reflection: teapots, glasses, bottles, spoons and even the human eye.

The researchers came up with this idea during a lunchtime walk about nine months ago, said Michael Backes, a professor at Saarland's computer science department. Noticing that there were a lot of computers to be seen in campus windows, the researchers got to thinking. "It started as a fun project," he said. "We thought it would be kind of cute if we could look at what these people are working on."

It turned out that they could get some amazingly clear pictures. All it took was a \$500 telescope trained on a reflective object in front of the monitor. For example, a teapot yielded readable images of 12-point Word documents from a distance of 5 meters (16 feet). From 10 meters, the researchers were able to read 18-point fonts. With a \$27,500 Dobson telescope, they could get the same quality of images at 30 meters.

Backes said he has already demonstrated his work for a government agency, one that he declined to name. "It was convincing to these people," he said.

That's because even though the reflections are tiny, the images are much clearer than people expect. Often, first-time viewers think they're looking at the computer screen itself rather than a reflection, Backes said.

One of his favorite targets is a round teapot. Looking at a spoon or a pair of glasses, you might not get a good view of the monitor, but a spherical teapot makes a perfect target. "If you place a sphere close by, you will always see the monitor," he said. "This helps; you don't have to be lucky."

The Saarland researchers are now working out new image-analysis algorithms and training astronomical cameras on their subjects in hopes of getting better images from even more difficult surfaces such as the human eye. They've even aimed their telescopes and cameras at a white wall and have picked up readable reflections from a monitor 2 meters from the wall.

Does Backes think that we should really be concerned about this kind of high-tech snooping? Maybe, just because it's so cheap and easy to do. He said he could see some people shelling out the \$500 for a telescope just to try it out on their neighbors.

So how to protect yourself from the telescopic snooper? Easy. "Closing your curtains is maybe the best thing you can do," he said.

Few expected to make June 30 PCI deadline for Web application security

Many firms just now shaking off the mental cobwebs

By Jaikumar Vijayan

May 12, 2008 (Computerworld) Retailers covered by the Payment Card Industry Data Security Standard (PCI-DSS) have just about a month and a half left to comply with new requirements for protecting Web applications. But as with previous PCI-related deadlines, this one appears destined to pass with a majority of merchants unlikely to be in full compliance.

After June 30, all merchants accepting payment card transactions will be expected to either use a specialized firewall for protecting their Web applications or to have completed a Web application software code review for

finding and fixing vulnerabilities in these applications. Companies that fail to implement either measure will be deemed to be out of compliance with PCI starting June 30.

"Most of our clients are not going to be ready," by that deadline, said [Avivah Litan](#), an analyst at Stamford, Conn.-based [Gartner Inc.](#) "We are amazed at how many companies are still only learning their way around the requirements" and what they call for, Litan said.

With the deadline fast approaching, though, Gartner has seen an uptick in the number of calls it is receiving from clients wanting to know more about the new controls and how to implement them, she added.

Section 6.6 of the new PCI requirements ([download PDF](#)) basically requires merchants to ensure that all Web-facing applications are protected against known attacks by applying either an application firewall or by completing an application code review -- either manually or by using application-scanning tools. The requirements have been recommended best practice for more than 18 months but are now becoming a formal mandate.

According to Litan, many of Gartner's clients are choosing to deploy Web application firewalls instead of going the code review route. "They are looking for quick fixes. Application firewalls are quick fixes" compared to finding and fixing flaws in application software, she said. However, such firewalls alone are not enough in the long run, she added: "Application firewalls are a reactive measure. You have a lot of vulnerable applications that still need to be fixed." As a result, companies that want to really secure their Web application environments will need to think beyond PCI compliance. Scanning for and fixing vulnerabilities in Web applications "should be given priority over the use of Web application firewalls, which should be used in addition to, not instead of," code reviews, she said.

Under 6.6, companies that choose to implement application firewalls need to ensure that the technology is deployed in full blocking mode, said [Jeremiah Grossman](#), chief technology officer and founder of WhiteHat Security Inc. Doing that effectively requires merchants to invest a substantial amount of time tweaking their firewalls to ensure that only malicious content is blocked, while letting legitimate traffic in. There is a learning process involved in doing this that can take anywhere from three to six months -- which, he noted, many companies may not be aware of or budgeting for.

There may be a similar disconnect over what the code-review component really means, [Grossman](#) said. Companies that choose to do a code review will need to make sure that they are not just identifying the vulnerabilities in their software but are actually going out and fixing them, which can be a time-consuming process, he said. There is also still some confusion over who exactly is qualified to be doing such reviews, Grossman said. Right now, PCI rules allow for either manual or automated code reviews performed by qualified third parties or by qualified internal resources. The problem is that without any formal certifications or other measures available currently, it's hard to say who exactly might be qualified to assess the security of Web applications internally, he said.

Whichever route a company might choose, Grossman noted, what's important to note is that neither firewalls nor code reviews by themselves are enough. "Vulnerability assessment, should always been seen as complementary to Web application firewalls," he said. "Vulnerability assessments overall are a measurement, while Web application firewalls are defensive technology. ... In the next two to three years, Web application security [assessments] and firewalls will be ubiquitous. The question is which will companies tend to adopt first."

In response to a request for comment, a spokesman for the [PCI Security Standards Council](#), which administers the standard, pointed to a recently issued update ([download PDF](#)) aimed at clarifying what exactly the code review and firewall requirements are.

"Most of the feedback we have heard is from merchants who have waited to implement a solution until now or procrastinated on implementation. We haven't heard anyone say this is something we ought not to be requiring," the spokesman said in an e-mailed statement.

The new PCI deadline looms even as some have begun questioning the effectiveness of the standard in helping companies to better secure payment card data. The questions first surfaced after supermarket chain Hannaford

Bros. Co. revealed in March that it had been breached even though it had been PCI compliant at the time of the breach. Since then, analysts and others close to the effort have begun to publicly air doubts about whether the standard needs to be tweaked to ensure better payment card security.

In a recent [interview](#) with *Computerworld*, [Bob Russo](#), general manager of the security council, downplayed such concerns and noted that the standard is solid despite those doubts. He added that the body is waiting to get details on the Hannaford breach to know if changes to the standard need to be made. He also pointed out that a new version of the standard will be released later this year aimed at addressing new and emerging threats to cardholder data.

New attack trend pushes POS encryption to the fore

Vendors offer new tools to try to help retailers stop data-in-transit thefts

By Jaikumar Vijayan

May 20, 2008 (*Computerworld*) The relatively scant attention that retailers have paid to securing their point-of-sale systems over the past few years is making the POS setups increasingly [attractive targets](#) for cybercrooks who are looking to steal payment card data.

