Understanding cyber Directors & Officers liability risks and buying insurance

INTRODUCTION

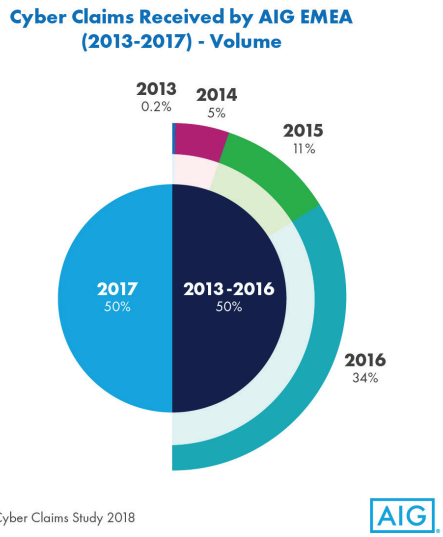
The guide to understanding Directors & Officers Liability risks and buying insurance was published in 2018 by Airmic in association with AIG and Marsh. The guide was designed to help risk managers and the leadership of their organisations navigate these liabilities in an environment of increasingly complex and connected risks.

Airmic is delivering a series of 'Academy Days' focusing on specific areas of risk. The objective of the Academy Days is to provide thought leadership and an opportunity for risk managers to discuss and debate managing risk with their peers. Each Academy Day will be supported by a paper exploring Directors & Officers Liability risks and insurance in the context of the Academy Day subject.

CYBER RISKS AND INSURANCE

Cyber risks are a key topic in many boardrooms and are driven onto the agenda by high-profile data breaches, distributed denial of services (DDoS) attacks, and the rising number of ransomware and cyber extortion attacks. The risk of cyber attack is a constantly evolving threat, and, for most companies, there is a recognition that it is not a case of 'if' but 'when' their organisation will be impacted by a substantial cyber attack. The implementation of the European General Data Protection Regulations (GDPR) in May 2018 has also focused the minds of risk managers and boards on data management and security.

Even before GDPR, the number of cyber claims notified was increasing dramatically. As this data from an AIG claims analysis shows, AIG received the same number of cyber claim notifications in 2017 as in the prior four years combined. Further, based on current data, 2018 notifications are on track to far exceed the 2017 numbers.



Source: AIG Cyber Claims Study 2018

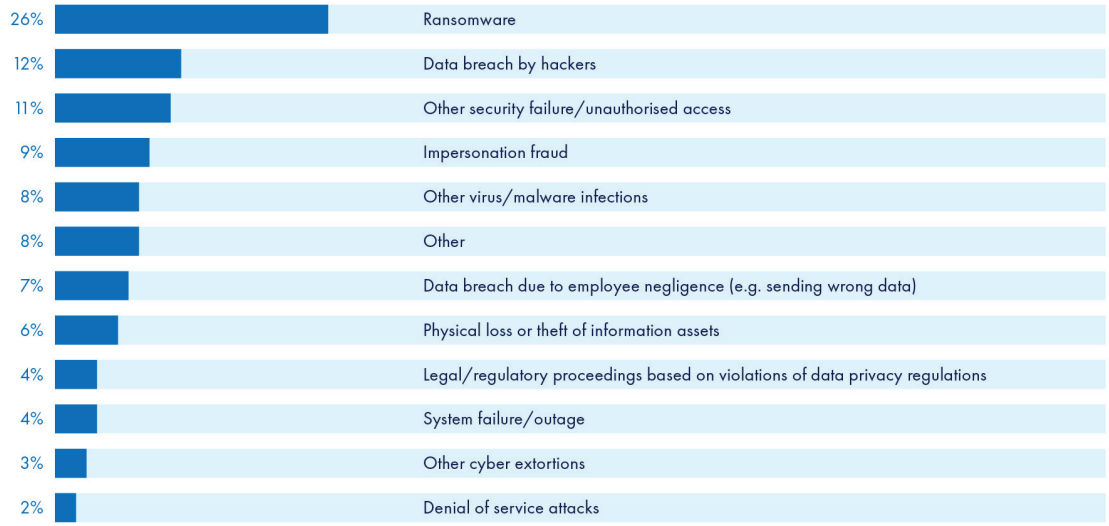
Global companies often have multiple regulatory regimes to take into account when determining their legal obligations for privacy notification. Although many boards understand that cyber breach is a risk management issue that affects the entire organisation and requires board oversight, it is becoming clear that managing risk must be more than a box-ticking exercise – it needs to be an intrinsic part of day-to-day life for management boards and their employees.

When a cyber security breach does take place, the actions of the board and senior management may be under scrutiny. Board members may breach their fiduciary duties to the company and its shareholders if they fail to implement appropriate reporting, system or cyber security, and data protection controls, or if having implemented such systems and controls, they fail to monitor or oversee these. The activity of the board of directors and C-suite management may also come under scrutiny during and immediately after a cyber attack or data breach with regard to how they handle notifying the relevant authorities, the financial markets and persons whose data may be affected. Therefore, it is important that senior management focuses its attention on establishing responsibilities for implementing and managing cyber and data security within a company, both before, and after, a cyber event.

