

DISCLOSURE OF PERSONAL DATA: A WAKE-UP CALL FOR HR

Don't look now, but someone is about to steal your identity

Just last year, a data analyst for the US Department of Veteran's affairs took home a laptop and disks containing the names, social security numbers, and other personal information of virtually every person discharged from the United States military since 1975. Despite an existing department policy prohibiting employees from removing such sensitive data, all it took was the actions of one person and the personal information of approximately 26.5 million people has since been compromised. Unfortunately, a data breach of this type is not unique. Over 100 plus data breaches have been reported in the last year alone. Every company that maintains personal and sensitive data and every company that has an employee illegally willing to procure such data is a candidate for a breach.

Consumers, employees, military personnel, and virtually everyone else who has personal information stored with a third party are vulnerable if and when that data gets into the wrong hands. The recent high profile data breach at The TJX Companies compromised the credit, debit and drivers' license numbers of millions of the company's customers. To make matters worse, an ongoing investigation of the breach has exposed the fact that intruders gained access to TJX systems almost one full-year earlier than first revealed by the company. In response, legislators in Massachusetts are now reconsidering a bill that would shift the financial burden generated by a data breach to the company itself. If passed, the law would be the first of its kind to make retailers, government agencies and even nonprofit groups assume full responsibility of a data breach, including all costs and fraud-related losses. As recently as January of 2007, the first of what is expected to be many class action lawsuits was filed against TJX in the Federal District Court in Boston. These types of negligence actions have the potential to create significant exposure for companies especially those that have not taken tangible steps to safeguard sensitive information.

While there is no single universal definition of private employee data, it generally includes employee addresses, photos, social security numbers, dates of birth and medical records. Despite the existence of certain state and federal acts that have narrowly tailored confidentiality provisions, personal information remains vulnerable to both theft and disclosure. Beginning in 2004, California became the first state to enact legislation requiring those businesses that maintain computerized personal data to notify the owner of such data of any breach of the security of the data immediately following the discovery of the breach. The California legislation, that now has been followed in large part by several other jurisdictions defines "personal information" to include the first and last name of an individual, social security number, drivers information, credit card information. Proper notice of a security breach includes written notice, electronic notice or substitute notice (e.g. notice provided through the employer's website or notification to statewide media) in appropriate circumstances. Some states have gone beyond imposing notice requirements on companies and have required those companies to either encourage or require employers to take certain actions to ensure the security of personal information. For example, in legislation passed last year, Colorado law now requires employers to develop a policy for the proper destruction or disposal of paper documents containing "personal identifying information."

Given the current landscape, it is important for employers to focus anew on their legal obligations regarding the privacy of employee data and to review whether they are taking sufficient steps internally to safeguard such data and respond appropriately to security breaches. The first step for any organization or company is to realize that legislation is now in place in at least 30 states requiring employers to protect the privacy and confidentiality of its employee records. In keeping with these new legal requirements, the following is a general focus list that your company can undertake to further protect itself in order to stop a breach or mitigate the effects of a breach once it has occurred:

1. Review all service agreements with your employee benefit plan vendors for privacy-confidentiality provisions.
2. Review all internal practices regarding the flow and protection of sensitive information.
3. Implement a comprehensive policy and identify an individual responsible for enforcing and maintaining the policy.
4. Avoid using social security numbers as employee identification numbers and review existing data collection forms with a focus on eliminating request for personal data unless absolutely necessary.
5. Ensure that employee medical information is maintained in separate, locked files and to store personnel documents (e.g. consumer reports, credit card information) in confidential files apart from employee files.
6. If personal information of employees is kept in electronic format, your company must take steps to ensure that the data is stored in a secure computer system and that access to such data be limited, particularly as to being vulnerable to being taken off site.
7. Establish destruction policies that effectively preclude unauthorized access to personal information. The use of shredders around the office is a cheap, effective way to accomplish this end.
8. Have a response plan in place that can be implemented in the event of a breach situation.
9. Conduct training of management regarding protection of employee data
10. Routinely audit compliance with privacy policies and procedures and
11. Make sure that all steps undertaken are otherwise in compliance with the most updated laws in your jurisdiction.

Data breaches can happen to any organization. All that it takes could be an accidental emailing of a file to the wrong party, a break-in committed by either an employee or third party or the failure by one staff member to follow existing policy at just the wrong time. Breach notification laws are here to stay. By following the list of suggestions presented above, you can help your company stay out of the news. By the way, if you believe that there is no such thing as bad public relations, you probably have not worked for a company that had to send out a breach notification to its employees.