Hoping to help merchants address that situation are a handful of vendors who have begun offering new products aimed at making POS environments a lot harder to crack.

The biggest of those vendors is VeriFone Holdings Inc., which last month [released](#) a security tool designed to let merchants encrypt credit and debit card data from the moment a card is swiped at a merchant's PIN entry device all the way to the systems of the company's external payment processor.

VeriFone's VeriShield Protect software is based on patented technology from Semtek Innovative Solutions Corp., which makes appliances for securely decrypting data. VeriFone said that Semtek's technology, called the Hidden Triple Data Encryption Standard, can be used to encrypt personal account numbers and the so-called Track 2 data stored on the magnetic stripe located on the back of payment cards. That information includes card numbers and their expiration dates.

A key feature in VeriShield Protect is that it encrypts payment card data in such a way that the information will still be recognizable as valid card data by other POS applications, said Jeff Wakefield, vice president of marketing at VeriFone. As a result, merchants won't need to tweak or modify their POS systems in any way to accommodate the encryption technology, he claimed. But at the same time, encrypting the card data will render it totally useless to anyone who steals the information, Wakefield said.

A separate device — which could be installed by either a retailer or its payment processor — then would be used to decrypt the data before transactions are processed.

Merchants using newer models of VeriFone's PIN entry devices can have the encryption function "injected" into them for less than \$50 per device in license and service fees, Wakefield said. He added that the vendor doesn't have a published list price for new PIN devices that support the technology, because per-device prices can vary depending on the individual installation.

Meanwhile, the decryption appliances, which are made by Semtek and sold by VeriFone, can cost from \$50,000 to upward of a million dollars for high-throughput, fully redundant systems. Larger retailers that want to exercise direct control over all aspects of their payment card transaction process might invest in such systems themselves, Wakefield said. But, he added, most small and midsize merchants will likely look to their payment processors to handle the decryption component.

Another company targeting the POS security market is Merchant Warehouse, a credit card processing firm that provides services to about 50,000 retailers, most of them small or midsize. The company offers a product called

[MerchantWare](#), which like VeriFone's technology is designed to enable merchants to encrypt card data from the beginning to the end of the sales and payment process.

Although VeriShield Protect is focused on the PIN pad devices that are used by customers themselves to swipe their cards, Merchant Warehouse CEO Henry Helgson said that MerchantWare is aimed more at POS systems in which cards need to be handed over to a cashier.

MerchantWare is based on technology from MagTek Inc., a rival of Semtek. Like VeriShield Protect, MagTek's product also encrypts data at the card reader. But integrating the technology into existing environments does require "minimal" updates to a company's POS software, Helgson said.

With MerchantWare, merchants never have to store any payment card data on their systems, according to Helgson. Instead, a retailer that needs to access payment transaction data to handle issues such as chargebacks or payment disputes would log into a MerchantWare payment gateway to get at the information.

Helgson said that the recent disclosures of several [data-in-transit thefts](#) are helping to generate interest in technologies such as MerchantWare. "This is our way of getting new customers," he said. "We expect huge demand for this.

Also offering capabilities similar to MerchantWare is payment processor Element Payment Service Inc., which is using MagTek's technology to provide bundled encryption services to retailers, said [Gartner Inc.](#) analyst [Avivah Litan](#). It's surprising, she added, that more vendors haven't already come out with similar products that can help retailers encrypt payment card data while it is inside their networks.

Currently, under the Payment Card Industry Data Security Standard mandated by the major credit card companies, merchants are required only to ensure that any payment card data being transmitted over a public network is encrypted. The lack of a rule requiring that data be encrypted while it is transmitted internally has been exploited in at least three major data breaches disclosed in the past few months.

The biggest of the breaches took place at [Hannaford Bros. Co.](#), a supermarket chain based in Scarborough, Maine. In March, Hannaford said that malware [planted on the POS servers](#) at nearly 300 grocery stores had been used to steal unencrypted payment card data on more than 4 million customers. Last month, Hannaford officials said that the grocer planned to spend ["millions" of dollars](#) on IT security upgrades in the wake of the breach.

Similar incidents have also been reported by Okemo Mountain Resort, a [ski area](#) in Ludlow, Vt., and by Dallas-based restaurant chain [Dave & Buster's Inc.](#), which said last week that credit and debit card numbers were stolen from 11 of its restaurants during 2007 by hackers who allegedly gained remote access to POS servers and then installed packet-sniffing software on them.

Such breaches highlight the need for companies to pay more attention to encrypting payment card data within their own network boundaries, Litan said. But thus far, she added, adoption of the available encryption technologies has been slow because many retailers appear unconvinced that encryption can be introduced at the POS level without requiring major changes. For instance, one concern is that encrypting data will make it harder for retailers to handle issues such as chargebacks.

"Most merchants are passive about this because their systems rely on card numbers for chargebacks," Litan said. "They need to be convinced that their systems need to change." In addition, many retailers have spent a lot of money, time and effort complying with the existing PCI requirements and are reluctant to implement even more security controls, she said.

Employers loosen rules on camera phones

Too many brands to keep track of, a lower security risk than once perceived, prompt IT managers to relax policies

By Matt Hamblen

May 19, 2008 (Computerworld) Cameras are available on just about every kind of wireless handheld device, from inexpensive cell phones to high-end smart phones, putting pressure on IT managers to reconsider corporate security policies banning cameras.

In 2004, when cameras first became widely available for devices, many companies that purchase devices for their employees dug in their heels and asked their wireless carriers to provide models with no cameras.

Four years later, however, that hard-line approach appears to be softening, at least in the private sector. "Some companies are still avoiding [devices with cameras], but that's a minority," said [Gartner Inc.](#) analyst [Ken Dulaney](#) in a recent interview. Dulaney works with many Fortune 500 companies on their mobile device purchases and policies.

"Many companies have now relaxed their rules, as most are resigned to the notion that virtually all phones include cameras built-in," added [Jack Gold](#), an analyst at J.Gold Associates LLC.

At one large U.S. corporation that provides [BlackBerry](#) wireless devices to 30,000 users, the camera ban was recently lifted for new device purchases. "Even the low-end phones are coming out with [Bluetooth](#) and cameras, so we've ended up adding cameras to the mix of devices allowed," said a senior IT manager at the company who asked not to be named because of corporate policies. However, the IT manager said that when the IT shop can disable the camera via management tools over the network, it will do so.

