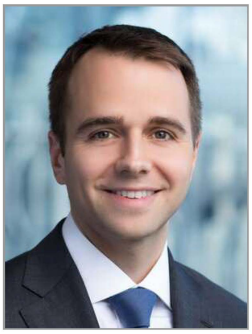
Private Equity Firms Shouldn't Overlook Cybersecurity Risks

By **Ray Bogenrief and William Ridgway** (May 25, 2023, 5:18 PM EDT)

Ray Bogenrief



William Ridgway

As advances in technology drive value creation across business sectors, private equity investors should seek to fully understand and protect the technological infrastructure of their investments, both during the deal-making process and in implementing standardized post-acquisition risk management strategies across their affiliated funds and portfolio companies.

Cybersecurity risk strategies are essential to protect the financial health of a firm's operations and investment portfolio, foster positive investor relations and market reputation, and ensure compliance with constantly evolving U.S. and foreign governmental regulations.

Increasing Attention on Cybersecurity Threats

Cybercrime has become a paramount threat for growing companies as consistently identified by many corporate management teams.

A 2022 Cynet survey of chief information security officers of small and medium-sized businesses found that 94% of respondents struggle to maintain their security posture due to a lack of skilled security personnel, excessive manual analysis and an increasingly remote workforce, among other factors. [1]

And yet, a cybersecurity misstep can undermine a portfolio company's mission and value proposition by subjecting it to unwanted publicity, litigation and government investigations and actions.

Both the U.S. Securities and Exchange Commission and the U.S. Department of Justice are also increasingly emphasizing cyber hygiene.

In order to protect investors, the SEC proposed enhanced cybersecurity rules on registered investment advisers, investment companies and business development companies, including an incident disclosure requirement that extends to private equity firms.

This rule would require registered investment advisers to confidentially report "significant cybersecurity incidents" to the SEC on behalf of a private fund client that experiences such an incident within 48 hours of it occurring.

This reporting obligation would represent a considerable shift for private equity firms in their accountability for managing and mitigating their cybersecurity risk and would require private equity firms to strengthen their internal cybersecurity policies and procedures in order to mitigate cyber risk and streamline incident response.

The DOJ's Criminal Division has also updated its evaluation of corporate compliance programs to include an assessment of how companies manage privacy and security in the context of employee communication platforms. The EU's General Data Protection Regulation and U.K. GDPR compliance also continues to pose risks — dozens of companies have already been fined under the GDPR this year.

As well as looking inward, private equity firms stand to benefit from being more involved in cyber risk management at their portfolio companies, especially in the middle market.

At the portfolio company level, cyber-risk has been traditionally managed as a part of standard operations, which can result in limited oversight by the controlling private equity firm.

With the escalating threats posed by cyber risk, particularly for growth-focused companies with leaner, less mature cyber operations, this model of cyber risk management should be continually reassessed.

In many situations, private equity firms will want to conduct rigorous operational and legal cybersecurity diligence before acquisition, negotiate key risk allocation terms in the underlying definitive purchase documentation, and set minimum standards in post-acquisition management to ensure the resiliency of the cybersecurity platform of a portfolio company and its potential for value creation.

Preacquisition Cybersecurity Risk Management

In the mergers and acquisitions context, an acquirer can potentially be exposed to material damages and liabilities arising from a target company's deficient preclosing cybersecurity practices — e.g., the issuance of a $23.98 million fine to Marriott International Inc. in 2020 arising from a preclosing breach of the hotel guest database of the Starwood brands that Marriott had acquired several years earlier.

The deal-making process often represents the best opportunity for a private equity firm to evaluate and manage cybersecurity risk in respect of portfolio company acquisitions and investments.

By comprehensively understanding the existing cybersecurity regime through due diligence, along with setting clear contractual parameters in the definitive acquisition documents around the allocation of losses and liabilities arising from any cybersecurity failure following a transaction, a private equity firm can more clearly manage financial and other risks associated with the legacy operations of such a target company.

Cybersecurity due diligence is a necessary step to evaluating a target company's resiliency and ensuring its digital assets are intact and well protected.

As cyber risks manifest differently in each company's operations, the diligence process must be tailored to the target company's industry, the value of its digital assets, its regulatory environment and its cyber risk profile. A one-size-fits-all approach to cybersecurity diligence will inevitably fail to reveal all potential liabilities and shortcomings of a target company's cybersecurity management.

Another key piece of the diligence process must be to evaluate the target company's cybersecurity insurance coverage.

