Don't be a TARGET -- No pun intended

ALERT | DEC 23, 2013

As you read this, you have most likely already cancelled one or more of your debit and/or credit cards if you recently shopped at a Target store. If you have, you are not alone. The Target breach, which affected 40 million credit card and debit card users, is the second largest credit card theft ever. While the massive data breach at Target has caused millions to again realize the risk of a data breach, entities that accept, store or utilize any type of Personally Identifiable Information (PII) and/or Protected Health Information (PHI) should see Target as yet another wake up call; a reminder that entities, even the most sophisticated, must do more to prepare for these inevitable, and potentially catastrophic, events. Do not think that you are exempt because you are not a Fortune 500 Company. Bad actors, rogue employees and mere negligent employees are causing data breaches and substantial liability on an exponential basis for much smaller companies.

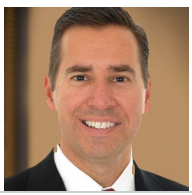
Think you're prepared? Consider this: Target, which is currently the third largest retailer in the US and 11th in the world with over $71 billion in sales, failed to discover for almost *three weeks* that thieves were "swiping" some of the most important PII that Target is tasked with securing. If a company like Target that has some of the most sophisticated and state-of-the-art IT protection software cannot effectively maintain PII, then who can?

Even though you cannot prevent these types of events from occurring, despite your level of sophistication, it is critical to proactively reduce the likelihood of a data breach and, most critically, be prepared to respond quickly and appropriately to manage this type of event. Big or small, your business is successful because of planning and hard work. Like all other business planning, you must be prepared for this event. You would not go into a new year without a discussion of projected sales, expenses, etc. Why would you not be prepared for this contingency? The only way to be prepared is to work with specialists in this niche area.

State legislation and federal regulatory agencies have made it crystal clear that when a data breach occurs, time is of the essence. If an entity is dilatory in properly responding to a breach, enforcement agencies will take issue and will impose far greater fines than if that entity responded appropriately. As if fines imposed by the government are not enough, think about the costs associated with repairing customer relationships and restoring their confidence. For example, Target offered customers 10 percent off purchases on December 21 and 22, along with free credit monitoring for individuals who used a credit card or debit card during the period at issue. This discount, while a hit to its bottom line, will most likely be the least of its economic damages. Target has also posted a letter on its website in which their CEO, Gregg Steinhaffel, apologizes to its customers, explains what to expect and provides contact information that customers can use to reach Target with questions. However, reports are now surfacing that customers have been experiencing difficulty with reaching the customer service representatives. Could Target have been more prepared? Is your business prepared? Lack of preparation is exceedingly costly on the back end.

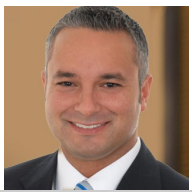
The only way to ensure that you are prepared to appropriately respond to a data breach is to formalize a plan now. Our Data Privacy and Cybersecurity team can help you prepare, developing a plan to reduce the likelihood of a breach, but more critically, developing an appropriate plan to respond to a data breach quickly, thoroughly and effectively. The time to act is now. If you suspect that your business has suffered a data breach, call our Hotline: 855-MH-DATA1 (855-643-2821).

For more information, please contact one of the attorneys listed below.



JAMES GISZCZAK

Read More



DOMINIC PALUZZI

Read More

ADAM SMITH

Read More

dont be a target no pun intended