Bloomberg Law®

Escalating Cyber Attacks Widen GC Responsibilities

Lisa Singh | March 1, 2019

Recent cyber attacks on major U.S. businesses and government agencies are putting pressure on general counsels to help fortify internal data protocols.

"General counsels must play an active role in supporting senior management and the board of directors in establishing a comprehensive enterprise risk management program, particularly as it relates to addressing legal compliance risks," said Marjorie Loeb, a member of Mayer Brown's corporate and securities practice.

Cross-border breaches, including ransomware attacks, speak to these risks. "General counsels play an essential role in ensuring the establishment and maintenance of applicable legal privileges across jurisdictions," said David Simon, a member of Mayer Brown's global cybersecurity and data privacy practice. Best practices include "employing outside counsel and [ensuring] appropriate markings on all documents and keeping communications to 'need to know' audiences within the business."

Beyond recent attacks against dozens of U.S. corporations and agencies, companies also face the escalating threat of financial liability. Earlier this year, former executives of a major web services provider agreed to pay $29 million to settle assertions they did not live up to their fiduciary duties in safeguarding customer data during cyber attacks between 2013 and 2016.

"In addition to ensuring officers and directors are fulfilling their fiduciary duties and … regulatory obligations with respect to the collection, safekeeping, and use of data in an evolving regulatory environment, [general counsel] play a critical role in incidence response," Loeb said.

Alongside data breach concerns, general counsel must stay apprised of accompanying data laws across jurisdictions. In this environment, effective training of teams is paramount, experts say.

“For general counsels, it will be more important than ever to upskill your people to minimize risk, to have clearly communicated policies in place, and demonstrate effective governance,” said Richard Buchband, senior vice president and general counsel at ManpowerGroup.

Effective measures include “roll[ing] out data protection and information training, including cyber security and GDPR modules, to employees across the world — GCs and their teams must ensure training is understandable, realistic, and relevant to the situations people face every day,” Buchband said. “Ultimately, behaving with ethics and integrity boils down to protecting relationships of trust. Reputational capital remains the most valuable asset a business possesses.”