D&O INSURANCE FOR CYBER LIABILITIES: INCREASED CYBER EXPOSURE SHOULD CAUSE DIRECTORS & OFFICERS TO TAKE ANOTHER LOOK AT THEIR D&O POLICIES

Date: 4 April 2018

Insurance Coverage and Global Data Protection, Privacy, and Security Alert

By: Sarah Turpin, Jeffrey J. Meagher

Scarcely a day goes by without news headlines reporting yet another data breach or cyber crime incident, which can have devastating consequences for any business in terms of both reputation and balance sheet. A cyber incident may also have serious additional consequences for the directors and officers of the affected business, including shareholder lawsuits, regulatory investigations and sometimes even criminal investigations. Directors and officers ("D&O") insurance is designed to provide coverage for these types of liabilities, but existing policies may not have been written with cyber liabilities in mind. This article discusses the cyber-related risks directors and officers may face and how their D&O insurance can be set up to respond.

INCREASED CYBER EXPOSURE

Cyber incidents are on the rise with attacks being orchestrated by increasingly sophisticated criminal organisations - sometimes backed by foreign governments - capitalising on vulnerabilities in cyber defences and hijacking companies' networks. Increased reliance on new technologies, cloud computing and mobile banking, and greater connectivity with third party service providers, increases these vulnerabilities and provides additional (and sometimes more accessible) points of entry.

Cyber attacks can impact an organisation in a variety of ways but experience has shown that the costs can be very significant. An annual study conducted by Ponemon Institute and sponsored by IBM Security reveals that the *average* cost of a data breach is currently US$3.62 million globally. One particular attack in 2011 is reported to have cost the company concerned an estimated US$171m and resulted in a £250,000 fine from the UK regulator, the Information Commissioners Office (ICO). The level of fines imposed by the ICO and other European regulators is set to increase significantly from 25 May 2018 when the GDPR (General Data Protection Regulation) comes into effect, introducing compulsory reporting of data breaches involving loss of personally identifiable information. Going forward, such breaches could result in fines of up to €20m or 4% of annual turnover, whichever is the greater. This is in addition to the significant costs likely to be incurred by the organisation in employing cyber security experts to determine the cause of the attack, the implementation of improved cyber security systems, notifying those affected by the data breach and setting up call centres and credit monitoring for their benefit.

ADDITIONAL CONSEQUENCES FOR DIRECTORS AND OFFICERS

It is almost inevitable, where companies experience such significant losses, that criticism will be directed at senior management, particularly given that cyber security is now widely recognised as a boardroom issue. In the US, there have been a number of shareholder derivative actions and securities-related class action lawsuits against directors and officers for alleged failure to take adequate steps to prevent a breach of the company's cyber security defences. For example, last year, shareholders filed a securities-related class action lawsuit against Equifax following the credit monitoring and reporting company's disclosure that it had sustained a data breach involving more than 140 million US customers. Until recently, most of these shareholder lawsuits had been unsuccessful from the plaintiffs' perspective. Earlier this year, however, Yahoo settled a data breach-related securities class action lawsuit for US$80 million. Yahoo's proposed settlement comes on the heels of new guidance from the Securities and Exchange Commission (SEC) that calls on public companies to be more forthcoming when disclosing cyber risks and incidents. Together, these new developments may lead to more shareholder lawsuits in the US.

In the UK, shareholder derivative actions are not common and, while the Companies Act 2006 introduced a statutory framework for such claims, relatively few such actions have been brought. That said, directors and officers may still be at risk of breach of duty claims particularly if the company goes into insolvency as a consequence of the cyber incident. Where the circumstances giving rise to the data breach occur prior to a change in control, former directors and officers may face breach of duty claims for management failings prior to the change.

Another potential concern for directors and officers is that they could be the subject of regulatory investigation or proceedings. In the US, the SEC has already brought several enforcement actions against regulated firms for cyber security failings. For example, in 2016, a prominent financial services firm agreed to pay a US$1 million penalty to settle charges related to its failure to protect customer information, some of which was hacked and offered for sale online. In 2017, the SEC announced the creation of a new cyber enforcement unit, which (combined with the new guidance discussed above) could lead to more cyber-related enforcement actions. In the UK, the Financial Conduct Authority (FCA) has made clear that “cyber risk remains one of the FCA's top priorities” and that what needs to be done to address this is “to ensure that this is regarded as a business-led risk, from the top of the organisation down”[1]. It seems inevitable that, in circumstances where directors or officers are suspected of not having complied with their extensive responsibilities relating to the prevention and management of cyber incidents, they will be personally exposed to regulatory enforcement action.

