

Sending Out an SOS

Many government agencies and corporations do a poor job of protecting sensitive records. It is costing them millions annually, and it is unnecessarily putting millions of individuals at risk for identity theft – or worse.

Nikki Swartz

In May, a file containing the names, birth dates, and Social Security numbers of 26.5 million U.S. military veterans and service members was compromised when a computer hard drive was stolen from the Maryland home of a U.S. Department of Veterans Affairs (VA) data analyst.

As if the theft weren't bad enough, VA admitted that the analyst improperly took the unencrypted electronic data home against the agency's policies – and had been routinely doing so since 2003. The VA has launched a full-scale investigation, and the Senate and House Veterans' Affairs Committees have held hearings, but it may be too little, too late for the veterans whose personally identifiable information was exposed. Initial reports were that the data included everyone discharged from the military since 1975 and

some discharged earlier who had filed a benefits claim. Subsequent reports indicated that the data for as many as 1.1 million active-duty service members, 430,000 National Guardsmen, and 645,000 members of the Reserves, may also have been exposed. By most estimates, those veterans will have to be vigilant for decades to ensure they do not become identity theft victims.

VA Secretary Jim Nicholson told the House Veterans' Affairs Committee that fixing the massive data breach could cost U.S. taxpayers "way north of \$100 million" and estimated the final toll could be as much as \$500 million. At the hearing, lawmakers cited the fact that VA has received an "F" grade in four of the past five years on an annual cybersecurity review by the House Government Reform Committee. One insider warned that the agency remains "at risk of denial-of-service

attacks, disruption of mission-critical systems, and unauthorized access to sensitive data," and added that VA has failed to control and monitor employee access, restrict users to only need-to-know data, and does not terminate accounts in a timely fashion when employees leave.

While there was no initial evidence that the theft was anything but random and, so far, no indication that the data has been misused, the incident has illuminated a frightening trend: Employees increasingly and frequently take sensitive data out of the office – authorized or not – via a portable device such as a laptop, memory stick, personal data assistant (PDA), iPod, or smart phone.

But the VA is hardly alone in this. Government agencies and corporations may have rules and policies, but surveys show that more employees are storing sensitive office data on their mobile devices and/or transferring

such information electronically via e-mail or the Internet. The problem is that they are not always securing that data, leaving it wide open to myriad risks.

Scary Statistics

The ability to carry large amounts of data in small but easily lost or misplaced devices has transformed the way millions work, but it has also increased the risk that a forgotten laptop or lost smart phone could fall into the wrong hands and result in a major security breach.

Earlier this year, for example, a laptop computer containing the names and Social Security numbers of 16,500 current and former MCI Inc. employees was stolen from the car of an MCI financial analyst in Colorado. A Fidelity Investments laptop holding Social Security numbers and other information on more than 196,000 current and former Hewlett-Packard employees was taken from a parking lot outside a Palo Alto, Calif., restaurant in March. In another case, a former Morgan Stanley employee sold a used BlackBerry on online auction site eBay with confidential information still stored on the device. In Chicago, 160,000 portable devices are left in taxicabs every year, according to a survey by Pointsec Mobile Technologies, a security software firm. Only 50 to 60 percent of those are reunited with their owner, according to the firm.

Experts say businesses are increasingly putting themselves at risk by allowing the unauthorized and uncontrolled use of portable storage devices. According to Ruggero Contu, Gartner research analyst, these devices can introduce malicious code that can be detrimental to networks. In addition, high data capacity and transfer rates and broad platform support mean that a Universal Serial Bus (USB) or FireWire (IEEE 1394) device (pocket-size hard drives, disk-based MP3 players, digital cameras with memory

Americans Want More Data Security

The American public has little confidence in the security of the nation's digital infrastructure, and most want stronger data security laws.

According to a recent survey, only 18 percent of Americans – or fewer than one in five – believe that existing laws are sufficient to protect them from fraud, identity theft, or other crimes on the Internet, according to the survey of 1,150 adults by the Cyber Security Industry Alliance (CSIA).

Sixty-six percent of respondents said Congress should make protecting information systems and networks a higher priority, and 71 percent thought Congress should pass a strong data security law, similar to California's SB 1386, which mandates that companies report breaches of personal data to consumers.

Of that group, 46 percent said they would have "serious" or "very serious" doubts about political candidates who do not support quick action to improve existing laws.

"While data security alone won't be a deciding factor in an election, the survey does reveal that voters have serious doubts about candidates opposed to strong data security laws," said Paul Kurtz, the CSIA's executive director, in a statement. "Consumers are beginning to understand the link between their privacy and data security, and they are looking to their government leaders for action."

