BRACEWELL

INSIGHTS

Protecting Yourself Against Data Breach: Don't Be a Target

May 6, 2014

To listen to the podcast, ***please click here***.

On May 5, 2014, Target Corporation Chief Executive Officer Gregg Steinhafel resigned after having been with the company for 35 years, another casualty of the massive data breach that continues to damage the nation's third-largest retailer.[1] The data breach already claimed the job of Target Chief Information Officer Beth Jacob, who resigned shortly after the breach had been discovered and disclosed.[2] But both of these high-profile resignations pale in comparison to the impact on Target itself, its business, its profits, and its future.

The data breach occurred on approximately November 12, 2013, at which time hackers began to access more than 40 million credit card numbers and 70 million addresses, phone numbers, and other personal information.[3] From that time through February 1, 2014, Target spent a whopping $61 million responding to the breach.[4] This total *does not include* the costs (and potential liability) incurred in the more than 90 lawsuits filed against Targets by their customers and banks, and it does not account for the fact that Target's holiday sales fell by more 46 percent from the same quarter in the previous year due to shaken consumer confidence.[5] Also, the $61 million does not capture the spectacle of Target Chief Financial Officer John Mulligan appearing before the Senate and testifying that Target was "deeply sorry"[6] but that it failed to have responded to multiple intrusion warnings from its software prior to the breach.[7]

The Target breach was followed by high profile breaches at Neiman Marcus[8] and Sally's Beauty Supply,[9] although none on the same scale as Target. Nonetheless, corporations remain at risk and the risks remain much the same: costs to repair the damage, costs to secure their systems, costs to repay the consumers, losses in profits, losses in consumer confidence, and lawsuits seeking damages for alleged negligence. Intense media and Congressional scrutiny have classified all data breaches as direct attacks on privacy, and any company that has possession of personal identification information should consider itself in possession of potentially explosive material.

The first three paragraphs of this client alert are the external view – in other words, what the public at large perceives of the corporation. But what about the corporation itself? What should it be considering when faced with a data breach? Very little is going to prevent determined thieves from getting into protected systems, even well-protected systems. But the company's response – from containing the damage to communicating with the public – will largely dictate whether it can survive intact.

So, we know the following must happen:

1. *You've got to do something.* There is a saying that ostriches bury their heads in the sand at the first sign of danger on the notion that if they can't see reality, reality can't see them either. But this is a myth. Actually, at the first sign of danger, ostriches take off running, at speeds of up to 40 miles per hour. Now, we are certainly not suggesting that a corporation flee from a data breach. But taking no action – much like what Target was criticized for doing – is tantamount to disaster.

2. *You've got to do something fast*. This is the age of instantaneous communication. Twitter, Facebook, and many other forms of social media mean that information spreads at the click of a button, whether it is true or not. This places tremendous pressure on the victim of a data breach; the longer the delay, the more likely it is that the corporation will lose control of the news cycle. Target's delay in responding to the data breach – a delay measured in weeks – was eons in Internet-time. In the void created by Target's silence, the narrative wrote itself.

3. *You've got to do something effective.* Effectiveness is measured in many different ways, and your response is going to involve corporate multi-tasking on a level that you will rarely ever see. For example, the corporation will need to provide information to law enforcement and its regulators, notify customers, publicly acknowledge the breach, repair the breach, and protect the systems, almost all simultaneously.

Knowing this makes the takeaway lesson simple: every single corporation that has access to personal information must have a crisis response team and a crisis response plan. The team is a collection of key individuals who understand technology, communications, and the core business; the crisis response plan sets forth the steps that must be taken in the event of a data breach. The plan must be rehearsed until it is second nature and it must be continuously updated. Practice does make perfect.

The best course of action is to pair your experts – the people that know your business and your technology – with outside experts – people who know communication, law, and technology. This concerted effort can make your corporation avoid being a target … or a Target.

If you have any questions, please contact ***Kevin Schutte***.

---

[1] http://www.dallasnews.com/business/retail/20140505-target-chairman-and-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach.ece

[2] http://www.bizjournals.com/twincities/news/2014/03/05/target-cio-resigns-wake-of-data-breach.html?page=all

[3] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

[4] http://pressroom.target.com/news/target-reports-fourth-quarter-and-full-year-2013-earnings

[5] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

[6] http://www.usatoday.com/story/cybertruth/2014/02/04/experts-testify-on-true-cost-of-target-breach/5205365/

[7] http://www.startribune.com/business/252451671.html

[8] http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html

[9] http://www.usatoday.com/story/money/business/2014/03/17/sally-beauty-data-security-breach-target/6516839/