Companies now recognize the immense opportunities—and responsibilities—of data in today’s always-connected world. We partner with you in maintaining the trust of customers, investors and business partners.

Each year, there are more than 1.5 million cyber-attacks on U.S. businesses. Increasingly, these attacks target small and medium-sized businesses, without regard to industry. Perhaps more importantly, everyday access to data can result in losses even without an attack: devices can be lost or stolen, for example; or employees can send an email to the wrong audience. Every data incident has the potential to become a legal matter and can result in financial losses, litigation and erosion of investor and customer confidence. We advise clients on compliance with government regulations, internal assessment and planning, and response to incidents and litigation.

In addition to securing their data, American businesses of all sizes must increasingly focus on data privacy issues. New rules in the US and elsewhere are changing the way we think about data: whose it is and what rights a business has to it. Access to valuable data—your own, your employees’, and your customers’—means that compliance with federal and state privacy laws is becoming increasingly complex. Non-compliance can create significant exposure. We provide industry-specific guidance in health care, financial services, consumer marketing, telecommunications and other segments. We also counsel on use of online and "cloud-based" networking capabilities and the specific risks and opportunities they can present.

Most companies benefit from a cross-functional team, including legal counsel, IT professionals and C-suite executives, that addresses risk management and best practices in order to limit exposure. Our breadth of experience is the perfect complement to your internal cross-functional team. Likewise, we have assembled a multi-disciplinary team of attorneys who work with clients to manage risks in advance of any problems, and respond quickly if an incident occurs.

CRISIS RESPONSE

Even the best-prepared company can experience a data breach. If this happens, it’s important to immediately involve legal counsel. We understand the urgency and broad implications a breach poses to clients. We can manage legal crisis response that coordinates IT measures and outreach to affected parties, lawsuit and claim mitigation, government and regulatory reporting and reputation management.

As part of our crisis response, we will:

- Coordinate with law enforcement investigations,
- Facilitate claims with the cyber-liability carrier,
- Interview forensic experts and IT managers to determine how a breach occurred, what information was compromised and how the company should respond, and
- Provide ongoing advice and counseling to management that addresses legal exposure as well as brand protection.

GOVERNMENT REGULATIONS AND LEGISLATION

Data privacy is an evolving field where companies must comply with laws governing national security, consumer privacy, health care privacy, financial services and telecommunications. Our team collaborates across our other industry-specific practices to guide clients in monitoring new legislation and complying with
the following laws, among others:

- Bank Secrecy Act,
- California Consumer Privacy Act (CCPA),
- CAN-SPAM Act,
- Children’s Online Privacy Protection Act,
- Communications Assistance for Law Enforcement Act,
- Fair Credit Reporting Act,
- Federal Right to Privacy Act,
- General Data Protection Regulation (GDPR),
- Gramm-Leach-Bliley Act,
- Health Insurance Portability and Accountability Act,
- IRS disclosure rules,
- Money-laundering regulations,
- Sarbanes-Oxley Act,
- Telecommunications Act, and
- USA PATRIOT Act.

INTERNAL ASSESSMENT AND PLANNING

The best—and most cost effective—way we can assist clients is to work with them to build privacy and security into their operations. We counsel clients on managing risks with a broad assessment of their data operations, with services that include:

- Auditing privacy and security functions.
- Assessing network architecture, employee policies, website terms and data management.
- Identifying areas of risk unique to a client’s business, such as health care information, payment card data or interaction with children.
- Reviewing contracts with suppliers, banks, customers and other business partners to ensure mutual compliance with contractual and regulatory privacy requirements and allocation of the risks of non-compliance.
- Implementing best practices that avoid exposure and that may provide a legal defense if a breach occurs.

LITIGATION

Each year, there are more than 1.5 million cyber-attacks on U.S. businesses. Victims include some of the biggest names in American business, as well as smaller businesses in every industry. Perhaps more important, everyday access to data can result in losses even without an attack: devices can be lost or stolen, for example. Every data incident has the potential to become a legal matter and can result in financial losses, litigation and erosion of investor and customer confidence. In addition to advising clients on the front end on compliance with government regulations, internal assessment and planning, we also have experience in
Data Security and Privacy

handling responses to incidents and resultant litigation involving cyber-attacks, diversions of funds from hacking, stolen or lost devices, and other episodes. In this area, our attorneys have worked closely with clients that include retailers, service providers and others to prevent and remedy data breaches and have written and spoken frequently on data security and breach issues, including for financial and other professionals.

The ubiquitous use of data in business exposes businesses to claims across the scope of legal practice. We have the resources and experience to represent clients in any area where there are claims related to data security or Internet use, including:

- Harassment,
- First Amendment,
- Libel and defamation,
- Infliction of emotional distress,
- Breach of privacy,
- Trade disparagement,
- Copyright infringement,
- Breach of contract,
- Breach of security,
- Misrepresentation, and
- Tortious interference.

PRACTICE HIGHLIGHTS

**Information Security and Governance Audits.** Advise on legal risks associated with penetration testing, gap assessment, and information governance audits and assessments, both internal and third-party.

**Breach Response.** Oversee all elements of response to a data incident, including coordination with forensic investigators, law enforcement, communications, and insurance provider.

**CCPA.** Advise on CCPA readiness and draft appropriate policies.

**Data processing arrangements.** DPAs and other data processing arrangements for retailers, service providers, B2B information technology companies, staffing companies, and other sectors.

**Privacy and security warranties.** Evaluation of privacy and security commitments in diligence and sale of privately-held enterprises.

**GDPR.** Assess GDPR readiness and provide ongoing counsel.
Data Security and Privacy

**IoT/Smart device launch.** Advise global appliance manufacturer on IoT/smart device launch.

**Data processing agreements and cross-border transfers.** Advise on data collection, processing, and transmission regarding domestic and international operations, including use and sharing of employee data, consumer data, and business partner data gathered via “smart” devices, in connection with marketing efforts, and through service provider relationships. Advise on creation and use of aggregated, anonymized, and deidentified data.

**Breach of credit card information.** Respond to breaches of client credit card information in multiple states; research state requirements and interface as required with state law enforcement officials or others.

**Privacy Policies.** Creation and review of privacy policies and procedures for media, healthcare, retail, service, and other clients in conjunction with findings from security audits and pursuant to emerging regulations such as the CCPA.