QUILTER CHEVIOT

RESPONSIBLE INVESTMENT

Defending data: Cyber security and critical infrastructure

Across Quilter we have identified three thematic engagement priorities. This is part of our human rights theme.

The idea of human rights is as simple as it is powerful: that people have a universal right to be treated with dignity. Every individual is entitled to enjoy human rights without discrimination – whatever their nationality, place of residence, sex, national or ethnic origin, colour, religion, language, or any other status. Human rights are interrelated, interdependent and indivisible[1].

SDG Alignment

> *"It takes 20 years to build a reputation and a few minutes of a cyber-incident to ruin it."*
>
> Stéphane Nappo, Chief Information Security Officer (CISO) and 2018 Global CISO of the year

The Sustainability Accounting Standards Board (SASB) has highlighted data security and customer privacy as material sustainability issues across critical infrastructure industry groups such as telecommunications (telecoms) and information technology (IT) software, as these businesses hold a wealth of sensitive and personal customer information. Effective cyber security procedures are critical to reducing regulatory and reputational risk, while also enhancing shareholder value. In the 2023 Global Risk Report published by the World Economic Forum (WEF), widespread cybercrime and cyber insecurity were highlighted among the top ten potential risks over the next decade[2]. Increasingly innovative technologies and the proliferation of data collection is likely to lead to companies and individuals being targeted at an unprecedented level. The average annual cost of data breaches in 2022 for companies in critical infrastructure industries was $4.82 million[3]. In addition to the potential cost for companies, data privacy is recognised as a human right by the United Nations (UN).

1 United Nations backed Principles for Responsible Investment
2 WEF_Global_Risks_Report_2023.pdf (weforum.org)
3 OHCHR and privacy in the digital age | OHCHR

Approver: Quilter Cheviot Limited 17 January 2024

Engagement

This engagement programme targeted our most material holdings in the IT software and telecoms industry groups. We completed a risk assessment on the cyber governance of these companies and have used the conversations as an opportunity to establish best practice cyber governance. Using the UN backed Principles for Responsible Investment's (PRI) cyber governance framework, we have evaluated board communication, business continuity, training, and skills and resources. We have also assessed the threat environment to identify current and emerging threats.

Findings

Board communication, skills, and resources: All the companies we engaged with have established a systematic process for regularly communicating cyber security risks to the board. The frequency of these conversations has varied between quarterly, bi-annual, and annual meetings. In some cases, cyber security was on the agenda of all board meetings, so it did not require a separate meeting. With regards to skills and resources, all the Chief Information Security Officers have been involved in the communications to the board. The audit and risk committee are generally seen as having the primary responsibility for monitoring cyber security closely at board level.

The current and emerging threat landscape: The current threat landscape is dominated by the rise of state actors from the outbreak of the war in Ukraine. From BT's internal research, the company has found evidence that these state actors have been actively targeting the company and other telecoms companies, seeking to make financial gain. Some of the other prevalent risks were insider threats, ransomware, and phishing. Regarding emerging risks, a key trend we identified was artificial intelligence and the use of deepfake videos to misrepresent a company. This has not posed a significant threat to any of the companies within this engagement but is expected to present a larger challenge in the future. Vodafone revealed that it expects emerging threats from companies that are using quantum computing. This new technology is being developed to solve complex problems within hours, which would take most current computers several weeks. Quantum computing is still at an early stage and Vodafone's internal research has found it may pose a threat to cyber security due to its ability to bypass encryption security.

Disclosures on cyber security budgets were limited: We did not receive explicit disclosures on cyber security budgets or spend, as this was generally seen as being confidential and non-public information. However, we did receive some useful metrics relating to the growth in overall operating expenses, including cyber security, and some metrics on the number of cyber security employees (see table 1 below), which we have used as a proxy for the cyber security budgets. The best performing companies who have had no significant breaches over the last three years, also had the largest cyber security teams and the faster growth in cyber security budget.

Cyber security training is standard practice: Mandatory cyber security training was the norm across all the companies we engaged with, and this was completed on a quarterly or annual basis by all employees. This training covers topics such as social engineering, phishing and in some cases was delivered through simulations and email alerts. Some companies such as SAP and Sage also have cyber security ambassadors who complete additional training and sit within technical teams.

Company Name	Industry Group	Cyber Security Budget
BT Group	Telecommunication Services	The company employs over 10,000 people in its technology unit and its cyber security budget for 2023 was £20 million.
SAP	Software & Services	Unfortunately, the company would not disclose this number, but the budget grows faster than the overall IT budget.
Vodafone Group	Telecommunication Services	The cyber security budget is embedded across the business, and Vodafone would not disclose how much had been spent. However, using the number of cyber security employees as a proxy for budget, this team has grown by 25% over the past three years from 800 employees to 1,000 which is one of the largest across the industry.
Sage Group	Software & Services	Sage Group has increased the staff in its technology unit by approximately 400% over the last five years. The cyber security budget is managed by the office of general counsel as part of the overall technology budget. This budget covers cyber security which ranges between 5-10% of the overall technology spend.
T-Mobile	Telecommunication Services	Unfortunately, the company would not disclose this information as it is not shared publicly. However, we received confirmation on a $150M budget in incremental spending during 2022-2023. This is court mandated owing to the serious cybersecurity breach.
Darktrace	Software & Services	Unfortunately, the company would not disclose this number, but the budget grows faster than the overall IT budget.
Cellnex	Telecommunication Services	Unfortunately, the company would not disclose this number, but the budget grows faster than the overall IT budget.

Summary

This engagement programme has been used to establish best practice cyber security governance for the IT software and telecoms industry groups. A key element of this engagement was understanding that different companies have different risk profiles; for example, a telecoms company focused on infrastructure and an IT software company have lower risk profiles than a telecoms network provider as the latter has customers. Holding retail customer data makes a company far more attractive to potential cyber security attackers.

Based on the level of disclosure, resource, and performance against the PRI cyber governance framework, and unsurprisingly given its customer facing role, BT is leading the way in setting best practice. The company has not experienced any major breaches in the last five years, and we could not find any cyber security controversies using our internal responsible investment evaluation model. During our meeting with BT, we explored how its approach leads to this outcome, noting of course that the measures that BT has taken would be disproportionate for other companies that do not face the same cyber security threat level. BT has a key role in maintaining the UK's communications infrastructure and therefore has greater resourcing needs. The company is using best practice security standards to protect applications and will constantly monitor threats to gather intelligence and quickly detect and respond to attacks. There is also continuous investment being made into cyber defences and all employees are engaged with regular training. Finally, the company has industry, government and customer partnerships which are used as an opportunity for wider learning. These are some of the main factors being used by the company to maintain its leading position and we would encourage industry peers who face the same threat level to consider this approach. Cyber remains a key investable theme in our portfolios.

Nicholas Omale
Responsible Investment Analyst

Greg Kearney
Responsible Investment Analyst

Ben Barringer
Equity Research Analyst

Matthew Dorset
Equity Research Team Associate

Quilter Cheviot
Senator House
85 Queen Victoria Street
London EC4V 4AB
+44 (0)20 7150 4000

To find out more please contact your investment manager or email: marketing@quiltercheviot.com

quiltercheviot.com