Don't be a Target

How to protect data security and customers' trust

CHRISTINA D. FRANGIOSA
Attorney
Semanoff Ormsby Greenberg & Torchia, LLC

(267) 620-1902
cfrangiosa@sogtlaw.com

Insights Legal Affairs is brought to you by **Semanoff Ormsby Greenberg & Torchia, LLC**

Recent media attention, including ubiquitous coverage of the Target Corp. security breach over the holidays, has highlighted the increase in security intrusions affecting organizations across industries. As technology moves forward exponentially, security threats and leaks continue to emerge.

"In the digital age, nearly every company holds personally identifiable information of its employees or customers in digital form," says Christina D. Frangiosa, an attorney at Semanoff Ormsby Greenberg & Torchia, LLC. "It's imperative that this information is protected from unauthorized disclosure and that companies have a plan to address any breaches."

Smart Business spoke with Frangiosa about data protection, the role of state laws when it comes to breaches and the importance of assembling a strong data breach response plan.

How should a business go about protecting the data it collects?

First, it's important to understand what kind of data are collected and what are stored. For instance, some companies collect credit card numbers in order to process transactions, but don't keep them.

Once a company understands what it stores, it's important to understand where the data are kept and who has access to them. Companies should limit access to relevant personnel and ensure that security protocols are up to date. If vendors or third parties will have access to these data, it is important to understand their policies so the company's privacy policies can accurately reflect them.

Customers need to know what the company is going to do with their personal information before they entrust it. It's essential that a company abide by the privacy policies it announces.

How should a business proceed if it experiences a data breach?

The first question to ask is, 'What has been accessed and how many people have been exposed?' Then it's important to act quickly. Hopefully, the company already has a plan in place for locking down the data to prevent further breaches, for investigating the source and nature of the breach, and for notifying affected individuals. State laws will govern when and how affected individuals need to be notified.

What role do state laws play in notifying affected individuals?

Forty-six out of the fifty states have implemented data breach notification laws. Companies should consider such laws in each state where their customers reside or where they do business. These laws provide the timeline for reaching out to individuals affected by a data breach and, potentially, notifying credit agencies. The notification may need to happen very quickly after the breach occurs. Some data breach notification statutes provide exceptions to the notification requirement. However, companies should plan ahead so they know what their obligations are and are able to meet them promptly.

What type of personnel should be included in a data breach response team?

A data breach response team should include not only internal personnel — like IT, HR, legal counsel, facilities management, and upper management — but also external resources, such as forensic investigators, law enforcement, notification firms and consumer fraud protection agencies. It's also important to enlist publicity/marketing personnel to help craft public communications about certain breaches. A security breach can have a negative impact on a company's reputation. For instance, Target reported that its profits plunged 46 percent in the fourth quarter of 2013, largely due to revelations of customer data theft. Preventing further loss will be important.

Why is it so important for companies to be proactive about data security?

If a breach occurs, there will only be a short window of time in which the company has to act. Companies that have prepared in advance and developed a response plan will be in a better position to protect themselves, their customers and their employees. It's important to reach out to potential resolution partners before there is an issue so that the company can complete its own assessment of available services and costs without needing to make immediate decisions in response to a ticking clock. ●