MARSH INSIGHTS:

CYBER LIABILITY BOARD EXPOSURE

Recent high-profile cyber events highlight cyber exposures for organisations and their senior executives.

The increasing focus placed on cyber-risk for executives comes as no surprise. Modern businesses rely heavily on computer programmes and the internet to store, transfer, and collate perhaps their most valuable asset: digital data. Even so, the risk of conducting business in this environment is ever-increasing due to the heightened threat of cybercrime, as has been experienced by many high-profile companies in the past year. This risk is particularly relevant for publicly listed companies, where a cyber breach may result in a drop in that company's share price. This leaves the company exposed to regulatory investigations and shareholder litigation, as well as possible reputational damage. Also, company directors and officers could be personally exposed to lawsuits alleging failure to properly put in place and adequately manage the company's systems and controls concerning data usage.

THE RESPONSIBILITY OF DIRECTORS AND OFFICERS

In order to mitigate the likelihood of such litigation, executives need to be aware of their role and responsibilities in relation to the management of cyber-related risk. Global companies often have multiple regulatory regimes to take into account when determining their legal obligations. Management boards should develop cyber strategies which take these legal obligations into account. However, it is becoming clear that such strategies must be more than a box-ticking exercise – the management of cyber risk is now an intrinsic part of day-to-day life for many management boards.

A director may breach his fiduciary duty to the company and its shareholders if they fail to "implement any reporting or information system or controls; or having implemented such a system or controls, consciously fail to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention"[1].

Often the IT and risk management departments of a company will be relied upon to make such decisions, as well as implement them, which could result in a conflict of interest.

Therefore, senior management needs to consider which of those matters should be approved by the management board, and which of those matters it is appropriate to delegate to senior executives. In doing so, boards are better equipped to ensure that the firm's cyber assets are adequately protected by internal controls in the event of any cyber breach. When a breach does take place, the actions of the board may be under scrutiny, so it is important that senior management focus their attention on establishing responsibilities for implementing and managing cyber issues within a company, both before, and after, a cyber event.

HOW WILL A TYPICAL DIRECTORS AND OFFICERS (D&O) POLICY RESPOND?

The consequences of a cyber breach could be extremely costly for companies and their boards. Directors may look to their D&O liability insurance programme to respond to any claim against them.

A typical D&O policy covers individual directors for all acts, errors, and omissions arising from their conduct as directors, which could include matters relating to a cyber incident. Cover may also be available for the company itself in the event of shareholder litigation; however, insureds should ensure that there is no cyber exclusion on the policy which may invalidate cover.

In circumstances where the company is unable to indemnify its directors, or is insolvent, an exclusion of this kind could have serious consequences for directors as they may find themselves with no cover for any cyber-related claim.

Aside from an explicit cyber exclusion, other seemingly-unrelated exclusions may also remove potential cyber cover. For example, typical D&O policies contain a bodily injury and property damage exclusion. Property in this context could include intangible assets – such as digital data – and, if the exclusion is couched in broad terms, cyber coverage may be excluded. Consequently, companies should ensure that if such an exclusion applies to the policy, it applies the narrowest terms possible.

[1]Stone v. Ritter, 911 A.2d 362, 370

While some insurers are now offering cyber extensions to provide affirmative cover, insureds should ensure that these do not inadvertently withdraw cover from other parts of the policy. To provide suitable protection from cyber-risk, a D&O policy should ideally provide cover in the following areas:

- **Investigation costs** – regulatory investigations arising out of a cyber incident, and at full policy limits.
- **Insured individuals** – all persons who are involved in significant cyber-related decisions and implementation on behalf of the company.
- **Investigation of cyber circumstances** – costs incurred investigating any circumstance resulting from a cyber event where litigation is anticipated.
- **Allocation** – clear demarcation between the entity and the individual. The loss attributable to the directors should be allocated appropriately.
- **Shareholder actions** – shareholder actions against the company which arise as a result of a cyber-related incident (for example, following a stock-drop).
- **Reputational damage costs for directors** – costs of mitigating any reputational injury resulting from a cyber incident.

SUMMARY

A cyber event can have a significant impact on a company's reputation and balance sheet. Management boards should be certain of their role and responsibilities relating to preventing and managing a cyber event. Senior executives should take a proactive approach to their insurance arrangements, ensuring that they have adequate cover in the event of a cyber incident, where they may face regulatory investigations or shareholder litigation. They should also check how to access their D&O policy directly in the event of a crisis.

CONTACT

For further information on this subject, please contact:

ELENI PETROS
FINPRO UK
+44 (0)20 7357 1507
eleni.petros@marsh.com

BETH THURSTON
Head of Management Liability
+44 20 7357 1355
beth.thurston@marsh.com

GRAPHICS NO. 15-0482