Privacy and Data Security – Tips for Avoiding and Dealing with Breaches

Publication
October 20, 2006
Garvey Schubert Barer

Contact

Melodie A. Virtue

Garvey Schubert Barer, October 20, 2006.

Headlines every day report breaches in security where personal identifying information (PII) has either been stolen or lost. PII can be an individual's name and address, social security number, credit card numbers, other account numbers, passwords, or medical or financial information. Under some international laws, it can mean any information that directly or indirectly identifies any individual or makes that individual identifiable, such as buying habits and tastes.

Various surveys report that around nine million Americans were victims of identity theft between 2003 and 2005. Businesses need to use safeguards to protect PII from unauthorized access, use, disclosure, modification or destruction.

A multitude of federal, state, common, and international laws protects privacy and can be used to enforce data security, both computer data and paper storage of PII. There are federal laws regulating privacy relating to medical information, financial institutions, credit reporting, children's on-line privacy, and email spam.

The Federal Trade Commission (FTC), under its own banner prohibiting deceptive and unfair practices, prosecutes companies for failing to adhere to privacy policies or public statements claiming to encrypt data or to limit access to data only to authorized employees.

Many states have laws more stringent than federal requirements. International laws, including Canada and the European Union, have even stricter laws than exist in the U.S. As with individual states in the U.S., foreign countries can claim jurisdiction for breaches of security because someone accessed a U.S.

Even though a company is physically located in only one State, it cannot ignore the often-incompatible laws of other States and foreign countries. Liability for breach of their laws could be triggered if a company's computer places certain types of "cookies" on the recipient's computer located in another jurisdiction.

Compliance with every law would be practically impossible. However, businesses should take certain steps to secure private information about their employees and customers. This article suggests some "best practices" for securing PII. It is based in summary form on "Recommended Practices on Notice of Security Breach Involving Personal Information" developed by the California Department of Consumer Affairs, Office of Privacy Protection, published April 2006. The full article can be accessed at www.privacy.ca.gov/recommendations/secbreach.pdf. Since this best practices list pertains predominantly to compliance with California's privacy laws, businesses should review whether their own State has adopted specific privacy laws. If a business has a web presence, it should survey all the state laws, and adopt measures that would meet the most stringent requirements.

Implement Measures to Protect and Prevent a Data Security Breach

1. Collect the minimum amount of PII needed, and retain it for the minimum time needed.

2. Identify locations where PII is maintained, such as computer systems, laptops, PDA's (e.g., Palm Pilots, Treos, Blackberries, etc.), and record systems.

3. Classify PII according to sensitivity – i.e., individual's name plus credit card number or social security number, plus any password needed to access it, would be the most sensitive.

4. Use physical and technical security safeguards to protect sensitive PII in paper and electronic records.

Authorize employees to have access only to information needed to perform their jobs.

Use technical means to restrict internal access. Keep file cabinets locked and protect computer files with alphanumeric passwords.

Monitor employees' access to sensitive PII.

Remove access privileges of former employees and contractors immediately.

Restrict the number of people who are permitted to carry PII on portable devices. Consider cabling PC's to desks or prohibiting downloading of sensitive files from servers to PC or laptops.

Use encryption on portable devices to protect PII.

5. Promote awareness of security and privacy policies through ongoing employee training and communications.

Monitor employee compliance with policies.

Train new, temporary, and contract employees regarding privacy training and monitoring.

Impose penalties for violating procedures.

6. Require service providers and business partners who handle PII on behalf of the business to follow the security procedures.

Make privacy and security obligations of third parties enforceable by contract.

Monitor and enforce third party compliance.

7. Use intrusion detection technology to ensure rapid detection of unauthorized access. Conduct periodic penetration tests to determine effectiveness of systems and staff procedures in detecting and responding to security breaches.

8. Use data encryption wherever feasible.

9. Dispose of records and equipment containing PII in a secure manner. Shred paper records with a cross-cut shredder and use a program to "wipe" or overwrite data on hard drives.

10. Review data security plans annually and adjust them to take into account changes in business practices.

Adopt an Incident Response Plan

1. Adopt written procedures for internal notification of security incidents that may involve unauthorized access to sensitive PII.

2. Designate one person to be responsible for coordinating internal notification procedures.

3. Train employees in their roles, collect all contact numbers for the incident response team, and make sure that all employees and contractors can recognize a potential breach and know where to report it.

4. Plan for and use measures to contain, control, and correct any security incident.

5. Identify appropriate law enforcement contacts to notify them of security incidents that may involve illegal activities. Include in the plan the contact information for appropriate local police, state high-tech crime official, FBI, and U.S. Secret Service.

6. Consider including in the plan suggestions from law enforcement with expertise in investigating high-tech crimes. For guidance from the FBI National Computer Crime Squad, go to: www.emergency.com/fbi-nccs.htm.

7. Establish written procedures to notify individuals whose unencrypted PII has been, or is reasonably believed to have been, acquired by an unauthorized person. Unencrypted PII is not limited to computer records but includes paper records of sensitive PII. If the plan includes notifying by email individuals whose PII has been breached, obtain the individual's prior consent to use email for that purpose.

8. After an incident, review the response to events and actions taken, and make changes in the plan as necessary. Review the plan annually to take into account changes in business practices.

Notify when a Security Breach Occurs

The following factors may trigger the need to notify law enforcement and individuals whose sensitive PII has been compromised:

When a computer or laptop is stolen or lost, and that computer contained unencrypted sensitive PII.

PII files have been downloaded or copied without authorization.

PII is being used without authorization, such as fraudulent accounts are opened or identity thefts are reported.

If unencrypted PII has been acquired by an unauthorized person:

1. Take steps to contain and control the systems affected by the breach.

2. Conduct a preliminary internal assessment of the scope of the breach.

3. Notify law enforcement.

4. Notify individuals in the most expedient time possible after discovery of a security breach, but within 10 business days, unless law enforcement indicates that providing notice within that time would impede their investigation. Be prepared to notify individuals immediately upon being informed by law enforcement that such notice will not impede their investigation.

The notice to individuals should contain a general description of what happened, the type of PII involved, steps the company has taken to protect the PII from further unauthorized acquisition, what the company will do to assist individuals and provide a toll free number for more information and assistance, and provide information on how individuals can protect themselves from identify theft (see, e.g., www.consumer.gov/idtheft), including contact information for the three credit reporting agencies.

Send the notice by first-class mail, unless the affected individuals have given prior consent to be notified by email.

If more than 500,000 individuals' PII is compromised, the cost of individual notification is more than $250,000, or the business does not have adequate contact information for those affected: i) post the notice conspicuously on the company's website, ii) notify major media – TV, radio and newspapers, and (iii) send a notice by email to affected individuals whose email addresses the company does have.

Be sure to notify only those individuals whose sensitive PII was compromised. Do not be over-inclusive.

5. If PII of more than 10,000 individuals is breached, contact credit reporting agencies (*i.e.*, Experian, Equifax, and TransUnion) before notifying individuals so that they can be prepared to handle a large volume of calls.

Further information on notification requirements can be found in the FTC publication "Information Compromise and the Risk of Identify Thefts: Guidance for Your Business" at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.pdf.