Given that a single cyber event can result in substantial costs and lost income associated with recovering compromised data and repairing affected systems, comprehensive cyber liability insurance is a necessity.

Private equity firms should make sure the coverage amounts of target company policies are aligned with loss expectancy and ensure there are no significant gaps in coverage.

As an increasingly common workstream in due diligence processes, private equity firms are engaging third-party diligence providers to conduct automated scans and other cybersecurity diligence in order to evaluate the target company's network security. Such engagement is particularly important for acquisition targets that are heavily regulated or reliant on digital assets.

Along with understanding the cybersecurity profile of a target company, private equity firms may also manage the allocation of financial risk arising from preclosing cybersecurity issues through the negotiation of deal terms in definitive transaction documentation.

A primary method to achieve the foregoing is the inclusion of contractual indemnities for losses or liabilities arising from breaches of representations and warranties covering cybersecurity issues, among other preclosing operations and circumstances of such company.

Such representations and warranties often also serve as an important due diligence function, as sellers are motivated to more fully disclose cybersecurity matters in their disclosure schedules to the acquisition agreement.

Aside from indemnification protections arising from breaches of representations and warranties in definitive documentation, specific indemnities may also be included to address particular or identified cybersecurity issues. While indemnification protections provide a strategy to allocate cybersecurity risk, such an approach is not without deficiencies.

Indemnification terms often include limitations such as deductibles and caps that can interfere with complete recourse. Further, aggressive buyer indemnification proposals can disadvantage such buyers in a competitive sale process or otherwise strain relationships with sellers that may roll over equity into the transaction or otherwise provide ongoing support to the company.

Finally, a coordinated approach to managing cybersecurity risk in the deal process often also includes reallocation of risk to insurers through representation and warranties insurance.

Representation and warranties insurance can serve as an attractive solution for both buyers and sellers to reduce exposure to certain post-closing liabilities, including those arising from cybersecurity issues, in exchange for the representation and warranties insurance premium.

The coverage under the representation and warranties insurance policies can be fairly robust given that buyers are typically able to negotiate broad representations and warranties — including those relating to cybersecurity issues — with less resistance from sellers given that the insurers would be assuming a proportion of the exposure as compared to the sellers in a seller indemnification deal without representation and warranties insurance.

Even so, redress under representation and warranties insurance policies is limited by the policy retention and policy cap, along with the allocation of the policy premium. Representation and warranties insurers are also sophisticated actors increasingly identifying cyber-related exclusions, and often declining to insure known cyber exposures and liabilities.

Post-Acquisition Risk Management

Following an acquisition, private equity firms can further manage cyber risk of their portfolio companies by implementing better cyber practices.

Many medium and small capitalization portfolio companies do not have the financial bandwidth or sophistication to develop robust in-house security teams and policies.

Private equity firms can assist by offering trusted advisers and best practices around strategies and tools that address their gaps, which accelerates the learning curve and allows management teams to focus on their core business.

Private equity firms are also in a position to set minimum information security standards for all of their portfolio companies. Depending upon the risk assessment, they may want to take an active role in setting out expectations and minimum standards by establishing a program and rolling it out to all portfolio companies while providing implementation support and resources.

Private equity firms could also monitor program success by participating in cybersecurity board committee meetings and reassess standards periodically to stay abreast of the constantly evolving cybersecurity risks.

Private equity firms need not develop standards from scratch. Instead, they can use information security frameworks such as the National Institute of Standards and Technology, the Committee of Sponsoring Organizations of the Treadway Commission, the International Organization for Standardization and support portfolio companies in obtaining cybersecurity certifications.

Under the most conservative approach, this program would substantially mirror the internal cybersecurity policies and procedures established by the private equity firm.

Conclusion

Given the operational, financial and reputational costs at stake, cybersecurity should be central to the deal-making process, internal governance and post-acquisition management for private equity firms.

Due diligence has long been a critical tool for uncovering and protecting against key risks in potential acquisitions, though private equity firms must continue to work to adapt their traditional diligence strategies to address emerging cyber risk.

Cybersecurity risk can be further managed and potentially reallocated through the negotiation of certain terms reflected in definitive transaction documentation or the procurement of representation and warranties insurance for transactions.

Finally, a comprehensive strategy also implements post-acquisition risk management to ensure best practices with a firm's investment portfolio.

Ray Bogenrief and William Ridgway are partners at Skadden Arps Slate Meagher & Flom LLP.

Skadden associates Serena Patel and Sahar Segal contributed to this article.

[1] https://go.cynet.com/2022_ciso_survey.