

Practices & Industries

Data Privacy, Protection & Litigation

Overview

Cybersecurity is a top global risk management issue on the minds of executives and boards of directors. Data breaches have reached epidemic proportions and are not likely to abate anytime soon. Cyberattacks will continue because companies have migrated toward increasing dependence on digital technologies and consistently more sophisticated computer applications to conduct their operations. The challenge for the 21st century is to continue to offer consumer-beneficial technological innovations while also protecting proprietary, confidential and personal information.

At Day Pitney, we believe in providing end-to-end service so our clients are able to confidently address data privacy and protection and cybersecurity risks before these risks ever materialize. We have the capability to cost-effectively review existing enterprise-wide data privacy and protection policies, design and implement new policies when warranted, and plan for the effective management of the crises (and possibly litigation) that might arise as a result of a data breach. Drawing on our broad experiences in law, compliance, information technology, finance and public policy, Day Pitney's Data Privacy, Protection and Litigation practice group is well-positioned to provide sound, innovative advice on continuously evolving cybersecurity and data privacy and protection issues across all business sectors.

Privacy

Day Pitney advises companies across a broad range of industries on data protection and privacy laws, including obligations under the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), the Electronic Communications Privacy Act (ECPA), the CAN-SPAM Act, the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), the Federal Trade Commission Act, Sarbanes-Oxley, breach notification laws, and other federal and state laws. We regularly work with our network of lawyers around the world to advise United States-based companies on the applicability of foreign laws, including European Union directives, laws, and regulations on data protection, privacy, and data retention. We also advise companies on the data privacy and security implications of mergers and acquisitions, outsourcing arrangements, and other transactions.

Managing Cybersecurity Risks Through Preparation, Planning and Training

No matter the size of the business or the computer systems already in place, a data security program is an essential element of enterprise-wide risk management. The new reality is that every business is vulnerable to cyberattack and data loss and is being forced to respond to these risks in what is still a largely unsettled legal environment. Although understanding cybersecurity risks as they relate to your business is a fundamental part of managing your business, the question of how to do so remains a challenging one. Managing your cybersecurity risks requires company-wide policies, careful preparation and rapid response. Day Pitney's attorneys have the experience and flexibility to help you navigate these unpredictable waters. We are well-situated to provide counsel to your business and to help you develop and implement the critical corporate infrastructure, policies, and procedures necessary to protect against, and react to, cybersecurity, data protection, and privacy threats. In addition to assisting with development or review of our clients' comprehensive written information security policies, Day Pitney also assists in implementation by providing on-site and remote training programs for all ranks of personnel, including corporate directors and C-suite officers.

Data Breach and Litigation Response

In the event of a breach, we provide rapid and comprehensive incident response under the protection of the attorney-client privilege. By maintaining close relationships with local, state, and federal governmental agencies charged with investigating data protection and privacy matters and a network of forensic and technical experts, the Day Pitney team can assist in effectively investigating data breach incidents and managing the activities of outside experts and local, state, and federal law enforcement authorities and state and federal regulators. We have advised companies in numerous industries, including retail, insurance, healthcare and financial institutions, in response to breaches. We have assisted these companies in determining the source and scope of the breach, assessing regulatory compliance requirements, managing notifications and call centers, and conducting after-action review. Notwithstanding the best planning and response, data breaches may sometimes lead to litigation. Our cybersecurity team includes litigators who effectively work together to respond quickly to both regulatory investigations and civil litigation that may follow a data breach. Day Pitney has developed a cybersecurity toolkit to help manage the risk of a data breach. The toolkit includes the following components:

- Cybersecurity education briefing for executives, boards of directors, or specific employee groups.
- Interactive workshop – *Beyond the Cloud* – covering best practices in vendor contracting to mitigate cybersecurity issues and their associated risks.
- Incident response plan to activate in the event of a data breach.
- Forensic analysis, notifications, and mitigation responses in the event of a security or privacy incident.
- Self-assessment template based on the Department of Health and Human Services' Office for Civil Rights audit tool to audit data security preparedness where protected health information is handled.