Cybersecurity, Privacy & Data Protection Alert

February 22, 2018

Recent Conference Highlights Cyber Risks and How to Protect Against the Same

On February 13-14, 2018, Advisen held a conference focused on exploring cyber risks and how companies can best move to address potential exposures. Below are key takeaways and trends discussed by the panelists.

I. **Developing Field for Reputational-Harm Coverage** – Two policies currently exist that offer reputational-harm coverage in relation to cyber incidents. Panelists noted the difficulty that both insured and insurers face in computing reputational-harm claims and the overlap at times between business interruption and reputational-harm coverage. Some attendees noted the difficulty that companies have in finding reputational-harm policies that provide a realistic amount of coverage, with most policies capped at $500,000. At least five additional reputational-harm policies are rumored to be in the works, which could increase competition in the field and help meet what generally remains a gap in coverage.

II. **States Continue to Dominate the Data Breach Context and Are Strengthening Laws** – Forty-eight states now have some form of data breach notification law after New Mexico adopted a new law in 2017. Several states revised their data breach notification laws, or are considering doing so, to strengthen regulations. Typical changes include shorter deadlines for notifications to be sent, new types of information added to the definition of protected information, expanded notification requirements, encryption exceptions, mitigation of harm from breaches and requirements for reasonable security measures. Some states also changed the definition of "breach" to include simple access to data. No panelists expected federal regulation in this area in 2018.

III. **Recent Decisions Suggest Steps to Protect Confidentiality of Post-Breach Materials** – Recent decisions from several federal courts have further defined situations pre- and post-breach where forensic advice may be considered protected by the attorney-client privilege or work-product doctrine. Companies should develop a plan to carefully manage risk and threat assessments and consider bifurcating post-breach forensic and remediation teams. Key steps to consider include having outside counsel engage the forensic firm, including in the scope of work clear indication that the forensic firm will be assisting counsel in providing legal advice and limiting circulation of the final report.

IV. **Standing Remains Threshold Issue** – New case law in leading jurisdictions in the context of data breach litigation has clarified the roadmap for defending civil class actions and derivative actions at the pleading and class certification stages. Defense counsel would be wise to consider standing as merely one threshold issue, along with Rule 12(b)(6) arguments.

V. **Dutch Law Offers Preview of What to Expect from GDPR, High Claims Likely** – Full implementation of the European Union's General Data Protection Regulation (GDPR) is just a few months away. Companies can look to the recently enacted Dutch Data Privacy Law (DPL) for a preview of what to expect from GDPR implementation. More than 5,500 data incidents were reported to the Dutch Data Protection Authority (DPA) in the DPL's first year. Extrapolating a similar rate of filings to the EU generally suggests that there may be more than 150,000 data incidents reported annually. It is unlikely DPAs across the EU will be able to handle such a high volume of complaints, given current staffing levels. This suggests that DPAs may focus their resources on high-worth claims.

VI. **Cyber-Incident Aggregation Concerns Among Insurers** – Insurers at the conference voiced concerns that reliance on cloud storage and computing is concentrating cyber risk in a smaller number of service providers, often within geographic concentrations. Even short outages can take longer to recover from as data flows back up. There is concern in the industry that these concentrations may lead to serious issues should a cyber incident affect a particular industry or geographic area. Companies that use the cloud should scrutinize their vendors and make sure that cloud service providers are using the same, or higher, standards of redundancy and backups as they would use themselves.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha Kohne
nkohne@akingump.com
415.765.9505
San Francisco/Abu Dhabi

Nick Adams
nadams@akingump.com
415.765.9529
San Francisco

Diana Schaffner
dschaffner@akingump.com
415.765.9507
San Francisco

Tylor Dominguez
tdominguez@akingump.com
415.765.9543
San Francisco