CYBER RISK – INSURANCE AS A RISK MITIGATOR IN THE ENERGY AND POWER SECTORS: PART III

In the first article of this series, reference was made to the CyRim report that suggested a concerted global cyber-attack could cost between $85 and $193 billion, whilst also suggesting that only 14% of this amount would be insured.

This low proportion can partially be explained by confusion in the insurance market, over how to offer the correct cyber insurance products at the right price. An understanding of the insurance market's current position on cyber exposure will help energy businesses considering risk mitigation measures.

Non-Affirmative Cyber Cover

The Mondelez case mentioned in the previous article illustrates one category of cyber insurance: so called non-affirmative (or 'silent') cyber cover.

This is where insurance cover is offered either inadvertently, inexplicitly or as a limited extension to an existing policy. For example, a typical property insurance policy may offer cover for '*all risks of physical loss…*' and one could assume that, perhaps following a cyber-attack that resulted in physical loss to a key component, this would be insured. It may equally be (as in the Mondelez case) that cover may be excluded if the loss occurred as part of a systemic 'hostile' attack. Overall non-affirmative cover is not ideal and indicates some laxity by both insurer and insured; even if cover is added to an existing policy, the applicable conditions on the extension of cover (i.e. the small print) will generally be those found on the original, master policy.

During 2018 the UK insurance regulator surveyed cyber underwriting practices and earlier this year wrote to all general insurance firms, outlining its findings and expressing concern about many insurers' unmanaged exposure to policies offering non-affirmative cyber cover. In short, the systemic exposure to insurers from inadvertent cyber insurance cover is a concern and could mean critical infrastructure assets may have inadequate or no insurance cover.

Silent cyber cover is thankfully rare in the energy sector, as most physical damage polices have an explicit cyber exclusion clause that means cyber cover must be purchased separately. Whilst Cyber insurance is a developing sector, some cover is readily available, although often not for very high limits (i.e. financial amounts). For example, cyber liability insurance covers risks such as IT breaches, data theft/loss and ransomware, and is competitively provided; policies may offer several additional benefits including loss of revenue, reputation damage, data recovery and cyber expertise to help with possible claims. However, cover for physical damage as a result of cyber and for cyber losses to the supply chain is more limited because of the obvious systemic risk to the insurer; these exposures will be carefully underwritten and could be expensive.

Conclusion

It is apparent that the cyber risk environment is evolving rapidly, for both the energy sector and the insurance market that serves it; a transparent, competitive insurance market will undoubtedly develop as experience of cyber risk grows. However, despite very high cyber risk awareness in all sectors, confusion over insurance cover is still apparent. In the short term, pending the development of a substantive cyber insurance market, cyber exposure can be managed and mitigated through some simple steps that could include the following:

- Putting cyber awareness at the heart of risk management, with constant review to keep abreast of the fast-moving cyber threat environment.

Prospect Law Ltd
23 Berkeley Square, London W1J 6HE
T +44 (0)20 7947 5354

Regus House, Pegasus Business Park, Castle Donington, Derbyshire DE74 2TZ

@prospectupdate
E info@prospectlaw.co.uk
www.prospectlaw.co.uk

- Auditing key processes and systems to help identify vulnerabilities or weaknesses, or where the greatest exposure lies.

- Considering risk mitigation measures to address these key exposures, including insurance if available.

- Checking all insurances and don't rely on silent cyber cover; instead seek out affirmative, specific new cyber cover.

- If insurance is already in place, checking it is fit for purpose and will respond; challenging brokers and underwriters with loss scenarios to verify this.

- Checking the limits, excesses and waiting periods of all cyber-specific insurances, again challenging the broker or underwriter.

- Considering which extensions, such as legal funding, post-event PR, business interruption or (if available) physical damage would be of benefit.

- Understanding how any claims will be handled before the event and ensure comfort with post-attack procedures; make sure cyber events are part of the Business Continuity Plan.

- Not opting for the cheapest insurance cover; better quality insurance cover provided by more solvent insurers will cost more, but such policies will be more secure and responsive to exposure.

Click here to read the first article in this series
Click here to read the second article in this series

About the Author

Mark Tetley has wide experience gained from senior positions across the London insurance market as both an underwriter and a broker , in a variety of sectors. He provides advice and assistance on a wide range of insurance and risk issues, including comprehensive nuclear liability and property insurance assistance, complex infrastructure project programme design and review, claims and policy reviews, assistance with project insurance design and implementation in developing countries, and many other aspects of risk mitigation.

Prospect Group is an award winning Multi-Disciplinary Practice combining the legal services of Prospect Law with the consultancy services of Prospect Advisory. Our lawyers and technical experts provide a single point of reference for clients involved in energy, infrastructure and other development projects.

This article is not intended to constitute legal or other professional advice and it should not be relied on in any way.

For more information or assistance with a particular query, please in the first instance contact Adam Mikula on 020 7947 5354 or by email on adm@prospectlaw.co.uk.

Prospect Law Ltd
23 Berkeley Square, London W1J 6HE
T +44 (0)20 7947 5354

Regus House, Pegasus Business Park, Castle Donington, Derbyshire DE74 2TZ

@prospectupdate
E info@prospectlaw.co.uk
www.prospectlaw.co.uk