

Cybersecurity and Data Privacy

We have a multi-disciplinary cybersecurity team with many years of experience in health care, information technology, commercial transactions, commercial finance, manufacturing, insurance, intellectual property, and data privacy. Our attorneys proactively work with clients to assess their current and future cybersecurity and data privacy needs while minimizing financial and operational risk. In the modern economy, threats to data security have real costs – the cost of an average data breach to a U.S. company ranges from \$3-7 million according to leading studies. And, a successful ransomware attack or other data breach can bring a string of lawsuits and government investigations. At Chambliss, our job is to do all we can to ensure every client is taking necessary precautions to protect their valuable information and minimize their risks.

Our team advises clients on:

- current and changing data regulations;
- cybersecurity risks and protocols;
- incident response plans;
- cyberattacks;
- cyber-related disputes and litigation;
- privacy and data security issues in mergers, acquisitions, or joint ventures; and
- cyber insurance coverage.

In cybersecurity and data privacy, a one-size-fits-all solution is not the answer. Our team partners with clients to identify their unique data and privacy issues, and we deliver tailored solutions to fit their particular business models and goals.

Every organization has valuable data to protect. Regardless of size, industry, or business model, entities are coming to grips with the vast amount of data that computerization and technology have created. This includes data related to employees, patients and consumers, vendors, clients, and intellectual property, as well as the ever expanding flow of data known as the "internet of things," in which everything from light bulbs to forklifts are connected to networks.

Even as technological advances allow companies to be more nimble, mobile, targeted, and efficient, they have made businesses of all sizes vulnerable to cyberattacks like never before. And, cyberattacks have become more sophisticated and wide-ranging, adversely affecting businesses as diverse as mom-and-pop corner groceries and international shipping giants.

Ransomware attacks can cost companies thousands to millions of dollars per day as key business lines are interrupted for days or weeks. For personal confidential information – of consumers, employees, or third party customers – the average cost is \$125 to \$150 per confidential record. In health care, the average cost is even higher – around \$200 to \$250 per patient record. Our attorneys serve as trusted advisers to minimize these data risks, allowing clients to focus on running their businesses in secure environments without undue disruption.