Engagement: CYBERSECURITY

Why cyberattacks are a growing risk to investment portfolios

Cyberattacks have tripled in the last decade as businesses have become increasingly reliant on technology.

As such, and in its role as an active engaged investor, Border to Coast Pensions Partnership has entered a new phase of engagement focused on companies' cybersecurity as part of a collaborative initiative led by Royal London Asset Management (RLAM).

Why do we consider this an important area for engagement?

Technology is directly or indirectly a ubiquitous segment of all investors' portfolios. The forecast for global IT spending in 2021 was USD$4.2trn. Furthermore, an RLAM analysis of market indexes for the last twenty years showed that technology is the largest segment of global indices, taking the place of financial institutions, and as high as it was during the 2000 dot.com bubble.

As such, cyber-attacks pose a significant risk. They 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, 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.

2021 CYBER SECURITY BREACHES SURVEY *

Phishing is the most commonly identified cyber attack. Among the 39% identifying any breaches or attacks, 83% had phishing attacks, 27% were impersonated and 13% had malware (including ransomware).

How have we engaged so far?

Through our collaboration with RLAM, we have supported two phases of engagement so far. This followed the 2019 publication of a call for action for pension funds to consider cyber and data security in their investment approach. Since the programme's inception in 2019, more than 35 companies have been targeted during phases one and two of this engagement with 65% of them engaged with, 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.

* https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

Engagement: CYBERSECURITY

How will future engagement look?

Based on corporate dialogue during phases one and two, the network has developed 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 three 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

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 three will focus on those companies where cybersecurity is deemed 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.

Jane Firth, Head of Responsible Investment, Border to Coast, said: "The digital world is a core part of everyday life, and many businesses are now reliant on digital assets to function day-to-day. As an active steward of our Partner Fund assets, we must recognise the risks that cyber-attacks pose to long-term value and use our scale and influence to ensure our portfolio companies are doing all they can to mitigate these risks. We know we are stronger together and joining an investor collaboration by the weight of RLAM means we have greater power to influence companies to improve.

"Phase three's robust and standardised set of expectations will help both investors and companies understand best practice when it comes to cybersecurity. It also lays out a clear roadmap to success which will lead to more resilient, and ultimately more successful, businesses in the long-term."

Important information

The intention of Border to Coast's Investment Insight and Engagement articles is to present information, data and on finance topics from a diverse collection of sources. This content should not be considered as advice or a recommendation to investors or potential investors in relation to holding, purchasing or selling securities or other financial products or instruments and does not take into account your particular investment objectives, financial situation or needs. All securities and financial product or instrument transactions involve risks, which include (among others) the risk of adverse or unanticipated market, financial or political developments and, in international transactions, currency risk.

Investments in the Alternative products are held within an unregulated collective investment scheme which is not authorised or regulated by the FCA. There are significant risks associated with investment in Alternative products and services provided by Border to Coast. Fluctuations in exchange rates may have a positive or an adverse effect on the value of foreign-currency denominated financial instruments. Certain investments, in particular alternative funds, distressed debt and emerging markets, involve an above-average degree of risk and should be seen as long-term in nature. Derivative instruments involve a high degree of risk. Different types of funds or investments present different degrees of risk.

This content may contain forward looking statements including statements regarding our intent, belief or current expectations with respect to Border to Coast's businesses and operations, market conditions, results of operation and financial condition, capital adequacy, specific provisions and risk management practices. Individuals should not place undue reliance on these forward looking statements. To the fullest extent available by law, Border to Coast accepts no liability (including tort, strict liability or otherwise) for any loss or damage arising from any use of, or reliance on, any information provided, howsoever caused.

Border to Coast Pensions Partnership Ltd is authorised and regulated by the Financial Conduct Authority (FRN 800511). Registered in England (Registration number 10795539) at the registered office 5th Floor, Toronto Square, Leeds, LS1 2HJ