Committed Capital

A GLOBAL PRIVATE EQUITY PODCAST

COMMITTED CAPITAL PODCAST SERIES

Managing Cybersecurity Risk in Private Equity Transactions: Investing in the Modern Age

FEBRUARY 23, 2021

Dechert's Global Private Equity group presented "Managing Cybersecurity Risk in Private Equity Transactions: Investing in the Modern Age," an episode of the firm's Committed Capital Podcast Series. The episode was hosted by Brenda Sharton (moderator), a Dechert partner and co-chair of the firm's Global Privacy and Cybersecurity practice, and featured Jessica Pizzo, Resource Partner focused on technology, security and digital transformation, Court Square Capital Partners, and John Ansbach, Vice President of Engagement Management, at global forensic and consulting firm Stroz Friedberg.

This podcast summarized the key issues and considerations surrounding cybersecurity and its importance for private equity investors, including evaluating cybersecurity risk as part of due diligence, best practices for mitigating risks post-investment, and steps to take if your company becomes a victim of a cyber attack.

HIGHLIGHTS FROM THE EPISODE

Unprecedented Cybersecurity Risks

The year 2020 and the beginning of 2021 have seen an unprecedented rise in the frequency of cybersecurity attacks. Threat actors saw the disruptions caused by the COVID-19 pandemic and the migration to the "work from home" environment as an opportunity and have redoubled their efforts to take advantage of the crisis. We have seen data breach incidents increase as much as fivefold after the beginning of the pandemic, and phishing emails have increased by 35 times. The sophistication of the attacks has also developed, with ransom and other types of attacks increasing in both frequency and sophistication. Most common are the business email compromise attacks in which hackers attempt to divert payments from the legitimate recipient. This arises both in the deal closing context and in the ordinary course of business with, for example, vendor payments.

Best Practices to Reduce Risk

When approaching transactions, private equity sponsors should make sure to include cybersecurity as a part of the due diligence process, including diligence with respect to security operations and technology, legal cybersecurity obligations (regulatory and contractual), cyber insurance coverage, and environmental, social and governance (ESG) aspects of cybersecurity. Third-party advisors are available to assist with cybersecurity diligence and offer a wide range of services. Whether internal or external, it is critical to use the results of this comprehensive cybersecurity due diligence to develop a post-closing action plan, as that is a particularly vulnerable time. Depending on the risk profile of a target, the cybersecurity measures needed can vary, but if not already in place, multi-factor authentication is one tool that should be deployed at virtually all companies now and across all company accounts. Another key measure is to make sure that the cyber insurance policy is in place at the appropriate amount and covers ransom payments. Finally, training for employees is critical so that they can identify risk and, in particular, for employees who are in a position to wire funds from the organization.

What to do After a Breach

One of the key things is to engage counsel early on and have counsel engage the forensic firm on the company's behalf so that all work can be done under attorney-client privilege. Having established relationships with a cybersecurity counsel and in turn a forensic firm will provide coordination across multiple teams. All of these should be the part of following your incident response plan. Early notice to your insurance provider is also important to securing coverage. Analysis of notification obligations must be carefully conducted, including those statutorily required, contractually required customer notice as well as SEC disclosure if implicated. One thing to avoid doing during the incident response phase is a focus on blame. This kind of attitude or focus from executives can put the information technology team in defensive posture exactly at a time when they need to be mainly focused on resolving the problem at hand. Finally, implementing recommendations designed to enhance security after the breach will be important.

To hear the episode in full, click here. For all episodes in our series, click here.