The Costs of Not Securing Personally Identifiable Data

By Benjamin Wright

Privacy rights and data security are colliding worldwide. On one hand, people assign greater value to the privacy of their identifying information, such as name, address, credit card number and government identification number, but on the other hand, the availability of this information to computer hackers is rising.

Caught in the middle of this collision are enterprises that hold personally identifiable data. They usually hold the data for legitimate reasons, such as tax requirements, and often they have held this type of data about their customers, employees and other constituents for years or even decades. But the accessibility of these data has changed on account of information technology in general and the Internet in particular.

The interest in these data on the part of criminals comes from the spoils they can reap through identity theft. With a victim's name, address and government ID number, a criminal can take out a loan in the name of the victim.

An alarming number of spectacular data break-ins have occurred recently and continue to occur. These break-ins come at a time when the public and legal authorities expect much more accountability from enterprises that hold private data. Legislatures are enacting new laws, and government watchdogs are taking action. Enterprises, therefore, are paying a price.

The implication is that corporations and government agencies must apply more creativity and resources to secure the data they hold. Personally identifiable data now merit as much protection as cash or intellectual property.

Leadership from California

The state of California is the bellwether in the US. First it adopted Senate Bill 1386, which requires the holder of personal electronic information about a California resident to notify the resident if the holder has reason to believe that security of the data has been compromised. In the US, personal information is defined as name in combination with:

- Social Security number
- Driver's license number
- Financial account number and password

Second, in late 2003, California adopted Senate Bill (SB) 1, which generally restricts the freedom of financial institutions doing business in the state to share personal data with others. Moreover, it specifically penalizes institutions that negligently allow such data to be compromised.

These developments in California have set the tone for events around the world.

The Notice is in the Mail

Since July 2003, a number of institutions have formally notified people about data compromises. After a criminal stole a laptop containing private information on 200,000 Wells Fargo customers, the bank changed the account number of each of the customers, mailed a notice to each of them, followed with a telephone call and offered a year of credit bureau monitoring service. The episode cost the bank millions of dollars and a great deal of negative publicity.[1]

When hackers breached the security of Citibank's online credit card application in Taiwan in November 2003, exposing customer data, the Ministry of Finance investigated and then disciplined the banking giant. Citibank was enjoined from issuing any new credit cards for a month and ordered to unplug all of its online banking services for at least three months to allow the Ministry to inspect security before reinstating the services.[2]

A confounding aspect of California's SB 1386 is that it protects any California resident, regardless whether the data holder knows that a data subject is a California resident. A California resident could, for instance, have an address in British Columbia. Hence, the practice of giving notice of data break-ins is becoming standard well beyond the borders of California. In March 2004, Equifax Canada notified 1,400 data subjects that the security of their information had been compromised.[3]

Also in March 2004, Softbank, Japan's largest broadband Internet service provider (ISP), disclosed to its 4.51 million current and former subscribers that someone had breached the security of its customer database. To atone, the company announced it was dedicating US $37.3 million to free services for its customers, and top executives agreed to forgo a portion of their annual salary. Although it is uncertain how the theft occurred, it appears to have involved the abuse of a password.[4]

Instruments for Snatching Passwords and Other Private Information

To swipe passwords, crafty hackers have a raft of tools at their disposal. One especially insidious tool is a keystroke logger. It surreptitiously records the keystrokes of a victim, enabling the hacker to obtain logon IDs and passwords, so that he/she can later masquerade as the victim.

A keystroke logger allowed a hacker to break into medical records at the University of Washington Medical Center (Washington, USA).[5] Then, a Boston College (Massachusetts, USA) student installed a similar tool on dozens of computers at the university's campus, which ultimately yielded him

private information on 4,000 members of the college community. He used the data fraudulently to shop at the college bookstore.[6]

Keystroke logging software was at the heart of a criminal wiretapping charge against Larry Lee Ropp, a former insurance claims manager. In March 2004, federal prosecutors in Los Angeles (California, USA) alleged that he planted the software on an insurance company computer for the purpose of stealing corporate secrets.[7]

Today, hackers are trying to propagate keystroke loggers and other forms of spyware through spam and other tricks, hoping corporate employees will unwittingly install the software, which will return passwords or other signals to the hackers.[8] The software might be a trojan that, for example, purports to be a benign network utility but includes a trapdoor into the network on which it is installed.[9]

Conclusion

The cost of notifying subjects about data robbery is high. Not only is the administration of the notice expensive, but it inevitably leads to bad publicity in the press, as well. The incentive has never been higher for securing data against password compromises and other break-ins, whether through audits, technical monitors or smarter data management practices.

Endnotes

[1] "The Cost of SB 1386 Damage Control," StrongAuth Inc. Newsletter, 5 December 2003, *www.strongauth.com/newsletters/2003Dec05.html*; Rasch, Mark; "The Wells Fargo Example," 1 December 2003, *SecurityFocus*, *www.securityfocus.com/columnists/201*

[2] Huang, Joyce; "Ministry Punishes Bank for Online Security Leaks," *Taipei Times*, 26 November 2003, p. 10, *www.taipeitimes.com/News/biz/archives/2003/11/26/2003077341*

[3] Suppa, Carly; "Credit Agency Reports Security Breach," *ComputerWorld*, 17 March 2004, *www.computerworld.com/securitytopics/security/story/0,10801,91319,00.html*

[4] Associated Press, "Softbank: Data Leak May Be Insider Job," 18 March 2004

[5] O'Harrow, Robert Jr.; "Hacker Accesses Patient Records," *Washington Post*, 9 December 2000, p. E1; Farrell, G; "Medical Records Particularly Vulnerable to ID Theft," *USA Today*, 12 December 2000, p. 3B

[6] Press release of the Massachusetts Attorney General, 6 February 2003, *www.ago.state.ma.us/press_rel/bc.asp*

[7] Reuters, "Man Charged Over Keystroke Logging," 25 March 2004, *http://news.zdnet.co.uk/internet/security/0,39020375,39149886,00.htm*

[8] Borland, John; "'Spyware' steps out of the shadows," CNET News.com, 19 November 2003, *http://news.com.com/2100-1032_3-5108965.html?tag=prntfr*

[9] Corcoran, Elizabeth; "Hackers Strike Popular Program," *Washington Post*, 22 January 1999, p. E03

Benjamin Wright
is chief legal counsel for PestPatrol Inc. (*www.pestpatrol.com*) and a member of the Texas Bar Association.

Reprinted from the *Information Systems Control Journal*, Volume 4, 2004, Information Systems Audit and Control Association, USA.