There are network management tools that curtail camera use. Research In Motion Ltd., maker of the BlackBerry, makes models that enable the IT staff to turn off the camera through the BlackBerry Enterprise Server, so an employee can't surreptitiously photograph proprietary information or inappropriate material. Similar photo-blocking is available with Windows Mobile Exchange synchronization functions, the manager noted.

But the manager said there's no similar way to control photos that are taken on some devices and sent over Bluetooth wireless. Because of such loopholes, there are questions about how any organization can control camera usage. "We want to minimize the potential risk, but there's minimal risk anyway, we've decided," the IT manager added.

Most phones today have cameras built in, and if you search for a good-feature phone, you will likely not be able to find one without the camera."

Jack Gold, analyst, J.Gold Associates

Some models of the latest cell phones and smart phones are available without a camera, to satisfy strict business buyers. Verizon Wireless spokeswoman Brenda Raney said some models are sold that don't have a camera, including the BlackBerry 8830 smart phone, out of an inventory of about 30 models from various manufacturers.

"Some companies don't see the camera as an issue, but some still prefer employees not have them in phones," Raney said. Some industries, and many government agencies, have tougher standards than others, she noted.

Gold, who advises corporations on wireless use, said he used to tell clients to buy phones without cameras to avoid security issues. "However, the truth is, most phones today have cameras built in, and if you search for a good-feature phone, you will likely not be able to find one without the camera," he said. Instead, he urges companies to educate their users about the security risks of cell phone cameras and to consider turning off the cameras over the network.

The anti-camera policies were designed to prevent employees from taking photos of information on computer screens or a company's new internal technology and then using the photos to compromise the company.

But a camera lens can be the size of a pinhole and easily hidden, so it can be extremely difficult for a security guard to detect a camera carried by a visitor, analysts noted. Even proving that a device has its camera turned off would be difficult, since the guard would need to carefully read the device's interface to determine whether a camera was turned off. Security guards sometimes confiscate phones suspected of having cameras, or even resort to putting tape over the lens.

Dulaney said he first wrote about cameras as a security threat in early 2004, after seeing a flood of camera phones at the Consumer Electronics Show. He said then that camera bans were "an overreaction" by business users, since there are many ways consumer devices, such as USB flash drives, can be used to grab information.

Blanket bans on cameras are "a stupid position," Dulaney said recently. "If you are a spy, you won't have a camera that people can see." Four years after writing his initial report, Dulaney said having a camera on a handheld device can actually be valuable for an employee in some situations, such as photographing a crime in an employee parking lot or other location.

Many companies deploy cell phones with cameras that are used for business purposes. Repairmen use them to take photos of defective parts, while real estate agents use them to grab a quick photo of the interior of a home for sale, analysts noted.

Dulaney urged companies to set up secure zones where restrictions on cameras are tightest because of the greatest risks involved. That might mean, for example, that a company would show off its latest product only in a secure zone and would search visitors and confiscate cameras at that location, he said.

"Usage guidelines are far more effective than outright bans," Dulaney said.

At the Los Angeles Community College District, camera phones are not banned, although there are plenty of locations where security is important, such as the school's finance offices, where student payment records are displayed on computer monitors and laptops, said CIO Jorge Mata.

To limit the risk of someone outside the school passing by a terminal and seeing and photographing private information, the college district has installed "hundreds" of privacy filters on laptop and PC screens, which prevent anyone but the user from seeing the information, Mata said. The filters range in price from \$45 to \$200 apiece, he said. "We don't want to risk privacy," he said.

As for the more general issue of cameras used to take photos of secure information, Mata said common sense by users and general guidelines make the most sense instead of a strict ban on phones with embedded cameras. "Some things do not come down to a technology solution," he said.

IT managers daunted by mobile device security

By Zafar Anjum

- May 27, 2008 (Computerworld Singapore) IT managers are reluctant to take on the responsibility of managing the mobile devices that employees are increasingly using and integrating with enterprise applications, according to a new report by Datamonitor in London.

The report "Enterprise Mobility: Trend Analysis to 2012" also predicts global enterprise expenditures on mobile devices.

According to the study, mobile devices will grow from \$6 billion (U.S.) today to an estimated \$17 billion by 2012.

The report highlights that this kind of growth underlines the need for IT managers to begin to implement mobile device policies.

"Enterprises are fighting a losing battle against employees when it comes to mobile devices, and they should consider supporting a limited selection of devices rather than banning them outright," said Daniel Okubo, an analyst at Datamonitor and the report's author.

Security concerns

According to Okubo, security concerns are the largest barrier to mobility deployments.

In March 2007, Datamonitor conducted a survey of 467 IT managers, CIOs and IT decision-makers to establish issues that are currently preventing enterprises from investing in mobility products. It found that the majority of the respondents rated security as the greatest barrier to adopting those products.

According to the study, as mobile devices like the iPhone are increasingly becoming popular among end users, enterprises are finding that employees want to be able to integrate their personal devices with their corporate e-mail account and other applications. They do not want one device for personal use and an IT-issued device for work.

However, according to the report, so far very few IT departments have yielded to these changing scenarios and are refusing to be responsible for managing such a wide variety of mobile devices. It also found that the iPhone has set a new standard for device usability and the trend of "consumerization" is going to continue.

"There is an element of fear of the unknown," said Okubo. "Enterprises question how security will be managed and whether mobility technologies will fit into their current IT infrastructure."

Need for device management applications

According to the report, now there are carriers such as Vodafone Group PLC that have started realizing the problems that many enterprises face in managing devices. They have started offering hosted device management applications, meaning that if an employee loses his phone, his operator will wipe or lock it. Similarly, if the phone is "broken," a user can contact his operator to remotely diagnose and fix the device and install updates.

"The popularity of mobile devices in the consumer markets is forcing enterprises to consider how best to manage these devices in the workplace, and they need to ensure they have clear policies in place to manage employee expectations," Okubo said.

Mobile-Related Security Threats On the Rise

More than half of information security staffers say risks related to mobile devices and remote workers are up significantly compared to a year ago, new research says. Combine more mobile people with more corporate data passing beyond the corporate walls, and you have a mounting challenge. - By [Al Sacco](#)

May 21, 2008 — CIO — Though viruses, worms and spyware are the IT security threats keeping the most CIOs, CISOs, CSOs and their teams up at night, more than half of them say risks related to mobile devices and remote workers are up significantly compared to a year ago, [according to survey findings](#) released this week.

