Marriott Hack Shows Risks Of Lax Cyber Diligence In Mergers
By Ben Kochman

Law360 (December 3, 2018, 10:02 PM EST) -- When hotel giant Marriott International Inc. merged with rival Starwood Hotels in 2016, it also unwittingly bought a reservation database where the company said Friday intruders were lurking undetected, illustrating the risks of missing cybersecurity gaps during due diligence.

Class actions and regulatory inquiries continued to pour in Monday in the wake of the breach that Marriott says exposed the sensitive data of roughly 500 million travelers, including their passport numbers, travel dates and encrypted credit card numbers, which were stored on a Starwood network dating back to 2014. The episode is now the second high-profile breach an acquiring company has inherited as part of a billion-dollar deal in recent years, after Yahoo Inc. announced a breach affecting 3 billion users in 2016 while telecom giant Verizon Communications Inc. was in the process of purchasing its assets for nearly $5 billion.

But there's a key difference in the case of Marriott, which finalized its $13.6 billion deal to buy Starwood a few months before Yahoo's announcement. In Yahoo's case, the breach was discovered before the deal was finalized. It ended up knocking $350 million off the purchase price and prompting an agreement to split the costs of some litigation and regulatory fines. Marriott, on the other hand, says it became aware of the breach this September — meaning that it will absorb the full financial and reputational hit from the breach itself.

Courts and regulators are now likely to question whether Marriott took "reasonable" steps to investigate Starwood's cybersecurity posture during due diligence, legal experts say. And the embarrassing episode could spur technical and aggressive cybersecurity research to take on a more central role in future mergers.

"Mergers and acquisitions historically have not required deep investigation at the time of the transactions, and if they did, the transactions wouldn't have occurred," said Jed Davis, a partner at Day Pitney LLP. "But in an era of cyber risk, the question is: What is deep enough?"

Attorneys who have advised companies through mergers say that cybersecurity is still not scrutinized during the due diligence process as closely as, say, a target's financial records. But with data breaches becoming more common and more dangerous, that calculus may need to change.

"No one wants to hear that a deal was held up on a cybersecurity issue," said Ed McAndrew, co-leader of Ballard Spahr LLP's privacy and data security group. "But this was not Marriott's problem until they bought it, and now they own it."

Among the challenges acquiring companies face is that the kind of cybersecurity research that might have dug up the intrusion into Starwood's database can be expensive and time-consuming, which can discourage a smaller company with limited resources or a bigger one that wants to beat out competing bids by acting quickly.

"Cybersecurity diligence is often limited by time, budget and expertise, and so the focus tends to be on reviewing relevant documents and security policies in a data room rather than doing a deep dive into the systems, servers and networks that are hosting and processing voluminous data assets that may contain crippling vulnerabilities," said Ieuan Jolly, who leads the privacy, security and data optimization practice at Loeb & Loeb LLP.

"Just as acquiring companies will use accountants to scrutinize a target's financials to check for irregularities and avoid surprises, the same level of diligence should be applied to uncover cyber risks and vulnerabilities that might lie hidden in a company's security architecture," he said.

Such research could include asking the company for reports from its own vulnerability assessments, or hiring outside firms to conduct penetration tests to dig up any unauthorized intrusions or security gaps, experts say. The purchasing company could also search the black market to see if any sensitive data pilfered from the firm is being offered for sale.

"Traditionally, targets have resisted sharing this kind of information, but in light of the growing number of significant cyber breaches, I think it's going to be harder for targets to push back on that kind of diligence, especially if they have large amounts of sensitive personal information," said Avi Gesser, a partner in Davis Polk & Wardwell LLP's cybersecurity and data privacy practice. Gesser added that acquirers should consider cyber insurance to protect them from risks stemming from breaches, something that Marriott says it has done in this case.

Several cybersecurity companies said in reports over the weekend that the stolen data has not appeared on the so-called dark web, suggesting that a government could have been keeping it and using it for intelligence purposes instead. The nonfinancial types of data exposed in the breach could be repurposed or combined with other information already available on the black market to mount sophisticated phishing attacks, for example, or to keep an eye on major company executives or government officials.

Marriott has offered a blanket apology to customers for the breach, but representatives did not respond Monday to a request to explain what level of cybersecurity research it conducted before finalizing the merger creating the world's biggest hotel chain. The company may be reluctant to get into specifics because lawsuits filed by shareholders and consumers will likely turn on the issue of whether a "reasonable" due diligence process would have discovered the breach earlier.

"It's very hard to predict the exact fallout here because we really don't have enough jurisprudence to be able to point to consistent reasonableness standards," said April Doss, a partner at Saul Ewing Arnstein & Lehr LLP. But in Marriott's case, the sheer size of Starwood's database

combined with the sensitivity of the information it contained should have called for a comprehensive cyber due diligence process, she said.

Bill Nelson, a partner at Lewis Roca Rothgerber Christie LLP, said that Marriott would have been expected to do a deep probe of Starwood's cybersecurity given the scope of the transaction.

"In the case of due diligence, what you have to do has to be reasonable, and that's a sliding scale, but this was a huge acquisition and one would expect significant effort and focus to be put on a transaction with so many dollars involved," he said. "If I'm a shareholder and I'm seeing my value of Marriott go down because someone didn't do adequate due diligence, that's a case that has legs in my mind."

"Regulators are going to be concerned that an entity as large as Marriott didn't detect an intrusion like this," said Hilary Wells, who chairs Lewis Roca's data protection and cybersecurity practice. "Here they are, four years past [the intrusion] and there's been this problem inside their own walls that went completely undetected."

--Editing by Brian Baresch and Kelly Duncan.