BLOGS

Archives;Privacy & Information Security;Workplace Policies

Set Your Target on Data Security in 2014

Target Corp's data breach has been big news this holiday season, with as many as 40 million holiday shoppers across the nation exposed to potential credit and debit card fraud. According to the Identity Theft Resource Center, which tracks U.S. data breaches, the Target breach was one of over 600 data breaches in 2013. In our increasingly digital world, data breaches are a growing risk with many potential causes, including system failures, human error, employee misconduct, or outside theft.

In the wake of the Target incident, many companies will be setting a 2014 new years resolution to review and upgrade their data security measures and to adopt or update their data breach response plan. These types of data security efforts are often focused on a company's customers, but companies should remember that they have human resources data security responsibilities as well. A number of federal and state laws require the safeguarding of sensitive employee information. For example, criminal and credit background check information is protected by the Fair Credit Reporting Act, employee medical data is protected by HIPAA and the American with Disabilities Act, and many states including Minnesota – have laws requiring the safeguarding of employee social security numbers. In addition to laws about safeguarding data, at least 46 states have enacted data breach notification laws that require a company to promptly inform individuals of security breaches involving personal data that might expose the individual to identity theft or financial fraud.

In light of this legal landscape, protecting employee data, whether in hard copy or electronic form, should be an HR priority in 2014. Protecting customer data is also an important HR issue given that employee error or misconduct can lead to a data security breach. While any information security program and data breach response plan needs to be customized to the particular company, the following are some steps that might be incorporated into a 2014 data security resolution:

- Appoint an employee to be in charge of overseeing and coordinating the company's information security efforts for sensitive employee and customer information stored in hard copy or electronic form.

- Have each company department that handles sensitive employee or customer information work with the company's information security coordinator to: (i) conduct and document an inventory of the type of sensitive information

Related People

Megan Anderson

Partner

Minneapolis

612.632.3004

megan.anderson@lathropgpm.com

handled by that department; (ii) assess potential internal and external data security risks; (iii) develop and document information security safeguards for addressing these risks; and (iv) communicate and train department employees on these safeguards.

- Limit access to sensitive employee or customer data to only those employees whose position requires access to the data and prohibit other employees from engaging in unauthorized access, use, or disclosure of the data.
- Ensure that hard copy records are stored in secured, locked locations and that only authorized personnel have keys to the locked areas.
- Ensure that the company has appropriate technology safeguards in place to secure electronic data from unauthorized access and to limit access to only authorized employees.
- Consider encrypting data when it is transmitted electronically over networks or stored on-line.
- Require employees to use unique, secure password-activated screensavers on computers and any personal devices used for work purposes and to regularly change passwords.
- Ensure that the company has a method for carefully selecting and only hiring third party vendors/contractors capable of securing confidential data and that third party contracts contain language requiring the third party to safeguard the data.
- Regularly train employees on information security measures and requirements.
- Ensure that the company has an effective system in place for obtaining hard copy and electronic data back from departing employees or third party vendors/contractors when their relationship with the company ends.
- Require employees and third party vendors/contractors to promptly report any potential data security breach to the company.
- Adopt a data breach response plan in advance so that the company is prepared to promptly and appropriately address any data breach that does occur.
- Conduct periodic tests and audits of security measures and make adjustments as appropriate.