

Privacy: It's what's good for business.
Carmen R. Gonzalez

Recent headlines of ChoicePoint's database breach sent shockwaves throughout the CRM industry. Already, the repercussions are spreading far beyond ChoicePoint's doorstep. Though the company must comply with reporting requirements to victimized consumers in CA, they have now capitulated to provide the same to other victims based on many states' Attorneys General demanding formal response. Moreover, there's an investigation by the House Committee on Homeland Security on the way, and it is the intention of Congress to introduce legislation calling for increased Federal Trade Commission oversight of businesses that collect personal data and package it for sale to other financial companies, employers and customers. This avalanche started, not by stealth computer hacking, by an age-old ploy: a con game relying on human weaknesses.

As reported in the Los Angeles Times (Feb.16,2005)¹, a fraud ring opened fictitious debt collection, insurance and other bogus companies based on other people's information, and then solicited credit background information on their targets. ChoicePoint accepted faxed copies of business licenses as proof of legitimacy. Apparently, this security flaw has been corrected by ChoicePoint, as it no longer accepts faxed copies of business licenses. This isn't exactly comforting news to consumers nor to holders of sensitive consumer data, but the pressing need for ensuring consumer protection is the duty of every company, not just those who trade in the dispersal of such data.

Before one assumes ChoicePoint is an aberration, take note that last July Scott Levine was indicted with 144 criminal counts, ranging from conspiracy to fraud to money laundering in having stolen large masses of sensitive consumer information from Acxiom, all the while using the Internet.² Acxiom happens to be one of the largest holders of consumer information in the world. You would have thought this a novel intrusion, but Acxiom suffered a previous security breach the year before when files were being transferred over the Internet to one its clients using a common file transfer protocol server (FTP) server which happened to lie outside its firewall.³ In the month of March alone, two other large holders of sensitive data were found to have been breached: LexisNexis and Bank of America.⁴ This should be a wake-up call to all companies to confirm the security of each of its portals to sensitive data.

Presently, California is the only state in the union that requires companies to notify people when their private information has been compromised. Given the publicity and gravity of this case, it won't take long for other legislatures to follow suit. The applicable sections include California Civil Code sections 1798.29 and 1798.82 to 17908.84 and

¹ Menn, Joseph, "Fraud Ring Taps Into Credit Data", Los Angeles Times, Feb. 16,2005, web link: <http://www.latimes.com/business/la-fi-hacker16feb16,1,7810219.story?coll=la-home-headlines>

² "Identity Theft Case Could Be The Largest So Far", CNN, July 21, 2004, web link: <http://www.cnn.com/2004/LAW/07/21/cyber.theft/index.html>

³ Rosencrance, Linda, "Acxiom Database Hacked", Computerworld, August 8, 2003, web link: <http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,83854,00.html>

⁴ Roberts, Paul, "Hackers Breach LexisNexis, grab info on 32,000 people", Macworld, March 9, 2005; web link: <http://www.macworld.com/news/2005/03/09/lexis/index.php>

apply to anyone, including businesses and governmental agencies, in CA. Those requirements stipulate that an unauthorized breach of personal information automatically triggers the holder of such information to notify the CA resident whose information has been compromised. Personal information includes a person's name plus the disclosure of any of the following: Social Security number, Driver's license or CA ID number, financial account number, credit or debit card number (along with PIN or access numbers). Moreover, the notice must be delivered "in the most expedient time possible and without unreasonable delay", which takes into account any delay imposed by law enforcement investigation and the need to determine the scope of a security breach and steps undertaken to secure the system. The means of notification may be any of the following: writing, electronic, or by "substitute notice". Substitute notice is allowed only if the cost of providing notice exceeds \$250,000 or if over 500,000 people would have to be contacted. Such substitute notice includes email, a web site posting, or notification in a statewide publication.

The events which resulted in ChoicePoint's security breach raise broader questions when it comes to complying with CA's requirements. What rules and processes were in place that contributed to the system's vulnerability? How was the data secured to begin with? What plans should any company have in place should their protections be pierced? No doubt other businesses hoping to avoid this morass are asking such questions of themselves now.

To assist companies in securing personal data using a best practices approach, California's Office of Privacy Protection has put together a set of guidelines.⁵ It lays out in easy-to-understand language everything from how to gather personal information to how to notify victims and how to coordinate with credit reporting bureaus. The key here is preparation and thoroughness in assessing what information is being gathered, how it is stored, who has access and under what circumstances, and how information is properly disposed. Such responsibility carries an on-going obligation to review your internal policies annually or at the very least when a business change may affect the security of personal data (e.g. outsourcing through a call center relying on personal data).

Aside from confirming where security must be shored up, it is equally important to plan a course of action in the case of security tampering. Certainly, CA has set the gold standard, but all our Southwest SOCAP Chapter members should be on the look-out for their own legislative movements in lock-step. By using the best practices set forth by CA's own Office of Privacy Protection⁶, they can stay ahead of the game and anticipate the demands of their consumers. Some key advice includes:

- putting together a written policy on how to deal with personal information breaches
- assigning responsibility within your company to one person to handle notification

⁵ Chief McNabb, Joanne "Recommended Practices on Notification of Security Breach Involving Personal Information", Office of Privacy Protection, California Department of Consumer Affairs, October 10, 2003, web site link: <http://www.privacy.ca.gov/recommendations/secbreach.pdf>

⁶ Ibid

- develop a training curriculum for all new employees on how sensitive information is to be handled
- have a “crisis-management” team in place before data is stolen
- make sure everyone understands what is meant by “personal information” and each term contained in your plan of action
- assume worst-case scenarios and develop responses to detect, manage and remedy such breaches before they occur
- have a system in place where a breach triggers notification to the victim
- mandate that your third-party service providers also adopt your security breach reporting requirements (Be sure to monitor and enforce your rules)
- establish a listing of law enforcement contacts when data security attacks occur (FBI, US Secret Service, National Infrastructure Protection Center, local police or sheriff’s office)
- include any advice from law enforcement into your data security plan
- obtain contact information of individuals whenever you acquire a piece of sensitive personal data that would trigger the California notice requirement if breached
- create written procedures for handling notification of persons whose unencrypted information may have been acquired by an unauthorized person (including data that may have been inadvertently disposed of containing such info)
- keep a record of handling all data breaches and the response your company took every step of the way; use such a record to improve your security even more
- review your security breach plan at least once a year and certainly when your business methods may affect the security of your system.

Aside from adopting these initial recommendations, companies should also be vigilant in employing software technologies to aid in the detection and prevention against security breaches. Just as the criminals are continually raising the ante by becoming more sophisticated, businesses must try to stay one step ahead. With the focus upon security and doing what’s best for the consumer, those aims will likely guide you to do what’s best for your business as well.