Such mobile threats include simple user operating error; unauthorized use or misuse of mobile devices; phishing attacks; and loss or theft of devices and data, the [Computing Technology Industry Association](#) (CompTIA) says. CompTIA commissioned market research firm TNS in early 2008 to conduct the online survey of 2,024 "individuals responsible for information security enforcement in their organizations." Surveys were conducted in the United States, United Kingdom, Canada and China.

"As global trends of workforce mobility and decentralization place a greater strain on IT security infrastructure, it is becoming increasingly more complex for IT departments to safeguard information," says Laurel Chivari, vice president, marketing and communications, CompTIA.

The challenge to IT is compounded by a lack of appropriate security training for users. Though 71 percent of respondents say their organization provides remote access to corporate data and systems to mobile workers, only 39 percent have offered specific security training to those remote staffers, the survey found. But the number of organizations providing such training does appear to be on the rise: **another CompTIA survey** from last year found less than a third of organizations holding security training sessions for mobile staff. And 19 percent of respondents in the recent survey say they plan to offer security training in 2008, compared to the 10 percent with such plans from the earlier survey.

The benefits of **security training for mobile workers** are clear: Ninety-two percent of respondents from organizations that have instituted some form of training for remote workers say they believe the number of major security breaches has been reduced, according to CompTIA.

Currently, the three leading IT skills, from a hiring manager standpoint, are security, general networking and operating systems, **according to CompTIA**. But mobile and wireless skills are expected to grow most in importance over the coming five years to become the number one most valued skill set.

Feds encrypt 800,000 laptops; 1.2 million to go

Encryption software sales boom against backdrop of more stolen laptop cases

By [Carolyn Duffy Marsan](#), Network World, 05/22/2008

U.S. government agencies are scrambling to plug one of their biggest security holes: sensitive information -- names, addresses and Social Security numbers, for example -- stored on laptops, handhelds and thumb drives.

In the last year, agencies have purchased 800,000 licenses for encryption software through the federal Data at Rest (DAR) Encryption [program](#), which is run jointly by the General Services Administration and the U.S. Department of Defense.

"Sales have been very brisk," says Fred Schobert, CTO for integrated technology services at the General Services Administration's Federal Acquisition Service. "We've been somewhat overwhelmed."

The government's fast adoption rate of encryption software comes after numerous headline-grabbing security breaches. Laptop encryption has also been on the rise among corporations, including the likes of [EMC](#) and [IBM](#).

It's been two years since [teens stole a laptop](#) from the home of a U.S. Department of Veterans' Affairs employee's home, putting at risk for identity theft a database of 26.5 million names and Social Security numbers for 26.5 million veterans and military personnel.

But this year alone, laptops with personally identifiable information have been stolen from Bolling Air Force Base, a Marine Corps base in Okinawa, Japan and the National Institutes of Health in Bethesda, Md. In all of these cases, data that wasn't encrypted on these laptops could have been used by thieves for identity theft, according to a list of known security breaches compiled by the Privacy Rights [Web site](#).

While sales on the DAR Encryption program are stronger than anticipated, federal officials admit they haven't secured all of their laptops, handhelds and removable drives yet.

``It was originally thought that there would be about 1 million laptops in DoD and one million in civilian agencies. We roughly came up with the number of 2 million laptops. However that number is informal. It's constantly being

expanded and contracted," says David Hollis, program manager for the Defense Department's Data at Rest Tiger Team.

"We're not worrying about how many laptops and PDAs there are in the government. We're trying to provide an opportunity for federal, state and local governments to secure what's out there," Hollis said.

The [Office of Management and Budget requires](#) federal agencies to purchase encryption software for laptops, handhelds and removable storage devices.

[Want to compare security products? Visit the IT Buyer's Guides now.](#)

The DAR program, which offers encryption software from [10 leading vendors](#), "is really one of the cornerstones of security information assurance overall in terms of the U.S. government," says Robert Lentz, deputy assistant secretary for Information and Identity Assurance at the Defense Department.

One reason feds are buying encryption software is that the prices are so low. On the DAR Encryption program, feds are paying only \$10 to \$12 per laptop for software that retails at \$125 or more.

"The federal IT budget alone is around \$70 billion. When you think about the scale of that budget, \$12 a laptop is pretty cheap insurance," says Ray Bjorklund, senior vice president of Fed Sources, a McLean, Va., market research firm.

Federal officials say they have sold \$17 million worth of encryption software through the DAR program to date. More significant, they say, are the total savings.

"The discounts we have achieved have resulted in a total cost avoidance of \$79 million," Schobert said.

Federal officials say they are getting a discount of more than 80% off retail pricing for encryption software. That's one of the reasons that state and local government agencies are using the contract to buy software.

So far, 76% of sales from the DAR Encryption contracts have been from federal agencies, while 24% have been from state and local government agencies.

"Our largest purchases were made by Agriculture, IRS, Transportation, Army and Social Security Administration," Schobert says. "Thirty state and local government agencies have purchased off the DAR [contracts] These include . . . the New York State Power Authority, the Florida Department of Corrections and Ohio State University."

The DAR Encryption program is the primary contract for federal agencies to purchase this type of software. Civilian agencies aren't required to use the DAR Encryption program, but military agencies are.

"From the DOD standpoint, it's mandatory," Lentz says. "We have made it clear to the department after this award occurred that we wanted to have all crucial mobile devices using this technology by the end of the year. This is the only vehicle they have to buy it."

Encryption of mobile data is a serious issue for government agencies, Bjorklund says.

"As the [wireless](#) technology becomes more robust and more reliable, there is a strong likelihood that it can be used for critical command and control-type applications, and that's where the need for security becomes very, very high," he adds.

Federal officials are expecting strong sales to continue on the DAR Encryption program, as agencies continue to encrypt the data on their laptops and increasingly on their smartphones. GSA said the five-year DAR Encryption contracts could be worth more than \$79 million when they were awarded.

"There is an opportunity for significant sales ahead," Schobert says. "The first year, we were in start-up mode."

The most popular products on the DAR Encryption program are hybrid software packages that offer full disk and file folder encryption.

“The larger organizations want to buy one software product. They want full-disk encryption on their laptops, but they also want to put it on their workstations to encrypt the files they put on removable storage devices,” Hollis says.

Orphaned Accounts Are a Growing Security Concern, Study Says

5/22/2008

By Jabulani Leffall

IT auditors examine accounts just like their financial auditing counterparts. Instead of trial balances, they look at system user accounts to determine who signed on when and who did what.

But what about who's logging into what account and when? More important, are these people even around anymore?

