QBE Insurance

Private equity firms enhancing cyber resilience of portfolio companies

Private equity firms manage sensitive financial data related to due diligence, investment strategies and financial projections, making them prime targets for cybercriminals. These firms also operate within networks that include portfolio companies and third-party providers. If the technology system of a single portfolio company or service provider is compromised, it could potentially open pathways to other connected entities including the private equity firm itself.

Aware of the financial, operational and reputational risks posed by increasingly sophisticated cyber incidents and attacks, private equity firms are enhancing the cybersecurity of their digital ecosystems. These findings emerge from a recent survey of 300 risk managers and Chief Information Security Officers (or equivalent roles) at private equity firms with assets under management between $1 billion and $50 billion.

Cyber due diligence is essential

Private equity firms face the complex challenge of securing not only their own digital landscape but also building cyber resilience across their investment portfolio. Prior to making an investment, cyber due diligence provides an opportunity for private equity firms to assess the cyber risks of target companies.

Private equity firms utilize various methods to assess the cybersecurity capabilities of target companies. Nearly half (49%) conduct regulatory compliance assessments and 46% perform third-party and supply-chain cybersecurity assessments. Some private equity firms may prioritize financial and operational evaluations over an in-depth assessment of an organization's cybersecurity controls, however, the survey findings indicate a growing awareness among firms of cyber risks across their investments. Target and portfolio companies are high value targets for cybercriminals and can present a significant risk to a private equity firm's investment if not effectively reviewed.

Due diligence helps private equity firms identify potential cyber risks and the associated mitigation costs. It is a critical step in understanding the cyber challenges that a target company faces and what it will take to improve their cyber posture.

Prior to making an investment, survey respondents say their firms are performing due diligence to evaluate the cybersecurity capabilities of target companies.

Cyber incidents driving need for improvement

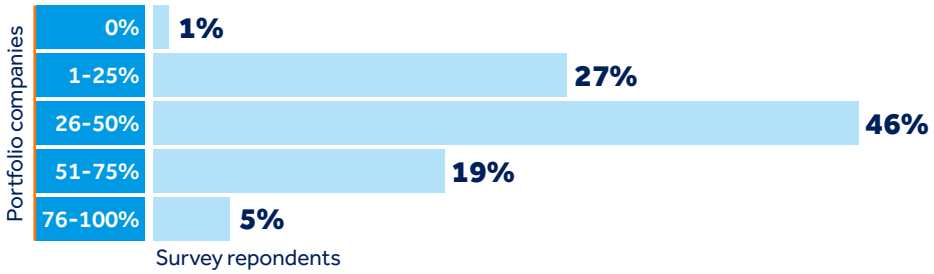
Cyber incidents and attacks can lead to substantial financial losses, potentially impacting a private equity firm's value, reputation and investor confidence.

According to survey respondents, the top cyber threats to private equity firms and their portfolio companies include software/IT vulnerabilities (42%), cloud-security vulnerabilities (40%), data breaches (35%), business email compromise (32%), and ransomware attacks (32%). These findings highlight the diverse range of cybersecurity challenges facing firms and their portfolio companies. Collectively these threats could allow cybercriminals to gain unauthorized access to systems, initiate fraudulent activities, or demand ransoms to unlock data.

The survey also reveals a concerning number of cyber threats reported to private equity firms by their portfolio companies. In the past 12 months, over half of respondents (54%) said that up to 25 percent of their firm's portfolio companies experienced a cyber incident or attack. Nearly a quarter of respondents (23%) reported that 26% to 50% experienced the same.

Among the portfolio companies who have experienced a cyberattack, 46% of respondents indicated that 26% to 50% of those companies reported an incident that involved a ransomware or extortion attempt. These findings underscore the need for robust and proactive cybersecurity measures to prevent against escalating cyber threats.

Private equity firms report that among portfolio companies who have experienced cyberattacks, many involved a ransomware or extortion attempt.



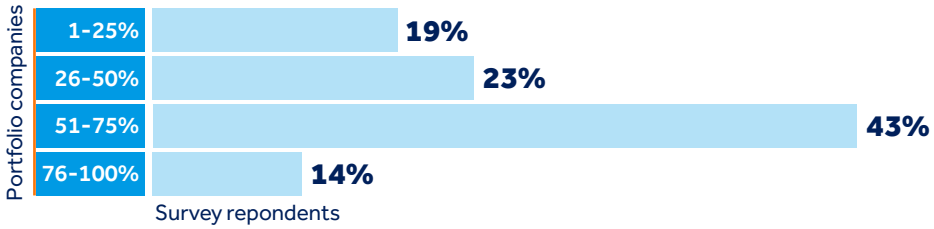
Cyber risk enhancements are making a difference

As cyber threats become more sophisticated, the need to secure technology systems throughout the private equity cyber ecosystem is driving action. To protect their investments, many firms are taking steps to enhance the cyber risk profiles of their portfolio companies.

Notably, 95% of respondents require their portfolio companies have baseline technical security measures such as data loss prevention, endpoint protection, privileged access management, and multi-factor authentication. Similarly, 96% require their portfolio companies implement consistent governance policies and procedures such as incident response plans, data classification, and asset management. Nearly all (97%) require portfolio companies provide visibility and reporting on cyber incidents and attacks.

Following the recommendations from private equity firms, many portfolio companies are revising their cybersecurity best practices. For example, 43% of respondents indicated that 51% to 75% of their portfolio companies have made cyber improvements such as enhancing technical protections and policies. Additionally, nearly a quarter (23%) reported that 26% to 50% of their portfolio companies have made similar cyber improvements.

