Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Ways To Keep Cybersecurity Risk From Derailing A Deal

By **Chelsea Naso**

Law360, New York (February 19, 2016, 2:13 PM ET) -- Cybersecurity threats are a growing risk to corporations of all sizes, and failing to take specific precautions when inking a deal — even one outside a highly regulated industry — can drive up the costs while weighing on the benefits of a transaction, experts say.

It's becoming more crucial now than ever to take the time and effort to incorporate cybersecurity risks into valuations, to ensure the right due diligence is being done, and to have cybersecurity-focused post-closing protections in place.

"Cybersecurity is no joke. It's an important issue and potentially crippling risk to a company," said Schulte Roth & Zabel LLP partner Robert Kiesel, who chairs the firm's intellectual property, sourcing and technology group.

Here, Law360 outlines how deal makers can mitigate cybersecurity risks.

Factor It Into the Price

While cybersecurity risks have been on the radar of businesses that are considered more likely to be victims of a breach — such as retailers or insurance carriers — any company with intellectual property, nonpublic data, customer lists or other electronic corporate assets can be a target, Mayer Brown LLP counsel Paul Chandler noted.

"It's coming up in virtually every deal," Chandler said. "We're seeing more buyers becoming more sophisticated with less obvious risks to the deal and the value they are expecting to get."

And buyers that have not yet fully internalized the impact that cybersecurity risks — or even actual breaches — can have on the company or assets they are acquiring could find themselves paying a high price for a damaged brand.

That's why it's essential to give weight to cybersecurity when trying to pinpoint how much a company or asset is worth, explained Baker & McKenzie partner Brian Hengesbaugh, who chairs the firm's data security practice.

"When you're assessing the value of the target, it's really critical to evaluate the cybersecurity house of the target company," Hengesbaugh said. "It's value may be less to you, or it may be so bad that you may

not even want to purchase it."

Size Up the Company Culture

Due diligence is key to finding any cybersecurity breaches or areas that may open the combined company to risks down the road. During the due diligence process, it's important that in addition to evaluating the financials, buyers also take stock of the target's cybersecurity programs and practices.

This is particularly essential when the target company is younger or less developed, as its cybersecurity protections may be less comprehensive, according to Hengesbaugh.

"Typically it's the case that the target company is not as risk averse or as cybersecurity conscious as the acquiring company," Hengesbaugh said. "Oftentimes the acquiring company is a bigger brand. Especially if [the target company] is a startup, they may be more lax in terms of what their practices are."

The due diligence process should include scoping out written procedures such as the written information security program, or WISP, and cybersecurity protections in third-party contracts, said Randy Sabett, vice chair of Cooley LLP's privacy and data protection group.

Checking that those practices are in place is essential, but it can be even more important to follow up with questions about how they implement those practices to get a feel of the target company's culture surrounding cybersecurity and data protection.

"Look at what I call the overall security culture within the target organization and how mature the company is when it comes to privacy and data protection," Sabett said. "Those companies that are more mature about [it] cybersecurity can essentially distinguish themselves from other companies because not only do they know what the compliance and cybersecurity requirements are, but they also practice them."

For some buyers that are eyeing target companies for which a cybersecurity breach could severely devalue its assets, a base-level analysis may fall short. More buyers are beginning to turn to third-party auditors to investigate in depth to identify any past or current breaches, Chandler said.

And while a target may not be comfortable with that level of scrutiny, their resistance could also be seen as a red flag.

"We're even seeing some companies that are looking at targets and engaging third-party counsel to review the target for an evaluation of their security practices or even going in and looking into any evidence of past data breaches," Chandler said.

Look Beyond a Breach

With buyers being even more vigilant in identifying any cybersecurity and data protection issues, any discovered incidents can give buyers pause on how — and if — they want to move forward, said Mark Young, a Covington & Burling LLP special counsel.

"We've dealt with at least a couple examples where deals were at least delayed if not reconsidered because of cybersecurity risks that were identified during the diligence process," Young said. "That's typically in sectors that are more highly regulated and with more detailed obligations to global

regulators."

But a past breach won't necessarily scare away all acquirers, and generally speaking, those deals do tend to move forward, according to Covington attorney Libbie Canter.

It really boils down to how well the incident was handled, and it can even offer a glimpse into the cybersecurity culture at the target company.

“There are superhackers, that no matter how good, there may been an incident that a reasonable company just couldn’t prevent. But did they have a documented response plan, and did they follow that?” Canter said. “Often there is a conversation with the target about the events of the incident, whether it occurred because there was some sort of deficiency."

Make It Part of the Deal

Solid due diligence in the area of cybersecurity, regardless of what it uncovers, can help create a road map for the data protection representations and warranties that should be included in the deal terms, according to Chandler.

Those protections can be further tailored to the specific deal, especially for high-risk target companies.

“You can look at including longer survival periods for cybersecurities reps, specific indemnities for cybersecurity, and even closing conditions surrounding cybersecurity," Chandler said.

But even if cybersecurity isn't an obvious risk for a company, having specific cybersecurity representations and warranties in place is one more way to ensure the acquisition can be deemed a successful one.

“It’s rapidly becoming industry standard, market standard, to get a representation from the sellers or the company that is being acquired that the company has not had a data breach within a certain period of time and that it has written policies and procedures in place that are also industry standard," Kiesel said.

Vet the Systems You Adopt

Proper representations and warranties will help with certain post-closing issues, but it’s important for buyers to prepare for the risks that can arise during the integration process — such as accidentally introducing a virus or other malware to the buyer’s system, noted Steven Caponi, a Blank Rome LLP partner and co-chair of the firm’s cybersecurity and data privacy group.

Those preparations should include ensuring that there is enough cash in escrow to handle any cybersecurity issues that arise during that integration process.

“Parties frequently manage post-closing liabilities by escrowing funds, adopting indemnification provisions and limiting the amount or categories of damages that can be sought," Caponi said. "Depending on the nature or extent of the cyber-incident, however, these efforts to manage the parties’ respective exposure can be woefully insignificant and eviscerate the economic justification for the transaction."

And even the most intense rounds of due diligence cannot prevent all risks, as the physical process of integrating systems and data can result in the buyer's being breached.

“Identifying breaches and security incidents that may have occurred before you bought the company is only part of the solution,” Caponi said. “During the integration process, IT professionals need to ensure they evaluate all hardware/software they are integrating into the organization in order to identify any latent malware, or compromised hardware. All too frequently a localized security breach can morph into a systemic post-closing problem that compromises the larger organization.”

--Editing by Jeremy Barker and Edrienne Su.