These are some of the questions that a [new study](#) by security software and consultancy firm Symark International attempts to address. The report, released Monday, revealed that 42 percent of the organizations surveyed have no idea how many orphaned accounts they have. Moreover, more than a quarter of respondents said they don't have a set procedure to locate or turn off orphaned accounts.

According to Symark and IT auditors, accounts that are no longer being used by former employees as well as temporary consultant sign-on accounts, among others, are a growing problem at enterprises large and small. "We're talking about plumbing here so it's not a sexy thing," said Ellen Libenson, vice president of product management at Symark. "But it's something security, database and system administrators should look at and take very seriously. It's not sexy until something goes wrong."

One need only look at what happened at online mortgage and loan company LendingTree to see a perfect example of how accounts with no corresponding users can cripple an enterprise. According to a [letter LendingTree released in April](#), a few of the company's former employees possibly helped a small number of their mortgage lender friends gain access to the personal information of LendingTree customers. They did this by sharing passwords and accessing different data and proprietary documents between October 2006 and early 2008. The company did not reveal how many individuals were complicit or the number of records affected.

The situation exemplifies something that is endemic in many IT shops where administrators don't have the time to shut off accounts or there's neither proper communication between IT and HR about who's coming and going, nor formal change management procedures in place.

"This issue is pretty common in many places in varying degrees," said Robert Green, a senior manager at PricewaterhouseCoopers' IT audit practice in Los Angeles. "Another thing that is scary is nameless admin accounts that are set up for development and programming purposes that just tend to sit there. No name is assigned to them so it's a tougher audit trail to traverse and, most of the time, you don't know who logged in when."

In cases like these, an IT auditor doing a security review may check off these orphaned accounts as anything from a minor "exception" in testing to a "significant deficiency," which--in the Sarbanes-Oxley and compliance world--can lead to a material weakness that has to be disclosed to shareholders and the public.

'Hack-and-Pier' Phishing on the Rise

More and more phishers are hacking legitimate Websites, reports say

MAY 21, 2008 | 5:00 PM

By **Kelly Jackson Higgins**
Senior Editor, *Dark Reading*

Researchers have witnessed a growing trend in phishers hacking into legitimate Websites to host their phishing exploits, enabling them to keep their attacks alive longer.

In a [blog post](#) today, F-Secure's Sean Sullivan noted a series of so-called 'hack-and-pier' phishing exploits that had been [reported](#) to phishing clearinghouse [PhishTank](#).

"Instead of setting up their own sites, we're seeing more and more evidence of phishing from hacked sites;

legitimate sites that are unknowingly hosting phishing,” Sullivan blogged. “And then the site cannot simply be pulled offline without collateral damage to the legitimate business. So the Website’s administrator must be contacted to repair the damage.”

Phishers increasingly have been using legitimate sites to host their attacks. According to MarkMonitor, only a small percentage of phishing sites today are created with purchased domain names or hosting. “A study we did in late 2007 showed that over 80 percent of phishing sites were hacked legitimate sites or free Webhosting sites,” says John LaCour, director of anti-phishing for MarkMonitor. (See [Phishers Enlist Google 'Dorks'](#).)

Traditionally, a phisher would register a bogus URL that looked a lot like the real thing, but was a letter or two off, such as “paypal” rather than “paypal,” or a more obscure URL that was less likely to get flagged. But those URLs can be easy to spot and shut down, so phishers have been moving to legit Websites as a way to extend the life of their exploits.

F-Secure’s Sullivan pointed to two recent hack-and-pier attacks that were reported to PhishTank, one on PayPal’s Website, and another on [BBC Sales & Service Ltd](#). PayPal had a phishing pier hidden in its /administrator/ folder, and BBCSales had one in its /includes/ folder.

The big problem, of course, is that most Websites carry vulnerabilities, and phishers are quick to exploit them. “There is a virtually unlimited number of vulnerable Websites on the Internet,” says MarkMonitor’s LaCour. And they’re susceptible to password cracking, remote file inclusion attacks, and malicious file uploads, he says.

David Ulevitch, founder of PhishTank and OpenDNS, says hack-and-pier phishing is really nothing new. “It’s always been much easier for a phisher to compromise a site and put up a phishing page rather than try to use a fraudulent credit card and register a domain and go through all the hassle,” he says.

F-Secure’s Sullivan said in an interview that his firm in the past has seen many examples of hacked legit sites for phishing and other cybercrime uses. “It is a growing trend,” he says. “Like any other technique, practice makes perfect.”

Meanwhile, as long as there are vulnerable Websites, hack-and-pier phishing isn’t going anywhere. “Until the Website’s vulnerabilities are resolved, the phishers will just continue to hack and pier,” F-Secure’s Sullivan wrote.

Why data-loss prevention tools scare the hell out of some

DLP can highlight poor data practices, raise legal issues, early adopters say
By [Ellen Messmer](#) , Network World , 05/22/2008

Though data-loss prevention gear is proving a boon for corporate security, its “see all, know all” style of content monitoring can cast a harsh glare on business practices and legal issues that end up putting information-technology staff on the spot.

DLP content-monitoring equipment often gets rave reviews from security managers deploying it because it can give them a view they never had before into their organization’s daily business communications. It may present the big picture, zeroing in on where sensitive data slipped out and who did the deed. But chief security officers with months of DLP experience caution all this newfound knowledge can be disruptive, spotlighting internal data-management practices that incite concern about possible regulatory violations.

“You move from ignorance to [compliance](#) jeopardy,” acknowledged Tony Spinelli, senior vice president of information security at credit information services firm [Equifax](#), describing one impact that deploying DLP — in this case, the [Symantec](#) Vontu equipment — made at his firm. “A lot of regulations say when you know what’s leaving your network, you have to disclose that.”

Spinelli, who spoke on a panel at last month's RSA Conference on the topic, said in spite of the initial disruption caused by finding out about internal business data practices that had to be fixed, Equifax is now so accustomed to DLP content-monitoring that it's now considered just part of the security "hygiene," he said.

DLP also has played a role in bringing together the human resources, legal and security groups at Equifax to coordinate content-monitoring policy, he added.

Two other security managers who joined Spinelli at the RSA panel to discuss DLP also cited its disruptive influence.

"How do you look at your data, know your data and understand what you have? We never had tools to tell us what was happening and we relied on anecdotal evidence or audits to find out," said Patrick Lefemine, chief information security officer at Hartford, Conn.-based firm Lincoln Financial Group, another Vontu user.

