Investors Expectation: Cybersecurity engagement

Why engaging on cybersecurity?

Technology is embedded in day-to-day life, and an increasing number of companies depend on digital access to run their businesses. While IT expenditure suffers from year-on-year volatility, the forecast for global IT spending in 2021 was a whopping USD4.2tr[1]. Furthermore, an RLAM analysis of market indexes for the last twenty years, showed that technology is the largest segment of global indexes, swapping places with financial institutions, and as high as it was during the 2000 dot.com bubble. Thus, technology is directly or indirectly a ubiquitous segment of all investors' portfolios.

As businesses become increasingly reliant on technology, cyberattacks have tripled in the last decade, according to the IMF[2]. These actions can impose substantial damages to the corporate targets in the shape of fines, loss of consumer confidence and revenues, and reputational harm. Attention on the matter has also increased across governments[3] some of which had been direct victims of attacks or have been affected indirectly through bailing out or intervening on attacks on commercial entities.

As the ransomware attacks increase in frequency and payout size, investors have responsibility to evaluate the risk in their portfolios, scrutinise their holdings and get reassurance that robust mechanisms are in place to mitigate this risk.

What have we done to date (engagement - phases 1 & 2)?

Our engagement followed the 2019 publication of a call for action on pension funds to consider cyber and data security in their investment

[1] IT budgets - Statistics & Facts | Statista

[2] Cyber Risk is the New Threat to Financial Stability – IMF Blog

[3] Executive Order on Improving the Nation's Cybersecurity | The White House; Cybersecurity | Shaping Europe's digital future (europa.eu)

approach[4]. Since the programme's inception we have targeted over 35 companies for this engagement during two phases since 2019 and have engaged with 65% of them, mostly via meetings, video conferences and two written responses.

We have evolved our understanding of this risk and how in order to mitigate it, an in-depth dialogue rather than increasing general disclosures may be in the best interest of investors. Consequently, we will redirect our efforts on uncovering the leadership and resources that underpin the governance and risk management, corporate culture and systems, with an emphasis on supply chains and corporate action (M&A) as areas of enhanced risk.

What do investors expect companies to do (background for engagement - phase 3)?

As a consequence of our corporate dialogue during phase 1 and 2, we have got a better understanding of the key enablers of cyber resilience. Based on the best practice we have observed, we set up our investors' expectations for phase 3 as follows:

MINIMUM EXPECTATIONS:

- Risk identification and oversight at board level
- A nominated Chief Information Security Officer (CISO) with supporting resources
- Inclusion of cyber covenants in supplier contracts and effective due diligence
- Inclusion of cyber considerations in inorganic growth strategies including in the due diligence and integration phases
- Timely disclosure of cybersecurity breaches
- Disclosures about a cyber resilient culture, to include tailored training across the workforce

[4] Railpen-Nest-Cyber-Security-Report.pdf

ADVANCED PRACTICES:

- Inclusion of information security and cyber resilience in executive compensation KPIs
- Use of NIST Cybersecurity Framework as a reference for cybersecurity risk management
- ISO 27000 for all operations
- Evaluation of cybersecurity in board effectiveness review

Phase 3 will focus on those companies where we deem cybersecurity to be a material risk to our portfolios and where there have either been known breaches or there is a disproportionately low level of disclosure on the approach taken. We aim to report on progress and learnings of Phase 3 within one year of this phase's commencement.