Safeguarding Investments: The Vital Role of Cybersecurity in Private Equity

David Dunn, Senior Managing Director and Head of EMEA Cybersecurity at FTI Consulting

In the dynamic, high-stakes environment of private equity investment where competitive edge is critical, the role of cybersecurity in value creation, retention, and growth is often overlooked. However, the ever-evolving digital landscape sees a commensurate evolution of the cyber threats that pose material risks to investments – making it imperative for private equity firms to prioritize cybersecurity throughout the investment lifecycle. From pre-deal due diligence to exit, a strong grasp of cybersecurity and corresponding risks not only boosts investor confidence but also bolsters the resilience and value of portfolio companies.

In today's interconnected digital landscape, cyber threats loom large and diverse. Ransomware, business email compromise, data loss, and insider threats are each capable of unleashing havoc on an organization's operations, financial performance, and reputational standing. Strategic investors understand that private-equity owned businesses are not immune to exploitation and will integrate cybersecurity into their pre-deal diligence processes. Conducting comprehensive cybersecurity due diligence allows investors to assess the cyber risk exposure of potential targets, identify critical vulnerabilities, and gauge the effectiveness of existing security measures. This proactive approach not only helps mitigate risks but also informs investment decisions – enabling investors to factor cybersecurity preparedness and remediated costs into their valuation models and negotiation strategies.

Robust cybersecurity due diligence can also unlock additional value in portfolio companies. By implementing targeted cybersecurity enhancements, investors can enhance the resilience and competitiveness of their investments. This may involve upgrading infrastructure, implementing robust security protocols, training employees on cybersecurity best practices, and establishing and practicing incident response plans. Proactive measures such as these can mitigate risks and potential costs of a

From a regulatory perspective, it is important to acknowledge the ever-deepening connection of data privacy and cybersecurity. As an increasing number of businesses leverage extensive datasets to enhance their products or drive strategic development, safeguarding sensitive and personal information is paramount. Being able to demonstrate adherence to, or deviation from, stringent regulatory standards such as GDPR and CCPA during the diligence phase can inspire the required level of investor confidence or, conversely, indicate the non-viability of a potential transaction.

However, the attention paid to cybersecurity should not be limited to the pre-investment phase. To enhance this investment safeguard, private equity firms must ensure that cybersecurity remains a top priority as the target is onboarded and finds its place within the portfolio during the first 100 days and beyond. In addition to remediating vulnerabilities identified during diligence, this process entails fostering a culture of cybersecurity awareness and incentivising continuous improvement within portfolio companies – something which can be practically achieved through the implementation of a portfolio company cybersecurity assessment programme. These programmes offer a regular assessment schedule that yields valuable risk-focused data for the private equity owner and gives the portfolio company access to cybersecurity experts who can advise them on how to achieve year-on-year cybersecurity maturity uplifts. Private equity firms who embark on these programmes demonstrate a commitment to the continual elevation of their portfolio's cybersecurity posture, with the potential to experience a corresponding decrease in the level of cybersecurity risk their investments are exposed to.

As portfolio companies prepare for exit, cybersecurity preparedness does not lose any of its significance. If anything, it becomes more critical than ever. Being able to evidence a robust cybersecurity posture demonstrates a commitment to the security of the portfolio company's assets and can significantly enhance its marketability and valuation. As awareness of the threat landscape grows, potential investors are increasingly scrutinising cybersecurity practices as part of their due diligence process, and a wanting security posture can be a deal-breaker. By addressing cybersecurity concerns and demonstrating compliance with industry standards and regulations, portfolio companies can instil confidence in potential acquirers and maximise their exit opportunities.

The pivotal role played by cybersecurity throughout the entire private equity investment lifecycle cannot be overstated, from identifying risks and affecting deal valuations to managing cyber threats and protecting business viability. A robust approach to cybersecurity can be viewed as akin to an insurance policy for private equity investments – representing a set of proactive measures which yield critical, risk-focused, and business-enabling data to drive portfolio growth and position private equity-owned assets for long-term success.