The Deal

FROM DECEMBER 16, 2016

CYBER RISK'S BRAVE NEW WORLD FOR DEAL DILIGENCE

Yahoo!'s hacks demonstrate the importance, and difficulty, of investigating the security of targets

BY CHRIS NOLTER

News of the mounting hacks of Yahoo! Inc. (YHOO) subscriber accounts will resonate in 2017 and beyond. Yahoo!'s latest revelation that 1 billion accounts were hacked in 2013, on top of the 500 million hijacked accounts in 2014, comes as CEO Marissa Mayer tries to close a $4.8 billion sale to Verizon Communications Inc. (VZ). The breaches underscore the growing importance of cyber security due diligence as the ambitions and capabilities of hackers grow.

"Not that long ago privacy and cybersecurity were really on the radar screens for buyers only when they were looking for certain types of businesses, ecommerce other B2C companies that collect a lot of information about consumers," Morrison & Foerster LLP lawyer Christine Lyon said, referring to hacks that targeted wallets and identities and were more limited in scope than today's mega-attacks. "The percepton was the cyber security was about [protecting against] someone hacking into your systems, stealing credit card numbers or social security numbers and selling them."

The Yahoo! breach and the October attacks that downed sites of Twitter Inc. (TWTR), Netflix Inc. (NFLX), Amazon.com Inc. (AMZN) and other sites underscore the breadth and scale of the latest attacks. M&A teams have taken note.

In a Morrison & Foerster survey shortly after the Yahoo! attacks, 80% of bankers, lawyers and executives who work on transactions said they are putting more emphasis on cyber security when they conduct due diligence. Buyers can write legal protections into merger agreements and bring in experts from companies such as FireEye Inc. (FEYE) or the big four accounting and consulting firms. Fundamentally, they must also decide how much risk they can stomach.

While Yahoo's hack does not include credit card numbers, it dwarfs other prominent breaches. The Nov. 2013 attack of Target Corp. (TGT), which occurred months after Yahoo's first incursion, exposed 40 million credit cards. The hack of Home Depot Inc. in November 2014, which occurred around the same time as the second Yahoo data heist, involved 56 million credit cards and 53 million email accounts.

News of the Yahoo! breaches sent investors and analysts to the sale agreement's material and adverse change clause, which can allow buyers to walk away from a deal in the case of acts of God and other catastrophic occurences.

WHILE MAC CLAUSES OFFER protection in some cases, Morrison & Foerster lawyer Robert Townsend said that generally they are not the ideal protection from breaches at a target.

"If a MAC is the only way you're protected with respect to cyber security breaches, the likelihood that you as a buyer would able to rely on that as a basis for not closing a transaction is low," Townsend said.

"The courts have found that in order to be able to use material adverse change clause to not consummate a transaction it has to be large material and ongoing detriment to the company that fundamentally impairs its value as opposed to a one time event that might over time might not impact the value of the company as much," Townsend added. "You can see the legal challenges with showing that a cyber breach would constitute a MAC," Townsend said.

Other provisions in the representations and warranties section of the merger agreement may be more useful to a buyer of hacked operations. These representations, in which the seller makes pledges regarding the state of certain aspects of the business, face a lower standard than the MAC clause for a buyer.

"The other measure that we're seeing buyers use is bringin in their own technical experts or having their attorneys bring in technical experts to assess security practices" Morrison & Foerster's Lyon said.

FireEye's Mandiant unit provides cyber due dilligence, as do accounting firms Ernst & Young LLP, KPMG LLP, PricewaterhouseCoopers LLP and Deloitte & Touche LLP and consulting firms such as West Monroe Partners.

"Assume that you've been breached," has become an adage in security. Increasingly, attackers will lurk in networks without overt signs of a hack or detection by IT departments. So if a company can't tell that its own networks are clean, how can it know with certainty that a company its buying is secure?

"One of the challenges you get into with the bidding process-no different from buying a house-is the diligence itself is going to be limited in nature,' said Sean Curran, director of security and infrastructure at West Monroe Partners. "You get to walk around but you don't get to pull the drywall off to see if there are termites."

West Monroe Partners of Chicago provides due diligence on about 240 transactions a year and has its own cyber security team. It works primarily with PE-backed firms.

The merger of Yahoo! and Verizon is something akin to "two elephants dancing," he said, with buyer and seller containing vast portfolios of assets. Verizon would combine Yahoo!'s advertising technology, user base and other assets with its own digital holdings. Calculating the impact of the hacks is complex math.

"The challenge is that we still don't have a true, good model to indicate what the impact of a breach is," he said. In the wake of an attack, a hacked company might release a figure for how much it spent to remediate the breach. Litigation could add to the costs. Then there is the drop in stock price over time.

After the costs that can be logged into the company ledger, there is the drop in stock price over time and damage to the business and brand, which are difficult to assess. "Where do you draw the line and say this is the impact?" Curran asked.

Buyers need to evaluate the risk associated with their purchase against their investment thesis, he suggested. If a company is purchasing a peer to gain new technology or products it can bundle with its own offerings, the damage from a hack may be less than if it were paying up for a large group of subscribers that were compromised.

Hacks will continue, but so will acquisitions.

"There are very few organizations who are saying if I found out there was a breach or I found out there are serious security holes I would walk away from a deal," Curran said.

TheDeal.com (ISSN 1547-7584) is published by The Deal.