**Cyber Risk – The Elephant in the Board Room**

It is becoming increasingly apparent that Boards need to be able confidently to assess cyber risk with the same, if not more rigour than other risks they analyse and manage. However, recent research[1] shows this is not always the case. While most Boards understand that cyber risk is something of which they should be aware, very few Boards have the knowledge, ability and experience to be able adequately to understand the potential risks. Most non-executives around the Board room table have not grown up in the digital world and, accordingly, are rarely equipped to be able to know the right questions they should be asking and to assess the validity of the answers which they are being given. Conversely, those people who are able to assess cyber risk successfully are equally often lacking in the breadth of skills required to make an effective contribution to the wider variety of topics discussed around the Boardroom table.

In the United States, the regulatory direction of travel is that Boards of listed firms will have to have someone nominated on the Board with cyber security experience to provide adequate oversight[2]. There is also a robust debate taking place between regulators across various fields including the PCAOB, SEC and Capitol Hill on the role Boards play in the management and oversight of cyber security and the liabilities which they may face. One can easily imagine that a similar requirement will come across the Atlantic. The major

[1] Marsh's Global Cyber Risk Perception Survey Report 2019 (Cyber perception survey)
[2] (forbes.com).

question is how such risks can be evaluated and how Boards can become comfortable that they have the knowledge to be confident that the cyber risks are being properly assessed.

The Board needs to be spending, in most cases, significantly more time on the areas of data and data security, especially given the significant liabilities which can attach to a data breach, given the potential damage to a company's P&L and its reputation. For instance, the 2017 attack on Equifax will cost the company some $700 million in fines, with a further $1.25Bn in post incident remediation costs. The credit rating agency Moody's downgrading Equifax in 2019 due to concerns relating to the longer-term impact of the hack. The Information Commissioner's Office in July 2019 announced its intention to fine British Airways and Marriott Hotels a total of £282 million, in accordance with the guidance for data breach fines under GDPR. The consequences of inadequate cyber security are potentially huge, but because it is difficult for most Boards to discuss in detail, it is less often discussed. However, Boards who fail to appreciate the possible consequences of a data breach clearly risk exposing themselves to significant liabilities.

Over the past few years, we have seen an increasing number of non-executive directors brought in to help Boards "understand how to do business in a digital environment". However, just understanding the digital world does not necessarily mean the same thing as being able to help companies assess the digital risk. One could argue that the more important risk for Non-Executives to focus upon is cyber. The costs of implementation and non-compliance are certainly greater. Non-executive directors need to be able to understand what is the critical data which they need to protect. They need to ensure that that data is secure not only within their own ecosystem but also, in this increasingly interconnected world, they must make certain that those people who have access to their systems are themselves secure. There is growing concern that a significant proportion of cyber-attacks are instigated through third parties rather than attacking the end user directly. A company can have all the security which it needs but, if they are interconnected with somebody who does not have proper security, such firewalls are irrelevant. Consequently, the US Department of Defence has implemented a Cyber assessment programme which will mandate the implementation of the NIST cyber security standard across its supply chain. (CMMC). Failure to comply could result in the supplier being removed from any tender process.

Clearly, the responsibility for assessing whether the business is cybersecure rests with the Risk and Governance committees of the Board. However, many Boards lack the knowledge to make such assessments. There is still an on-going debate on the role of cyber security and ideal reporting lines to the Board table. Cyber is an enterprise wide risk, which impacts all aspects of corporate operations. Whilst there is some way to go before the CISO sits at the Board table, there is clearly a need for cyber security expertise to be at the table to provide advice, challenge and oversight on Board decisions. Fortunately, there are steps which a business can take in order to ensure, to the extent possible, its cyber security posture.

Firstly, the business should engage an outside expert to evaluate the security measures in place to protect the organisation. It is not sufficient to rely on assurances given by the CTO/CIO/CISO ("Chief Information Security Officer"), as, in most cases, the non-executive directors (and indeed many of the executive directors) do not have the skill base to be able to evaluate any answers given to them. It is therefore of paramount importance that an outside audit is undertaken.

Secondly, following completion of the audit, and the implementation of any recommendations therefrom, we would recommend that the Board hire an adviser to the Chairman of the Audit/Risk/Governance committee (or wherever cybersecurity falls within the Board committee structure) who has an ongoing responsibility to engage with the relevant executives within the organisation and provide answers to the non-executive directors in a language which they are able to understand. Such individuals will not be full Board members but will be more than purely advisers and will have a long-term relationship with the organisation which allows them to engage, on an ongoing basis, with all relevant people within the organisation to ensure, to the extent possible, that the business is "cybersafe".

Thirdly, to make sure that there are regular external tests and evaluations of the organisation's cyber defences the results of which are reported to the Board, with appropriate commentary from the special adviser.

Tyzack and Parava are working closely to provide a holistic solution to the problems mentioned above. As partners, they are able not only to perform the audit of the company's defences, assess whether the individuals responsible therefore as executives are of the right calibre, make recommendations around cybersecurity generally and, thereafter, ensure that the business as a whole has the requisite executive and non-executive resources to be able to provide comfort to the Board that the organisation is as secure as possible.