The Target Data Breach: What can you and your business learn?

PUBLISHED ON
April 1, 2014

Unless you have been in hibernation this winter, you are likely aware of the massive data breach that Target Corporation suffered between November 27, 2013 and December 15, 2013. Target has disclosed that hackers accessed more than 40,000,000 accounts during that time by stealing customers' personal information -- encrypted PIN data, customer names, credit and debit card numbers, card expiration dates and the embedded code located on the magnetic strip on the back of cards.

What lessons can your business learn from this massive data breach? While the size of your business may be a fraction of Target's, your business may face the same cyber threats as Target and may be responsible to meet similar legal obligations following a data breach.

No doubt, having a system of data security policies, procedures and tools in place to guard against data breaches in the first place is of paramount importance to a business. Such a system will likely reduce the occurrences of data breaches and may serve to reduce some of the costs of a data breach. However, a multi-billion dollar company like Target likely has a very complex, and seemingly thorough, system in place to guard against data breaches, simply proving that no system is perfect and that data breaches are inevitable. Consequently, it is in the best interest of your business to be aware of the myriad of laws relating to the protection and sharing of data, all of which impact the liability a business can suffer upon the occurrence of a data breach. These laws include a web of federal and state laws. The federal laws include the Federal Trade Commission Act, Gramm-Leach-Bliley Act, the Fair and Accurate Credit Transactions Act, and the Health Insurance Portability Act. State laws include breach notification laws, consumer protection laws, safeguard laws, social security number protection laws and disposal requirements.

As an example, the relevant data breach notification law in Pennsylvania is called the "Breach of Personal Information Notification Act." This law applies to all types of businesses and covers breaches of personal information that occur under many circumstances -- including both purposeful, illegal "hacks", like what occurred in the Target breach, along with inadvertent disclosures, like a lost laptop or PDA containing personal information. The law requires that upon discovery of a breach, or reasonable belief that a breach may have occurred, the business must provide notice without "unreasonable delay" to the customer whose personal information may have been compromised. The form of notice varies depending on the breadth of the breach. In addition to notifying the affected resident, the business may also be required to notify all major reporting agencies. A violation of the law constitutes a violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Act, which could result in damages and costs to the violating business.

Since the Target breach affected Pennsylvania residents, Target was required to follow the Pennsylvania law.

However, it is likely that your business, like Target's, also handles personal information of residents from various states. Therefore, upon a data breach, your business, like Target, may have to follow the breach notification laws of dozens of states. Most states and the District of Columbia have enacted their own laws relating to data breach notifications. While there are several common notification obligations across the various sets of state law, many states have enacted provisions that require unique forms and timing of responses. In addition to requiring notice to affected persons, some states also require notice of the breach be made to certain state agencies and law enforcement authorities. Furthermore, businesses regulated by certain governmental authorities may have additional data breach notification requirements. As you can probably guess, the task of figuring out what sort of notice your business would need to provide, when you need to provide it and to whom you need to provide it to could be a complex and expensive endeavor.

Without a doubt, Target is quickly learning that a data breach is long and painful. While the breach itself lasted less than three weeks, litigation will likely last for years. You can expect to see many individual lawsuits brought against Target by affected customers, many of which may ultimately combine into a class-action lawsuit. Experts are estimating that Target may end up spending over $100,000,000 in legal fees alone.

With your business' reputation on the line, data security should be on your radar screen. You must be aware of the laws and the risks now, and develop your own comprehensive data security policy and procedure before a data breach occurs. Please contact us for more information on responding to a data breach, or general questions relating to data security policies and procedures.

View PDF of Entire Publication: The Target Data Breach: What can you and your business learn?

:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com