INSURING AGAINST CYBER THREATS GOING INTO 2019

07 December 2018 | London
Legal Briefings – By **Sarah McNally & Sarah Irons**

Cyber remains a very hot topic for all businesses, including in the mining sector. As projects become more automated, the potential for cyber disruption increases. Equally the controls and/or safety systems for a project may be some distance from the project itself, creating risks across a wider geography. Different structures may be put in place to manage data and communications and that may mean data is held with third parties in different geographies. How to ensure those risks are managed robustly and effectively is a key question.

One of the challenges in the event of a cyber incident is the broad range of implications and effects, all of which will require immediate attention and action. We have seen in recent times the media scrutiny which can follow an incident and the pressure which may be created by social media posts from any affected individuals. It is essential both that the internal crisis response team has in mind the insurance implications of any actions or steps the organisation plans to take and that the business is ready for some intense scrutiny of any cover procured.

The issues which will likely need to be considered include the following:

- **Communications:** there will be various communications to consider at the outset of and during an incident. These may include internal communications, communications with customers/clients (potentially responding to social media) and regulators. There may also be a need for market disclosures. These should be prepared in the knowledge of any insurance cover and requirements.

- **Notification:** Notification under any applicable insurance policies should always be a priority. In determining where there may be cover and what policies to notify, organisations should look at their insurance programme holistically both because there can be cover for cyber risks in traditional policy lines, and because cyber incidents can give rise to such a broad range of different risks (such as first party tangible property damage, first party loss of funds, third party liabilities for property or injury, third party liabilities for data breach or financial loss, and first and third party liabilities for losses following outages of production). Depending on the nature of the cyber incident, cover for terrorism and political violence may all need to be considered.

  The key point from a policyholder perspective is to think about the entirety of its insurance suite of policies as a package that needs to operate as a whole to manage these risks. In this regard, scenario planning in advance of any incident would be prudent to ensure that the appropriate cover is obtained, readily understood and available when an incident occurs.Some of the real scenarios that could be faced in 2019 and into the future are not necessarily those of the past.

- **Incident response costs:** It is likely that the business may look to third party providers such as forensic investigators, PR crisis consultants and lawyers to assist in the event of an incident. Insurers' prior consent may need to be sought to the incurring of those costs. The practicalities and terms of such clauses in the cyber context should be considered as part of scenario planning of such risks.

Mining businesses are operating in a rapidly changing world and insurance will only ever be one of many risk litigants when it comes to cyber risks. However pre-planning and analysis is likely to ensure it is as effective as possible in a crisis situation.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

SARAH MCNALLY
PARTNER, LONDON

+44 20 7466 2872
Sarah.McNally@hsf.com

SARAH IRONS
PROFESSIONAL SUPPORT CONSULTANT, LONDON
+44 20 7466 2060
Sarah.Irons@hsf.com

LEGAL NOTICE