A rash of high-profile data breaches – including the recent Department of Veterans Affairs breach of 26.5 million veterans' records – in the past 18 months have compromised more than 55 million personal records, Kurtz said.

Congress has spent more than a year debating data security legislation without taking action. There are currently eight identity theft, breach notification, and data regulation bills pending in the Senate and House. Many hope the VA data theft will force Congress to pass a comprehensive national data security law sooner rather than later.

Kurtz said such legislation should set reasonable security measures, make notification consistent and predictable, implement industry best practices, and strengthen enforcement. It should also include a safe harbor provision that encourages organizations to encrypt their stored data, said Liz Gasster, the CSIA's general counsel. She said the provision would protect the organizations from liability and remove their need to notify customers if they can prove they encrypted their data.

The CSIA survey can be downloaded in PDF format from www.csialliance.org/resources/publications/CSIA_Internet_Survey_May_2006.pdf.

media) has the capacity to quickly download much valuable corporate information, which easily can be leaked to the outside world, he said.

According to recent studies commissioned by Symantec, 60 percent of respondents store confidential business or client data on their handheld mobile devices and send or receive e-mails that include such sensitive

information. The Symantec study revealed that only 40 percent of those surveyed worked at companies that have corporate policies addressing wireless security.

Pointsec Mobile Technologies and *SC Magazine's* 2005 Mobile Usage Survey revealed that one-third of professionals using mobile devices do not use passwords or any other security

protection, despite three out of 10 storing their PINs, passwords, and other confidential information on the devices. The survey of 73 IT managers also found that almost 80 percent of users do not encrypt the information on their PDA or smart phone even though they store sensitive personal and corporate information on the devices.

According to the survey, 81 percent use PDAs and smart phones to store business names and addresses, 45 percent to receive and view e-mails, 27 percent to store corporate information, and 14 percent to store sensitive information about their customers.

Costs and Risks

In last year's "Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey," nearly 50 percent of the 700 businesses, government agencies, and universities surveyed reported a laptop or mobile device theft in the previous year, representing a total financial loss of \$4.1 million. But,

industry sectors that had breaches affecting between 1,500 and 900,000 consumer records – a total of 1.4 million compromised records. The study revealed that:

- Total costs to recover from a breach averaged \$14 million per company, or \$140 per lost customer record.
- Direct costs for incremental, out-of-pocket, unbudgeted spending averaged \$5 million per company, or \$50 per lost customer for outside legal counsel, mail notification letters, calls to individual customers, increased call center costs, and discounted product offers.
- Indirect costs for lost employee productivity averaged \$1.5 million per company, or \$15 per customer record.
- Opportunity costs covering loss of existing customers and increased difficulty in recruiting new customers averaged \$7.5 million per company, or \$75 per lost customer record.
- Overall customer loss averaged 2.6

ship with the company that lost their data, and 40 percent were considering doing so.

Security Solutions Lacking

Despite the very real risks, many businesses do not seem to be taking data security seriously. A 2006 Symantec Global Survey by The Economist Intelligence Unit found that businesses have been slow to deploy mobile security even though almost one in five businesses has experienced financial loss due to attacks via mobile data platforms.

While the survey revealed that 82 percent of businesses worldwide indicated that they see the damage from virus attacks as the same or greater on a mobile network than on a fixed network, only 26 percent have actually assessed the security risks of smart phones, compared with 81 percent of enterprises conducting security assessments for laptops. Despite the proliferation of mobile device use in the enterprise, only 9 percent of companies have incorporated a comprehensive security architecture designed to include mobile device access. Of the rest, 10 percent of companies have no measures for addressing mobile security, 39 percent are granting mobile devices access to corporate networks on an ad hoc basis, while another 39 percent are integrating mobile devices into their existing fixed network security architecture.

The Economist Intelligence Unit surveyed more than 240 global company executives and found that 55 percent of Western European businesses have deployed security software to protect mobile data, compared to 44 percent in Asia-Pacific and 36 percent in North America.

A recent survey by Centennial Software showed that 91 percent of businesses polled believe portable storage devices pose a large security risk to corporate and network integrity. However, 66 percent of businesses have yet to implement a

Experts say businesses are increasingly putting themselves at risk by allowing the unauthorized and uncontrolled use of portable storage devices.

according to a recent study by The Ponemon Institute, a data breach can be much more expensive – costing a company \$14 million when both tangible and intangible costs are considered.

That study examined costs incurred by 14 companies in 11

percent of all customers and ranged as high as 11 percent.

But that is not all – a related Ponemon survey revealed that, upon receiving notice that their data had been lost, 20 percent of respondents said they had severed their relation-

solution to prevent the unauthorized use of such devices on the corporate network.

