Why Investment Management Firms Must Engage in Cybersecurity Due Diligence & Monitoring

Charles Clark | charles.clark@darkbeam.com

The importance of cybersecurity as an investment risk that sits alongside other more traditional risks such as financial, technology, total addressable market, product/market fit, and GoToMarket strategies, is underpinned by the growing body of evidence:

1 Size of the threat

- 1% of Global GDP is being lost to cybercrime (McAffee, The hidden cost of cybercrime)
- Cyber criminals earn $1.5Trn / Year (Atlas VPN)

2 Likelihood of a hack

- Four in ten businesses (39%) and a quarter of charities (26%) report having cyber security breaches or attacks in the last 12 months.
- This is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%) (UK Government Statistics)

3 Cost of a hack

- Average cost of a cyber-attack $590,000 (McAffee, The hidden cost of cybercrime)
- Average cost of cyber-attack for an SMB $98,000 (Kaperskey)

4 Impact on business value

- Average cost of cyber-attack for an SMB $98,000 (Kaperskey)

These stats provide investors an insight into the cyber threat environment their investee companies are exposed to and the shape of the financial risks that exist across a portfolio.

According to EY, **only 7% of security leaders are able to quantify the financial impact of breaches** which means investment managers are left guessing at best. By understanding not just the threat but the vulnerability of an investment company to a cyber-attack, combined with the financial impact, we can provide investment managers a forward looking "risk statement" of their value at risk and a means to prioritise remediation and the potential opportunities to offset this through cyber insurance policies or warranties.

Pre-investment due diligence

- Technology is being designed and built with security by default
- Cyber security maturity assessment
- Vulnerability assessment
- Cyber threat intelligence

This provides investment managers a “risk statement” and advice that can be used to reduce risk for all parties.

Portfolio monitoring

- Weekly vulnerability scans
- Monthly value at risk models
- Monthly threat intelligence updates
- Remediation advice and support

Supporting services for investee companies

- Horizon platform – Freemium can be used by all companies for not just assessing their own cyber vulnerabilities but their suppliers and 3rd parties
- Incident response – this is known to reduce the average cost of an incident by 50% (IBM cost of a data breach)
- Remediation services
- Certification and awareness training
- Cyber insurance and/or cyber warranty

Value to fund manager

- Cyber risk quantified within the context of portfolio risk management
- Proactive program to lower investment & operational risk over the life cycle of all investments
- Trusted Partner to respond immediately in the event of an incident – according to IBM, effective incident response reduces the cost of the incident by +50%
- Managed service that is an extension to the investment managers existing capabilities

Price

- Annual subscription based on size of portfolio
- Services – transparent partner pricing. Lower than what investee companies are able to negotiate individually