Directors and officers may even be at risk of criminal action in certain circumstances. In the US, directors and officers may face criminal liability for insider trading if they sell company stock before a data breach is disclosed to the public. For example, federal prosecutors recently announced insider trading charges against a former Equifax executive arising out of the data breach described above. According to the complaint, the former executive sold almost US$1 million worth of company stock two weeks before the massive data breach was disclosed to the public. In the UK, the Data Protection Bill, which is designed to implement GDPR into English law, introduces personal directors' liability, incorporating provisions directly from the Data Protection Act 1998. Where an offence is committed by a company and it is established that it has been committed "with the consent or connivance of or

attributable to neglect" of a director, that director as well as the company will be guilty of an offence. Offenders will be “liable to be proceeded against and punished accordingly”.

HOW D&O INSURANCE SHOULD BE SET UP TO RESPOND

D&O insurance is specifically designed to cover claims against directors and officers for breach of duty and other management failings. At present, it is not common for claims alleging or arising from the failure to ensure proper management of cyber risks to be excluded from D&O policies, but this needs checking particularly as claims exposures increase. In addition, some policies impose jurisdictional exclusions which can prove problematic in the cyber context given the increased risk of liability arising from violations outside the country in which the company operates.

The cover provided by the D&O policy should include claims not only by third parties but by the company, liquidators, administrators and shareholders. In the past, many policies imposed “insured -v- insured” exclusions which were aimed at excluding “collusive” claims designed to take advantage of the D&O cover. Such exclusions are now typically subject to various carve outs or exceptions which are designed to add back cover for certain types of claims. It is particularly important to ensure that cover is available for shareholder actions and other claims brought on behalf of the company especially in an insolvency context.

D&O policies typically provide some cover for regulatory investigations where directors or officers are targeted or required to attend for interview in the context of an investigation of the company. However, the cover may be subject to certain limitations and the coverage triggers may require attention as in practice these often apply fairly late in the investigation process, with the result that preliminary legal costs may not be recoverable unless the policy is suitably amended. Coverage may be provided for civil fines and penalties where insurable in the relevant jurisdiction, although many regulators (including the SEC and the FCA) prohibit regulated firms (and individuals) from recovering any fines or penalties they impose from insurers.

Most D&O policies will cover criminal investigations and proceedings although the cover will be limited to defence costs only. Criminal fines and penalties are excluded as a matter of public policy. An exclusion will generally be imposed in respect of claims arising from dishonest or fraudulent conduct, though that exclusion will typically only apply when such conduct is established by final adjudication. Some policies go further and seek to exclude any misconduct which is deliberate or intentional. The wording of such exclusions requires careful examination. Most conduct is intentional and such exclusions should only apply where there has been an intentional breach of the law. In any event, the policy should make clear, by means of a severability provision, that the misconduct of one director or officer will not impact the cover available to other directors and officers covered by the same policy.

Another important point worth considering when assessing availability of cover in the cyber context is the potential impact of the professional services exclusion. This typically seeks to exclude any claim arising from the provision of professional services, the reason being that such claims will typically be insured under a Professional Liability or Errors and Omissions (E&O) policy. Care needs to be taken to ensure that the exclusion does not affect the ability of the D&O policy to respond where shareholders, regulators or other third parties seek to hold directors or officers responsible for the acts of others providing professional services. Such claims typically involve alleged management failures and it is worth ensuring such claims are carved out of the professional services exclusion. This is particularly important in the cyber context given the potential for data breaches and other cyber

incidents to arise from employee error. If there is evidence to suggest lack of staff training and user awareness then criticism may be directed at senior management as a result.

Finally, cyber claims may arise out of actions by “hacktivist” organizations or government or quasi-government actors. If so, D&O insurers may argue that a war or terrorism exclusion applies unless it expressly exempts cyber-related incidents.

CONCLUSION

Directors and officers face increased exposure to cyber-related liability in the US, the UK and elsewhere in Europe. D&O insurance can help protect directors and officers against such liability, but existing policies may not have been written with cyber and technology related risks in mind. Directors and officers should review their existing D&O policies and request changes aimed at maximising coverage for cyber liabilities, where necessary. Just as directors and officers must adapt to the growing cyber threat, so must their insurance.

Notes:

[1] Speech delivered by Nausicaa Delfas, Chief Operating Officer at the FCA, at the Cyber Security Summit and Expo 2017.

KEY CONTACTS

SARAH TURPIN
PARTNER

LONDON
+44.20.7360.8285
SARAH.TURPIN@KLGATES.COM

JEFFREY J. MEAGHER
PARTNER

PITTSBURGH
+1.412.355.8359
JEFFREY.MEAGHER@KLGATES.COM