Safeguarding Sensitive Data

Considering all that is at stake, what steps can government agencies, businesses, and universities take today to better protect their valuable information?

1. Hire a chief security officer (CSO).

According to "The Global State of Information Security 2005," a worldwide study of 8,200 IT and security executives by CIO and PricewaterhouseCoopers, just 37 percent of respondents said they had an information security strategy. At companies with CSOs, however, that number is 62 percent. Companies with an executive security function also reported that their spending and policies are more aligned with the business and that a higher percentage of their employees comply with internal information security policies. Companies with a CSO also measured and reviewed information security policies more than those without a security executive, and they were far more likely to prioritize information assets by risk level. Companies with a security executive have more resources, too. They averaged more full-time employees and higher budgets.

2. Ask security vendors to help.

Because it is not practical to ban employees from taking work home or using portable devices at and for work, the best bet is to protect sensitive data. According to *The Washington Post*, security companies have devised ways to install layers of password protection and automatic locks on devices. Wireless providers are developing weapons to use against their own products, like digital "bombs" that can wipe out information from long distance so one misplaced device does not result in corporate disaster. Sprint Corp., for example, helps its business

customers protect information even when a device is lost or stolen. Information can be deleted by sending a "kill" signal to a phone over the air. If the device is turned off, however, the signal will not work. Japanese cell phone carrier NTT DoCoMo sells models that include fingerprint scanners to biometrically unlock phones.

information. Gartner's Contu suggests using host-based intrusion prevention tools to ensure employee compliance. The system can be set to generate alerts when portable devices connect to a system. In this way, companies can monitor user activity to ensure that individual access procedures are followed.

Because it is not possible to lock down all their sensitive data, companies should concentrate on managing who is handling that information.

3. Prioritize data-security efforts.

Andrew Jaquith, a senior analyst at Yankee Group, told *CIO Today* that it is not worth it to try to safeguard everything. He said CIOs stand a better chance of protecting information if they prioritize data-security efforts. CIOs should adopt a rationing process for selected critical data, protecting the most important data. Information that includes growth forecasts, for example, might be more critical for some companies than others and, therefore, should be protected accordingly.

4. Monitor data access.

Blocking access to certain data is an ideal solution, but not a practical one. According to Jaquith, without access to certain company information, employees cannot do their jobs efficiently, if at all. But if companies cannot control access, they should monitor it. Because it is not possible to lock down all their sensitive data, companies should concentrate on managing who is handling that infor-

5. Install security software and encrypt data.

Some businesses are installing software on their networks to make it impossible to download corporate information to a portable device or memory stick. If employees need to download data, then they should ensure it is encrypted before storing it on a portable device.

6. Consider banning or restricting the use of portable storage devices with corporate PCs.

In a 2004 report, Gartner advised companies to consider banning uncontrolled, privately owned portable storage devices such as Apple's iPod from corporate personal computers because they can spread viruses or steal critical corporate data. Such devices can bypass perimeter defenses like firewalls and introduce viruses onto company networks. If these small devices are lost or misplaced, they can also expose proprietary corporate information. In addition, the report suggested adopting "personal firewalls to limit activity on USB

ports,” investigating products that can control ports selectively, and “consider employing mobile data protection products to encrypt corporate or sensitive data.”

7. Implement policies and procedures for securing data.

The best defense against breaches is a carefully structured set of policies and procedures that apply appropriate security measures based on the value of the data as well as on the potential risks from internal and external sources, according to *CIO Today*. IT managers need to establish an acceptable use policy that outlines what devices can and cannot be used in the work environment and select an appropriate application for enforcement. Organizations should strive to allow the legitimate use of approved devices by authorized staff, ensuring that business productivity is not affected while actively guarding against the removal of data by unauthorized parties.

8. Train employees.

According to a report by *The Arizona Republic*, all Intel employees – 85 percent of whom use company laptops – are required to participate in a security awareness class, which Intel updates annually. Intel also has a broad-reaching policy that instructs employees to encrypt data before putting it onto a mobile device. If employees are a company’s front-line defense in the battle to secure data, then training is their secret weapon. After all, it is their responsibility to protect and maintain sensitive information, so they must be trained in how to do that properly and effectively. Gartner’s Contu says a security-conscious workforce will be less likely to unwittingly leak sensitive information, by misplacing a storage device, for example.

