# Cyber Insurance and Data Privacy

In today's technology-driven world, the need for data privacy and cyber security are a concern for all businesses and individuals. At Drew Eckl & Farnham, we maintain a team of attorneys who focus their practice on Cyber Insurance and Data Privacy and Security Compliance. As part of our leading 35 year attorney insurance coverage practice, our cyber insurance team can handle claims and coverage disputes in this highly technical and specialized practice. Additionally, we also work together with our clients to develop and improve data privacy practices and incident response plans for Cyber Insurance, Cyber Privacy and Data Security Exposures.

## Cyber Insurance

On the cyber insurance side, our Cyber Team represents insurers at all stages – from claim analysis and monitoring to coverage litigation or alternative dispute resolution. We advise and represent insurers or their insureds regarding exposures with:

- Defining and analyzing coverage under first-party cyber policies for privacy counsel, forensic investigations, notification costs, credit monitoring, etc.
- Data security-related claims associated with investigations by federal and state regulatory authorities.
- Claims by banks, financial institutions, and other companies or individuals involving large-scale data security breaches involving sensitive health or financial information.
- Claims involving network outages made by third parties against insureds.
- Business interruption claims under cyber policies.
- Ransomware and extortion claims.
- Business email compromise or email schemes and wire fraud under commercial crime insurance policies.
- Claims involving data security and other coverage lines, including general liability, E&O, and D&O policies.
- Exposures of individuals, including directors and officers and attorneys, investment advisors, and other professionals.

## Data Privacy and Security Compliance

On the Data Privacy and Security Compliance side, our DEFCorp Team provides cutting edge assistance to develop and improve client data privacy practices and incident response plans. The goal is twofold: to implement legal measures to minimize the risk of a data breach, and to put our clients in the best position to respond if a breach occurs. In this practice, we:

- Assess risks in connection with ongoing operations, acquisitions, and new service offerings and technology platforms.
- Assess and advise on specific regulatory and contractual data privacy security obligations applicable to a client's business.
- Coordinate communications with company employees, officers, directors, regulators, customers and stake holders.
- Advise on cyber-insurance coverage insurance and exposure.
- Design internal data security structures, policies and practices.
- Integrate response measures to contain breaches, investigate incidents, provide notifications, and communicate with law enforcement and regulators.
- Assist in managing internal investigations.
- Assess and advise on litigation readiness practices.
- Preserve data correctly after a cyber-attack for response to breach-related government subpoenas, investigations and related litigation.
- Deliver required reports to regulators.
- Identify and coordinate with security consultants.