Published on *The National Law Review* https://natlawreview.com

The bebe Hack: Guarding Against Cyberbreach During the Holiday Shopping Season

Article By:

Hilary Tuttle

On Friday, retail chain bebe announced that it had identified an attack on computers that operate the in-store payment processing system. The attack may have exposed data from cards swiped in retail locations in the U.S., Puerto Rico, and the U.S. Virgin Islands between Nov. 8 and Nov. 26, including cardholder name, account number, expiration date and verification code. The breach did not impact customers who shopped online or in other international locations, bebe reported, and the company has hired a security firm to stop and investigate the attack.

Almost exactly a year after the massive Target hack, this latest incident comes after a steady stream of sizable breaches among retailers, including Home Depot, JPMorgan Chase and eBay. Consumers have begun to find these hacks increasingly less surprising, and stopped paying as much attention – a phenomenon many are calling "breach fatigue."

But companies are not entirely off the hook. While Target is on the rebound and subsequent breach victims have endured less damage to consumer perception, these cybersecurity incidents still demand a notable amount of contingency planning and mitigation.

According to public relations and social media firm Affect, there are four keys to protecting brand reputation in the event of a security breach:

1) Develop a Fully Locked and Loaded Response Plan

In the digital age, it is essential to have a cyber attack plan in place as part of an

organization’s crisis management strategy. Companies can get ahead of a crisis by leveraging social media to diffuse damaging situations. In order to prepare, be sure to anticipate and understand the kinds of threats that could influence your business and your industry.

“There are four phases of crisis communications: readiness, response, reassurance and recovery,” said Sandra Fathi, president of Affect. “In order to properly respond to a crisis, each stage must be ready to go at a moment’s notice — develop materials such as messages and prepared statements, prepare delivery channels like hotlines and social media platforms and train employees regarding awareness and organizational procedures.”

2) The Customer is Top Priority

Arguably the most important step in maintaining a brand’s image amid a breach is to be honest with customers and inform them about what has occurred — the sooner the better, especially if their personal information is at stake. In fact, 47 states have Security Breach Notification Laws that govern communication with customers in the face of a security breach including the timeline for those communications. Several weeks elapsed before Target released an official statement to their customers and as a result, experienced massive backlash from customers, other organizations and the media alike.

Adam Levin, chairman and founder of IDT911, a provider of data risk and identity management services, believes every company needs to demonstrate three things in the wake of a data breach. “Urgency, transparency, and empathy are all critical. I don’t think they [Target] showed enough of those three,” Levin said in an interview with ABCNews.com. Not being upfront with customers can result in a loss of confidence in the brand that can hinder not only the company’s reputation, but could lead to a loss in revenue.

3) Monitor the Situation in Real-Time

Social media can be a powerful tool but “with great power comes great responsibility.” While positive engagements boost a brand’s respect, companies must always monitor for negative interactions in real-time and be even more stringent during a security breach, as customers will turn to social media to respond to situations, regardless of their allegiance to the brand. Develop a Social Media Response Map that outlines anticipated situations and correlated standard responses to avoid any last minute shuffle. Don’t shy away from angry customers that continuously post adverse comments. Depending on the situation, it may be worthwhile to engage with these individuals in a private forum and resolve their concerns, taking the negative sentiments offline.

4) Don’t Repeat the Same Mistakes

For brands, it is especially important to not make the same mistakes twice. Customers may or may not forgive a first offense, so a second go-around is even harder to rebound from. Companies must carefully document and analyze each breach to identify how it happened, why it happened and how to prevent such an event in the future. Consider changing security vendors, deploying new software, re-training staff and amending company policies. It is also important to communicate these changes to customer to reassure them that a similar breach will not reoccur.

National Law Review, Volume IV, Number 348