K&L GATES

“Cyber” Insurance Experience

Every company faces cyber risk. Reports of high-profile cyber attacks make headlines almost every day and confirm that cyber attacks are on the rise with unprecedented frequency, sophistication, and scale. And they are pervasive across industries and geographical boundaries.

Insurance coverage can play a vital role in a company’s overall strategy to address, mitigate, and maximize protection against cyber risk. This fact has the attention of the securities regulators in the United States. Amid more frequent and severe cyber incidents, the U.S. Securities and Exchange Commission’s (“SEC”) Division of Corporation Finance has issued guidance on cybersecurity disclosures under federal securities laws, and has advised that companies *“should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents”* and that appropriate disclosures may include, among other things, a *“[d]escription of relevant insurance coverage.”* The SEC’s guidance provides another compelling reason for companies subject to US securities laws to review carefully their insurance programs, evaluate what coverage may already be available under their existing policies, and consider whether any supplementation through cyber insurance products is warranted.

While the newer cyber insurance products can be extremely valuable, including the provision of post-breach services and assistance to the insured, assessing and negotiating these products presents a real and significant challenge. There is a diverse and growing array of cyber products in the marketplace, each with its own insurer-drafted terms and conditions that vary dramatically from insurer to insurer—and even between policies underwritten by the same insurer.

Our insurance team has a comprehensive understanding of both the coverage that may be available to respond to cyber risks under traditional policies, as well as the newer cyber products on the market. We work closely with our clients’ in-house legal counsel and risk management, information technology, compliance, and other personnel in securing insurance coverage for cyber and privacy risks tailored to a company’s specific risk profile, potential exposure, and risk tolerance. We also counsel clients when insurers dispute their obligations to cover cyber and data breach incidents.

We have substantial experience in helping clients structure and negotiate insurance programs to protect themselves from cyber risk, and we have done so for clients in a wide variety of industries, including:

- Banking and financial services
- Manufacturing, including chemicals and metals
- Energy, including utilities
- Transportation
- Telecommunication and Media
- Technology
- Health care
- Outsourcing
- Retail

Among the many issues we negotiate are the scope of coverage for a company’s third-party vendors and outsourcers, including “cloud” providers; the scope of covered personal and company confidential data; and retroactive and extended reporting provisions reflecting the reality that cyber incidents often go undetected for long periods of time.

Our lawyers provide our clients with a cohesive, comprehensive approach to address and mitigate cyber risks and liability through insurance coverage. They are a part of our firm’s leading Cybersecurity and Cyber Law and Privacy, Data Protection and Information Management practice groups.