Legaltech news

Has Hyatt Hotels Learned Its Lesson From Series of Breaches?

Especially following another point-of-sale data breach for the hotel chain, continued negative publicity can reduce the public's trust in a brand.

By **Ed Silverstein** | October 26, 2017

Hyatt Hotel. Photo by Diego M. Radzinschi.

A recent data breach at Hyatt Hotels has led the hotel chain to apologize and once again strengthen its cybersecurity.

The most recent incident, in which data at 41 properties was stolen at point-of-sale systems, follows earlier breaches in 2015 that reportedly impacted some 250 hotels. And while Hyatt Hotels has formally apologized for the incident and said it will ramp up security, some are wondering whether the company has learned from it.

“Every breach is a lesson that there is more that can be done,” Robert E. Braun, an attorney at California-based Jeffer Mangels Butler & Mitchell, told Legaltech News.

This breach occurred at point-of-sale systems, which Braun described as “the common factor in most hotel data breaches.” He noted, “We don’t know what Hyatt did in response to the first breach, but they presumably would have audited their third-party systems and received confirmation that their vendors had taken the appropriate steps to protect their systems.”

Braun also said the company “should have—and may have—reviewed its procedures and policies so that they can avoid breaches where possible, and in the case of a breach, discover and react to them promptly.” Though in this case, he added, “it does appear that Hyatt discovered the breach fairly promptly.”

The hotel chain discovered the most recent breach in July, and it was announced to the public earlier this month. It took place at the hotel locations between March 18, and July 2, 2017, according to a company statement from Chuck Floyd, global president of operations at Hyatt Hotels.

Specifically, the breach involves “unauthorized access” to “payment card information from cards manually entered or swiped at the front desk of certain Hyatt-managed locations,” the hotel company said. It was revealed the breach was caused by using a “malicious software code from a third party onto certain hotel IT systems.”

In response, the company undertook what it describes as a “comprehensive investigation to understand what happened and how this occurred, including engaging leading third-party experts, payment card networks and authorities.” That investigation led to the company implementing “enhanced cybersecurity measures.”

Yet, there are consequences to a company from continual breaches. Braun said these could include:

- Continued negative publicity reduces the public’s trust in the brand. That will likely have an impact on loyalty.
- It “suggests” the company “isn’t able to identify, quantify and remediate its risks, which can further deteriorate trust in the firm.”
- It also means that more resources will need to be devoted to data security, which can only come by taking away resources from other areas, such as marketing, product development or other key areas.
- Even if the direct costs of a breach might be covered by cyber liability insurance, the secondary costs of lost business and lost trust are difficult to overcome.

“It’s important to move beyond a reactive position and get ahead of the issue,” Braun advised. “Companies that have been subject to a data breach need to do more than simply report the breach and fix the individual problem. They need to analyze their risk profile and create a culture of security and privacy. Security issues have more to do with individuals than just technology, and the corporate culture that prioritizes awareness of security will be more effective in avoiding and responding to threats. This goes beyond computer technologies—treating all guest information with care, by all levels of the company, will go further to reduce business and legal risks.”

David Thaw, a professor at the University of Pittsburgh School of Law, further told Legaltech News, “There are many reasons an organization may experience multiple breaches, ranging from gross negligence to being an attractive target for repeated attacks by the most sophisticated attacks.”

However, he added, “The most important thing is not to jump to conclusions in the absence of necessary technological details.”

Looking ahead, Braun added that Hyatt should take a “fresh, top-to-bottom approach. Even if the company has conducted a complete risk assessment, it makes sense to start from the beginning, and identify the risks the company must take, those it must avoid at all costs, and how to minimize the remaining risks. These lead to changes in policy to reflect a better understanding of the company’s risk profile, and help drive the company to a culture of security.”

Similarly, **Nicholas Tella, director of information security at Johnson & Wales University**, said support at the company’s board level “is critical. Providing proper financial support for the requisite network security tools and the hiring of highly skilled staff—legal and information security—should be part of the company’s strategic approach to cybersecurity.”

“To be truly effective, cybersecurity must become part of a company’s ethos and fully adopted and implemented by employees at all levels and strictly monitored for adherence by connected partners,” Tella added.

http://www.law.com/legaltechnews/sites/legaltechnews/2017/10/26/has-hyatt-hotels-learned-its-lesson-from-series-of-breaches/