Lefemine acknowledged the initial piloted use of DLP "scared the hell" out of both management and IT staff, especially the time it spotted the CEO's salary, Social Security Number and home address being inadvertently transmitted. "That got us the funding for this project," he added.

Lefemine said one of the toughest realizations imparted by the hard wisdom of DLP was the need to stop the sharing of even a single unencrypted Social Security Number with business partners -- a demand pressed by Lincoln Financial Group's audit department after it discovered how powerful DLP was in monitoring content.

The third panel speaker, Rhonda MacLean, global information security officer at Barclays Bank, said use of the Vontu DLP highlighted the difficulty of conforming to the many cross-border data-flow regulations of Europe and elsewhere.

"The problem has gotten more complex," she said, noting Barclays Bank operates in 67 countries. "One incident could [set in motion] regulation dominoes." Though DLP can shed more light than you might like on corporate data practices, she commented, it does offer "a source for truth for data" so that needed changes can be made.

MacLean said one drawback Barclays has noticed in its DLP installation is that it's "CPU-intensive" and might impact some real-time communications. But she also noted DLP's broader capabilities are only beginning to be explored as a tool to monitor how business partners, such as outsourcing firms or call centers, treat sensitive data that's shared. "You have to be able to put in your own castle walls with your business partners," she said.

Symantec Vontu isn't the only DLP in town. The range of host- and network-based content-monitoring products (also sometimes called "data-leak prevention" or "data-loss protection") is growing, including those from McAfee, Proofpoint, Reconnex, Verdasys, Vericept and Websense, plus EMC, which last year acquired [Tablus](#) and is now partnering with [Cisco](#) on DLP. (Compare [data-leak prevention products](#).)

[MedStar Health](#), which operates hospitals in the Washington, D.C., area, two years ago deployed the Reconnex gear in its Maryland data center area to make sure that no patient healthcare data covered under the federal [Health Insurance Portability and Accountability Act](#) would leak.

But according to Ron Baklarz, the former director of information systems there (and now [Amtrak](#)'s chief information systems officer), DLP turned out to be a general education tool about what people were doing. Sometimes that meant finding out that employees were doing things online that had to be stopped, such as downloading pornography.

Getting the attention of legal staff or others on the business side wasn't always easy in terms of DLP, says Baklarz, but probably the best approach he found was to set them up with a log-in to the [Reconnex](#) console so they could see what was going on.

"You need to partner with them on compliance," says Baklarz, noting the business people need to be active participants in data monitoring, not leaving it to the IT department.

"People once used to think what you don't know won't hurt you, but what you don't know will hurt you," says Baklarz, adding he found DLP so important, he plans to bring it into Amtrak for use there, too.

Smart phones 'bigger security risk' than laptops

By Leo King

June 2, 2008 ([Computerworld UK](#)) Smart phones are seen as a more of a security risk than laptops and mobile storage devices, according to new research.

Some 94% of senior IT staff fear PDAs present a security risk, just above the 88% who highlighted mobile storage devices as a worry.

Nearly eight in 10 said laptops were an issue. Only four in 10 had encrypted data on their laptops, and the remainder said the information was "not worth" protecting.

The results come from a survey of 300 senior IT staff conducted by endpoint data protection supplier Credant Technologies.

A key danger with PDAs was that over half of IT executives surveyed were "not bothering" to enter a password when they used their phone.

Nine in 10 of the smart phones were being given access to company networks without extra security, even though the phones were individually owned by users. There were no access restrictions being applied to 81% of the phones.

Credant Technologies said smart phones had become "easy pickings" for any opportunists trying to steal them and access information.

Peter Mitteregger, European VP at the company, said: "Companies need to regain control of these devices and the data that they are carrying, or risk finding their investment in securing the enterprise misplaced and woefully inadequate."

Five effective ways to burglar-proof your laptop

Traveling this summer? Check out these easy, yet effective, strategies to protect your laptop and the data stored in it.

By Nestor E. Arellano

June 5, 2008 ([ITBusiness.ca](#)) -- Theft of laptops and other mobile devices is spiraling, and the consequences -- financial and other -- are getting increasingly dire.

These two disconcerting realities are attested to by survey findings from a range of different organizations:

-- More than 81 percent of companies reported the loss of one or more laptops containing sensitive information between 2005 and 2006 -- Ponemon Institute

-- Financial losses from laptop theft exceed \$6.7 million. Around 97 percent of stolen computers are never recovered -- FBI Computer Crime & Security Survey

-- A data breach involving personal customer information can cost a company \$268,000 in reporting expenses, a recent survey by McAfee and Datamonitor indicates.

Despite the irreparable harm such losses/theft -- and potential data breaches that result from them -- can cause to a company's reputation and bottomline, research indicates North American businesses aren't doing enough to

protect themselves.

Around 73 percent of companies surveyed by analyst firm Gartner Group in Stamford, Conn. didn't have a specific security policy for their laptops.

And it's not so much the cost of securing mobile devices -- and the data on them -- that is the issue, according to one Canadian analyst.

There isn't any shortage of easy to use, inexpensive laptop security tools in the market today, says James Quin, senior research analyst at consultancy firm Info-Tech Research Group, in London, Ont.

Commercial encryption software can be purchased for as low as \$50 to \$80, he notes.

The real issue, the analyst says has to do with a lack of employee awareness and education.

To remedy this we've put together five tips on information workers can use immediately to protect their laptops and data from loss and theft.

Some of these may seem self-evident, but it's amazing how little they are practiced.

1. Dock it or lock it up

Nearly 40 percent of laptop theft occurs in the office. It can be prevented by using a docking station permanently attached to your desk with a feature that locks the laptop in place.

More than 80 percent of laptops in the market today are equipped with a universal security slot.

This allows users to attach a cable lock or laptop alarm to the machine. These devices might not foil bolt cutters but they can deter most casual thieves. Locks and alarms usually retail for \$30 to \$50.

While your laptop may be tethered, thieves can still get away with the PCMCIA NIC card or modem that is sticking on the side of your machine. Consider ejecting these cards and keeping them in a safe place when not in use.

2. Tag your laptop for quick recovery

Permanently marking or engraving the outer case of your laptop with your company name, address and phone number is the most basic way of increasing the odds of your machine being returned should it be carelessly misplaced.

Such a marking might also deter thieves, as it could make it harder to resell your machine.

Asset recovery service providers offer tags that cost anywhere from \$5 to \$10 each. Typically the tags come with a 24-hour 800 number which finders can call to report the recovery. Finders are also offered a reward.

