PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Private Equity Must Focus on Cybersecurity Defenses

By Michael Corcione, Principal; Stefan Prins, Senior Manager; Jay Monaghan, Partner and John P. Kavanaugh, Partner

Private Equity (PE) firms are taking notice of the increasing number of queries from investors and new or proposed regulations from the Securities and Exchange Commission on cybersecurity risks. As such, PE firms are enhancing their pre-acquisition due diligence efforts to gauge a portfolio company's current cybersecurity maturity and to identify gaps and weaknesses exposing them to the risk of cyberattacks.

Additionally, PE firms are also becoming more cognizant of the need to maintain portfolio company oversight of their responses to cybersecurity risks during the holding period to ultimately avoid surprises when the time comes to exit the investment.

Pre-Acquisition

For PE firms, the catastrophic impact of a potential cyberattack, the need to get a deeper understanding of an acquisition target's implemented cybersecurity controls, and, most importantly, how essential it is to control cyber gaps and weaknesses have risen to a new level. Historically, addressing cybersecurity risks was more of a "check the box" exercise during pre-acquisition due diligence. Today, the risk has risen near the top of concerns. PE firms are now digging deeper, asking more questions, and engaging the expertise of third-party cybersecurity specialists to conduct thorough assessments of an acquisition target's cybersecurity maturity and areas for improvement.

During the Holding Period

Once an acquisition is successfully completed, efforts to remediate cybersecurity weaknesses and gaps identified should be a focus for the PE firms. Both the previously implemented cybersecurity controls, and any newly implemented controls to address the weaknesses and gaps, must be routinely monitored to ensure they are remaining efficient and effective.

The cybersecurity threat landscape will continue to evolve. Attackers will become more sophisticated, attack schemes will become more complex, and the attack surface will continue to expand for every portfolio company as it grows its business. These evolving threats must be monitored, and cybersecurity controls will require enhancements. Addressing cybersecurity risk is a continual and iterative process of testing and refining controls.

Preparing for the Exit

Exiting an investment should be rewarding for a PE firm which has spent years working diligently nurturing the portfolio company and increasing its value. However, before the exit is completed, the acquiring firm will conduct due diligence. It's critical to this process for the selling PE firm to have full visibility into the portfolio company's current state and history since being acquired. Cybersecurity weaknesses or gaps, failures to keep up with industry best practices, and cyberattack history may be discovered, and then the deal's value will be diminished, or the entire deal could fall apart.

Market Forces and Investor Pressure

The cybersecurity threat landscape is more ominous than ever. Global tensions are heightening the threats of nation-state cyberattacks and the risk of market disruption due to cyberattacks is greater than ever. This is increasing investor concerns and leading them to add cybersecurity at the portfolio companies to their ever-growing list of due diligence inquiries.

Conclusion

PE firms' cybersecurity risks at the portfolio company are real and expanding every day. PE firms must continue to increase their focus on portfolio company cybersecurity risks, threats and the posture of their cybersecurity program. As cybersecurity risks and regulatory requirements continue to grow, PE firms must adopt new processes to ensure they are managing this risk and maintaining compliance with regulatory obligations.

Contact Us

Our professionals have deep experience in PE and cybersecurity, from your side of the desk and beyond. Our team consists of chief information security officers, chief financial officers, chief risk officers, chief operating officers, chief technology officers, traders, internal auditors, and global professionals in the PE space.

If you have any questions about this article or wish to set up a 30-minute conversation with our cyber experts in the PE space, please contact the partner in charge of your account or any of the specialists named below.

Michael Corcione, CMMC-AB, RP
Principal, Cybersecurity and Privacy Advisory
mcorcione@pkfod.com | 646.546.7871

Jay Monaghan, CPA
Partner, Financial Reporting
jmonaghan@pkfod.com | 646.699.2887

John P. Kavanaugh, CPA
Partner, Tax
jkavanaugh@pkfod.com | 646.449.6394

Stefan Prins
Senior Manager, Financial Reporting
sprins@pkfod.com | 203.705.4124