Private equity firms report that portfolio companies are making cyber improvements based on their cybersecurity best practice recommendations.



These developments are likely due to the higher level of cybersecurity support that portfolio companies receive from private equity firms. For example, 48% of respondents said their firms provide cybersecurity awareness training, while 46% assist with third-party/vendor cybersecurity management needs. Additionally, 45% of firms both fund technical cybersecurity protections and assist with incident response planning.

While the survey demonstrates that private equity firms have helped their portfolio companies make cyber improvements, it also highlights the ongoing need to enhance cyber risk preparedness. Survey respondents report that post acquisition, their firms continue to evaluate the cybersecurity practices and policies of their portfolio companies at various intervals: multiple times per month (3%), monthly (23%), quarterly (34%), semi-annually (21%), and annually (19%).

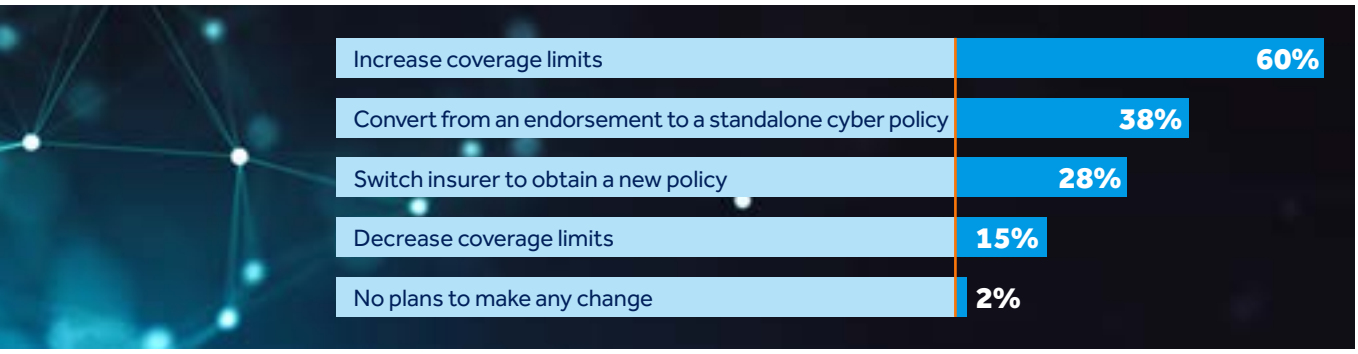
48% of private equity firms provide cybersecurity awareness training to their portfolio companies

Cyber insurance adoption lags

One of the more notable findings of the survey is the rate of cyber insurance adoption among private equity firms and their portfolio companies. Prior to making an investment, 60% of respondents reported that fewer than half of target companies had cyber insurance coverage in place.

When it comes to private equity firms, 53% report having a cyber insurance policy in force. Of the private equity firms with a cyber insurance policy, 60% plan to increase their coverage limits in the next 12 months.

> Private equity firms who have cyber coverage are planning to make changes to their cyber insurance in the next 12 months.



Overall, seventy-six percent of respondents have utilized the value-added cyber risk services offered by insurers over the last three years, indicating these services drive value for private equity firms. Among those firms with a cyber insurance policy, the value-added cyber risk services utilized include cybersecurity assessments (39%), network vulnerability scanning (39%), and incident and response planning (38%).

The survey findings indicate that companies need more education on how cyber insurance provides a valuable layer of protection in an evolving cyber risk landscape and offers additional value from services that can assist in improving technical controls, governance, and cyber resilience across their organization and portfolio.

Cyber insurance policies typically provide comprehensive coverage for both liability and first-party exposures resulting from cyber incidents. On the liability side, most policies cover costs related to data breaches, privacy regulation violations, and third-party claims arising from cyber events. First-party coverage generally includes incident response expenses (legal counsel, forensic investigation, public relations, and crisis management), customer notification and credit monitoring services, business interruption losses, data restoration costs, and ransom payments in extortion scenarios. However, coverage details and exclusions vary between policies, making careful review essential.

53% of private equity firms have cyber insurance coverage

Building cyber resilience

Cybersecurity risk is present throughout the entire private equity investment lifecycle, from pre-deal negotiations to exit – when the firm divests from a company to realize gains and redistribute capital to new opportunities.

Overall, the survey suggests that many private equity firms have sharpened their focus on cybersecurity, helping their portfolio companies better identify, assess, manage and prepare for a cyber incident or attack. However, private equity firms must prioritize cybersecurity within their portfolio companies and reinforce the need for ongoing assessment and improvement.

Here are several measures private equity firms can implement to help their portfolio companies maintain robust cybersecurity postures.

- Provide standardized cybersecurity frameworks and policies to ensure consistent best practices.
- Conduct regular cybersecurity risk assessments to identify potential vulnerabilities.
- Establish and test incident response plans to ensure quick and effective responses to cybersecurity incidents.
- Implement advanced security monitoring tools to detect suspicious activities.
- Offer training programs to elevate cybersecurity awareness among employees.
- Implement third-party risk management policies to assess and monitor the security practices of third-party providers.
- Engage cyber insurers to better understand available coverages and levels of protection.
- Host workshops on cybersecurity threats, regulatory updates, and best practices.

Survey Methodology

The survey was conducted by Wakefield Research among 300 risk managers and CISOs/IT/CISO-equivalent roles at private equity firms with between $1B and $50B in assets under management, between December 13, 2024 and January 9, 2025, using an email invitation and an online survey.

QBE Insurance