Some of the companies offering such services include TrackITBack, YouGetItBack.com, BoomerangIt, ArmorTag and zReturn.

Also consider filing out those manufacturer registration cards. It's a very slim possibility, but if a thief ever sends in the machine for maintenance, this could raise a flag. Keep a record of laptop series numbers this.

This will help authorities determine ownership when the laptop is recovered.

3. Use tracking software

Many vendors offer software products that enable your laptop to stealthily send out a signal to tracking centers in the event the machine is stolen.

The device connects to the Internet and uses GPS technology to alert the service provider or the police of the laptop's location.

Some of the providers and their starting prices include: CompuTrace (\$50 per year), zTrace Technology (\$50 per year), Inspice (\$30 per year), Brigadoon's PC PhoneHome (\$30 lifetime fee), and Stealth Signal's XTool Laptop Tracker (\$40 per year).

Organizations such as government agencies, police and military services or healthcare providers, should consider laptops pre-equipped with tracking devices, said Susan Black, national sales and marketing manager at Mississauga, Ont.-based Panasonic Canada Inc.

For instance, she said Panasonic laptops come with built-in hard drive encryption tools, embedded asset tracking software from CompuTrace and fingerprint scanners that allow only registered users access to the machine.

Some top-of-the-line tracking products enable administrators to remotely delete data from a stolen machine.

4. Deploy a strong BIOS password

Thwart data thieves by password protecting the basic input/output system (BIOS).

The primary function of the BIOS is to identify and initiate component hardware to prepare the laptop so software programs stored on the machine can load, execute and assume control of the laptop.

Some laptop manufacturers have stronger BIOS than others. Find out if the BIOS password locks the hard drive so it can't be removed and reinstalled into a similar machine.

5. Back Up and encrypt data

Always make sure to backup sensitive data. This doesn't have to take a long time you can use built-in backup utilities that come with most operating systems.

If your network doesn't have disk space for back ups, you can consider other offerings such as external hard drives, CD-Rs, tape back-up, even USB flash drives or online storage service.

There are also numerous vendors now offering data encryption tools that render information intelligible to anyone who does not have the proper decryption keys.

Another option is to employ a company virtual private network that encrypts data.

Info-Tech's Quin said there are also many free alternatives available. For instance, Microsoft offers an encryption tool native to its operating system.

"Users only need to activate the Windows encrypting file system (EFS) on their laptop but many people are not aware of it".

The EFS previously suffered from negative publicity because of a reports that it had an inferior management system.

But Quin said this has improved over the years to match many commercial encryption tools.

Another option is Truecrypt -- an encryption tool available for free downloading.

"This is a very powerful tool but it is hindered by the lack of central management capability," said Quin.

Companies deploying a large fleet of laptops might skip Truecrypt but the tool would be ideal for individual professionals or small businesses, he said.

UnitedHealthcare data breach leads to ID theft at UC Irvine

Scammers used stolen data to file false tax returns, steal students' refunds

By Robert McMillan

June 3, 2008 (IDG News Service) A data breach at United Healthcare Services Inc. has led to a rash of identity-theft crimes at the University of California, Irvine.

To date, 155 graduate and medical students at the school have been hit by the scam, in which criminals file false tax returns in the victim's name and then collect their tax refunds. The breach affects 1,132 graduate students who were enrolled with the university's graduate student health insurance program in the 2006-07 school year, said Cathy Lawhon, the university's media relations director.

UC Irvine police and IT staff have been investigating the crime for several months, she said.

"In February, the police began getting reports from graduate students that when they filed their income tax returns, they were being told that their returns had already been filed using their Social Security numbers," she said.

Local and federal law-enforcement agencies have been called in to help with the investigation, and they have traced the source of the data breach to UnitedHealthcare, the carrier for the school's graduate student health-insurance program, Lawhon said.

Based in Minnetonka, Minn., UnitedHealthcare is one of the largest health care service providers in the U.S. A company spokeswoman confirmed that some university students' personal information "may have been accessed without authorization," but she could not comment on the source of the breach.

Other UnitedHealthcare customers have not been affected, she added. "As far as we know, this situation was isolated to UCI."

According to [U.S. Internal Revenue Service](#) spokesman Jesse Weller, scammers have been [particularly aggressive](#) this year, hoping to cash in on the federal government's economic stimulus payments. "Even before the law was signed ... scammers were attempting to get victims related to the stimulus payment, and it has continued since that time," he said.

The IRS is now in the process of sending checks of \$300 to \$600 per person to an estimated 130 million households in the U.S. as a result of the Feb. 13 stimulus package.

Weller could not comment on the UC Irvine breach.

The university has set up a [Web page](#) for those who think they may have been affected by the scam.

"China's Cyber-Militia"

National Journal (05/31/08) Vol. 40, No. 29, P. 16 ; Harris, Shane

China-based computer hackers, including those working on behalf of the Chinese government and military, have deeply intruded into U.S. federal and corporate information systems, stolen strategic information from American executives prior to business negotiations in China, and accessed U.S. electric power plants, possibly causing

major outages, according to U.S. government officials and computer security experts. Among those sounding such warnings is former Cyber Security Industry Alliance President Tim Bennett, who says these incidents emphasize the poor security of critical U.S. electronic infrastructure, as well as government and company officials' lack of acknowledgment of such vulnerabilities. Another information-security expert says that hackers in China have been aggressively mapping the technology infrastructure of American companies, leading to concerns that such mapping is a prelude to information theft, network corruption, and other malevolent activities. "The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction," says federal counterintelligence official Joel Brenner. "It's a kind of cyber-militia." At a recent hearing, Rep. Jim Langevin (D-R.I.) criticized the private sector's "halfhearted approach" to enhancing security, while Cybrinth CEO Stephen Spoonamore says U.S. officials should be more forthcoming about system breaches if the security of U.S. electronic infrastructure and the sensitive information and operations embedded in that infrastructure is to be fortified. Military analysts say China's aggressive pursuit of offensive cyber-capabilities is one tool in a series of "asymmetric" warfare tactics to counter U.S. military might, which neither China's nuclear arsenal nor armed forces can match. The U.S. military is preparing for the day when China or any other nation or hacker group launches a full-bore cyberattack against the country's critical infrastructure through programs such as the Air Force's Cyberspace Command.

Most data breaches discovered too late, study says

500 investigations examined, with ugly results

By Brad Reed

June 12, 2008 (*Network World*) Most companies only learn about network data breaches in the months after their data has already been compromised, according to a new study.