Some boards have done this by appointing a director who comes from a security background. The cyber security board member can help the management team make difficult risk management decisions as well as increase the general level of cyber security knowledge and awareness on the board. Some boards also create a separate committee for cyber risk management. Regardless of whether there is a dedicated board member or committee, boards need to make sure there is sufficient expertise at board level for the board to evaluate and manage cyber risk. In addition, executive management and the board should work together to consider which matters should be reviewed and approved by the board, and which matters can be delegated to other senior executives or committees. Education and training of all company employees and directors also plays a vital role in cyber risk management.

Further, transferring the risk via cyber insurance can also be an effective risk management tool and provide a safeguard against catastrophic loss and the costs associated with a cyber event. The level and scope of cover should be evaluated to ensure that any cyber policy meets the needs of the company and that those within the company who will be first notified of a cyber or data protection breach know how to access the policy.

Cyber Claims received by AIG EMEA (2017) – By reported incident



Source: AIG Cyber Claims Study 2018

AIG

Cyber claims come in many different guises. AIG claims statistics for 2017 reveal the following causes of loss by type:

In addition to ensuring adequate cyber cover is in place, directors may also look to their Directors & Officers Liability (D&O) insurance programme to respond to any investigation or claim against them personally in the event of a cyber event. In order to directly protect the directors and officers of a company in the event of cyber incidents, it is critical to ensure that a company's D&O policy will respond in the event of a regulatory investigation and/or litigation alleging traditional claims for breach of fiduciary duties relating to a cyber event or data breach. 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.

You should discuss what cover is appropriate for your company with an experienced broker who can advise what coverage is available and which insurers have the appropriate expertise. For example, you should consider whether there is cover under the D&O policy 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. As the D&O policy is for the benefit of the individuals, consider how joint costs will be allocated between the cyber and D&O policies. 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 (e.g. following a stock drop).
- Reputational damage costs for directors – costs of mitigating any reputational injury resulting from a cyber incident.

Executives should ensure that there is no overly broad cyber exclusion on the policy which may invalidate cover.

While some insurers are now offering cyber extensions on their D&O policies to provide affirmative cover, insureds should check that these do not inadvertently withdraw cover from other parts of the policy. On a broader level, while the area of potential D&O exposure to a cyber-related claim continues to develop, it is critical to ensure that the company has sufficient D&O limits of liability. Directors and officers should also check that any entity cover on the D&O policy is not so broad as to erode the limits, leaving nothing for the directors themselves, or that they are adequately protected for the worst-case scenario through purchase of Side A only limits which cannot be eroded by the company.

GDPR fines against the company will not be covered under a D&O policy. There is currently no liability for personal fines under GDPR. However, under the proposed clause 189 of the new UK Data Protection Act 2018 (DPA) – which has the purpose of transferring GDPR into UK law – executives will commit a criminal offence under the DPA in circumstances where an offence has been committed by the company and that offence has been proved to have been committed with the consent or connivance, or is attributable to neglect on the part of an executive. Any fines levied against individuals under the DPA are likely to be criminal fines and uninsurable.

As cyber risks continue to grow and their potential impact on the economy increases, organisations will face rising pressures to implement a robust and comprehensive cyber risk management framework. Effective risk management strategies such as appointing a board director to specifically focus on cyber risk, as well as setting up special committees and providing extensive training, can help mitigate this risk. Appropriate insurance such as cyber insurance and D&O insurance can also be deployed by companies and their directors as risk management tools. 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 and the company may face regulatory investigations or shareholder litigation.

How does a cyber event become a D&O claim?

There have been several high-profile cyber incidents that have resulted in shareholder class actions. In one example, an American company became aware of a security failing in March 2017, which it did not adequately and promptly remedy. Suspicious activity was first noticed by the company in late July, with a breach confirmed by the company by 29 July. The company revealed the breach publicly in September and the company's stock dropped over 15% on the announcement. A number of securities class actions were filed against the company and a number of executive officers and directors.

The complaint alleges, among other things, that the company:

- failed to maintain adequate measures to protect its data system;
- failed to maintain adequate monitoring systems to detect security breaches;
- failed to maintain proper security systems, controls and monitoring systems in place; and
- as a result of the foregoing, the Company's financial statements, which said it had systems in place, were materially false and misleading

The class action is currently pending.

In addition, public filings show that a number of senior executives sold shares in early August, i.e. within the period after the data breach had been discovered but before this was publicly disclosed. Although the company has performed an internal investigation and said these individuals were not aware of the breach at the time of the sale, it highlights the importance of making sure systems are in place to ensure possible insider trading is avoided.

View the full directors & officers liability guide here: **airmic.com/DandO**

View the cyber risk governance white paper here: **airmic.com/CRG**