Securing confidential information is not easy or cheap, but the consequences of not doing so can result in litigation, public embarrassment, federal investigation, and even the loss of the business. ■

Nikki Swartz is a freelance writer based in Kansas City, Missouri, and former Associate Editor of The Information Management Journal. She may be reached at nikkiswartz@hotmail.com

References

- “Americans Want Better Data Security Laws.” *Federal Computer Week*. 23 May 2006. Available at www.fcw.com/article94613-05-23-06-Web (accessed 6 June 2006).
- Berinato, Scott and Lorraine Cosgrove Ware. “The Global State of Information Security 2005.” *CIO*. 15 September 2005. Available at www.cio.com/archive/091505/global.html?action=print (accessed 6 June 2006).
- Brewin, Bob. “VA Cannot Allay Vets’ Fear of Identity Theft.” *Federal Computer Week*. 24 May 2006. Available at www.fcw.com/article94636-05-24-06-Web (accessed 6 June 2006).
- “Centennial Software Security Survey Reveals Companies Slow to React to Portable Device Threat.” *Portland Business News*. 22 May 2006. Available at http://portland.dbusinessnews.com/shownews.php?newsid=77441&type_news=latest (accessed 6 June 2006).
- Contu, Ruggero. “How to Tackle the Threat from Portable Storage Devices.” *CSO Online*. Available at www.csoonline.com/analyst/report2714.html (accessed 6 June 2006).
- “Gartner: iPod, Portable Devices a Corporate Security Risk.” *Mac Observer*. 7 July 2004. Available at www.macobserver.com/article/2004/07/07.18.shtml (accessed 6 June 2006).
- Germain, Jack M. “Protecting Your Most Vulnerable Corporate Data.” *CIO Today*. 6 March 2006. Available at www.cio-today.com/story.xhtml?story_id=41887 (accessed 6 June 2006).
- Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. “2005 CSI/FBI Computer Crime and Security Survey.” Available at <http://www.usdoj.gov/criminal/cybercrime/FBI2005.pdf> (accessed 8 June 2006).
- Gross, Grant. “Lawmaker Calls on VA Chief to Resign after Data Theft.” *IDG News Service*. 25 May 2006. Available at www.infoworld.com/products/print_friendly.jsp?link=/article/06/05/25/78684_HNvacall_1.htm (accessed 6 June 2006).
- Keizer, Gregg. “Data Security Could Be Potent November Election Issue.” *TechWeb News*. 24 May 2006. Available at www.smallbizpipeline.com/shared/article/printablePipelineArticle.jhtml;jsessionid=WU2UFN2XSXY5IQSNDBOCKHSCJUMKJVN?articleId=188500274 (accessed 6 June 2006).
- Keizer, Gregg. “VA Worker Took Data Home for Years Before Break-in.” *TechWeb News*. 26 May 2006. Available at <http://internetweek.cmp.com/shared/article/printablePipelineArticle.jhtml;jsessionid=TGBF3KUI52ZAWQSNDBECKICJUMKJVN?articleId=188500852> (accessed 6 June 2006).
- Masley, Ed. “Lost, Stolen Laptops Bring Security Risks.” *The Arizona Republic*. 13 May 2006. Available at www.azcentral.com/arizonarepublic/business/articles/05120513laptop-ON.html (accessed 6 June 2006).
- Noguchi, Yuki. “Lost a BlackBerry? Data Could Open A Security Breach.” *The Washington Post*. 25 July 2005. Available at www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135_pf.html (accessed 6 June 2006).
- Reuters. “Data on 26.5 Million Veterans Stolen from Home.” *CNN.com*. 22 May 2006. Available at www.cnn.com/2006/US/05/22/vets.data.reut/index.html (accessed 6 June 2006).
- Rothstein, Joel. “Veterans’ Data Theft May Cost \$500 Million.” 25 May 2006. Available at http://news.yahoo.com/s/nm/20060526/us_nm/crime_veterans_dc_7&printer=1;_ylt=AqrpoZn9_6F48YJuLZVIwYXIr0F;_ylu=X3oDMTA3MXN1bHE0BHNIYwN0bWE- (accessed 26 May 2006).
- Symantec. “Symantec Global Survey Finds that Businesses are Slow to Deploy Mobile Security.” Press Release, 4 April 2006. Available at www.symantec.com/about/news/release/article.jsp?prid=20060404_01 (accessed 6 June 2006).
- “Taking Steps to Protect Customer Data.” *CIO Today*. 25 May 2006. Available at www.cio-today.com/story.xhtml?story_id=121000034YRA&page=5 (accessed 6 June 2006).
- Young, Ken. “Firms Admit to Mobile Security Shambles.” *Vnunet.com*. 16 November 2005. Available at www.vnunet.com/vnunet/news/2146149/mobile-security-shambles (accessed 6 June 2006).