The study, conducted by Verizon Business, looks at [data breaches](#) in a wide variety of industries, such as retail, food and beverage, technology services, and financial services, and it examines more than 500 forensics investigations involving roughly 230 million records over a period of four years.

Looking at the big picture, the study finds that three-fourths of all data breaches lead to compromised data within a matter of days. Despite this, the study also finds that 63% of enterprises don't learn about data breaches until months after their data has been compromised. What's more, 70% of all data breaches are discovered by third parties, such as customers or banks, meaning that most companies have no idea that their data has been compromised until they are alerted by an outside voice.

And even after breaches are discovered, the study finds that nearly half of them take weeks to fix, while only 37% are fixed within a matter of days or hours.

A strong majority (73%) of enterprise data breaches come from external sources, while only 18% come from internal sources such as IT administrators or employees. However, while internal data breaches are far less common than external data breaches, they are far more damaging to data security: A median of 375,000 records are compromised during internal security breaches, compared with a median of 30,000 for external security breaches, according to the study.

The most popular method for breaching company data is hacking, which accounts for 59% of all data breaches studied. Thirty-nine percent of all hacks occur at the application or service layer, while 23% occur at the operating system or platform layer. Interestingly, the study finds that 18% of all hacks exploit known data vulnerabilities. Of these known vulnerabilities, fully nine-tenths had patches available for six months prior to the breach.

The study lists several ways for businesses to guard themselves against future data breaches, most of which do not require a heavy investment in upgrading IT infrastructure. In the first place, the study says that companies fail to actually enact their established security policies. The study also notes that 83% of all network attacks are

not difficult to thwart and that 85% are opportunistic attacks that are not directed against a particular entity but are rather initiated randomly through techniques such as phishing.

What's more, the study finds that evidence of 82% of all breaches studied is available to the victims, but that this evidence is not noticed or acted upon. Thus, the study recommends that enterprises concentrate on enforcing the basics of data security -- such as actively monitoring data logs and creating data-retention plans -- before they take extra precautions against sophisticated hacking or malware assaults.

"Security breaches and the compromise of sensitive data are very real and growing concerns for organizations worldwide," says Peter Tippet, vice president of research and intelligence at Verizon Business Security Solutions. "This can help companies better understand data breaches. ... Most importantly, it urges organizations to be proactive in their approach to security."

Gartner: Be cautious about letting new iPhones into your company

Limit access to corporate apps because of security issues, consulting firm says

By Jaikumar Vijayan

-
- June 11, 2008 (Computerworld) The enhanced security features built into [Apple Inc.](#)'s new [iPhone 3G](#) will enable the devices to be connected more securely into corporate networks. But that doesn't mean they should immediately be given the same kind of broad access to internal applications that PCs typically enjoy, according to Gartner Inc. analysts.
For now, at least, the [iPhone](#) remains largely untested from a corporate security standpoint, Gartner analyst [Ken Dulaney](#) said after Apple's [iPhone 3G announcement](#) this week. He added that although Apple's upgraded handheld may be capable of doing many of the same things that a laptop or desktop PC can do, it has yet to be proven that the iPhone can be locked down in the same manner as PCs can be.
As a result, it may be better for companies to consider providing iPhone access to only [a limited set of applications](#), such as Exchange and Apple's Mail e-mail client, instead of opening up their entire networks to the device, Dulaney said.
"Much about being secure is being consistent," Dulaney said. "If you have two platforms, a PC and a handheld — one of which has years of improvements in security and is very mature, against one that is barely a year old — you are only going to be as secure as the second piece of hardware."
When Apple unveiled the iPhone 3G, which will run the second-generation [iPhone 2.0 software](#) that the vendor announced in March, CEO Steve Jobs and other executives touted several features that they claimed will make the new device suitable for enterprise uses.
Among the most significant of the enhancements is support for Cisco Systems Inc.'s IPsec virtual private networking technology, which will let iPhones connect securely to enterprise networks and communicate using IP-based encryption. The new hardware/software tandem also supports wireless network services via the enterprise version of the [Wi-Fi Protected Access 2](#) protocol, featuring 802.1X-based authentication. In addition, it offers a remote-wipe capability for erasing data if a device is lost or stolen. Those functions are all considered crucial for corporate users.
"Cisco IPsec VPN gets you most of the corporate world," said Glenn Edens, an independent mobile device consultant. Provisioning and configuration management capabilities are also "very well done" on the iPhone 3G, Eden said via e-mail. "It is probably good enough for Department of Defense applications," he added, pointing to the fact that the U.S. military was one of the beta users showcased during the iPhone 3G launch at Apple's Worldwide Developers Conference in San Francisco.

At the product announcement, Bob Borchers, senior director of Apple's iPhone business line, claimed that the security capabilities in the new iPhone will be sufficient for companies looking to [adopt the device internally](#). For example, he said that the iPhone 3G and iPhone 2.0 technologies have managed to "attract the interest of eight of the 10 biggest banks in the U.S."

[John Pescatore](#), another Gartner analyst, acknowledged Apple's focus on enhancing the security features and the policy management and enforcement capabilities in the new iPhone. Apple has narrowed much of the security gap that existed previously between its handheld and rival products, Pescatore said. But he added that the iPhone still doesn't offer quite the same level of security as either BlackBerry or Windows Mobile devices do.

One major issue that remains for the iPhone is the relative lack of third-party security software, such as antivirus and encryption tools, Pescatore said. By comparison, such products are readily available for BlackBerry and Windows Mobile devices.

Because of the iPhone's [relatively small presence](#) within companies, it also has yet to be widely checked for vulnerabilities by third-party penetration testers or even by malicious attackers, according to Pescatore. "There's been no pounding on the software yet or third parties who have been brought in to validate the security," he said.

However, Edens dismissed such concerns and said that many of the third-party tools available for other mobile devices are designed to fix "basic security flaws" in individual products. In contrast, the iPhone is secure out of the box, he said.

Nonetheless, the upcoming release of the iPhone 3G increases the need for companies to pay attention to potential security issues surrounding its use by their workers, said Amrit Williams, chief technology officer at BigFix Inc., a security vendor in Emeryville, Calif.

Williams said that Apple's new support for third-generation wireless networks and for Microsoft Corp.'s Exchange ActiveSync technology, which can be used to push e-mail to iPhones, means that the handheld is much more capable of storing, forwarding and manipulating data than it was before. But, he cautioned, those same capabilities are also likely to make the device a more appealing target for attackers.

"The iPhone is cool, and it is flashy," Williams said. But it also creates new avenues of attack that many enterprises are "just not ready to deal with," he added.

