

## Cybersecurity and Data Privacy

### Overview

**Virtually every company, organization and institution, regardless of size, has an aggregation of information that is of critical value to its mission.**

Unfortunately, we are in an age where that information is under an ever-increasing cyber threat. Data concerning clients/customers, employees, finances, intellectual property and strategic plans are made vulnerable by their accessibility via unsecured mobile devices, e-mail scams, third-party connectivity (i.e., payroll administrators), and out-sourced storage (real or virtual). Furthermore, as technology evolves, so do the laws, regulations and compliance requirements related to the protection of privacy and data, which increases the burdens on institutions of all natures and sizes as well.

The members of Bond's cybersecurity and data privacy practice are residents of the full range of Bond's diverse practice areas, and thus draw from the firm's collective wealth of experience in governance, compliance, and litigation across a wide array of industries and markets. The attorneys in the group provide insight into cybersecurity and data privacy matters concerning business transactions, compliance, information management, governance, human resources, intellectual property, litigation and technology.

Collectively, they possess an extensive reservoir of practical knowledge having counseled a wide range of clients including:

- Defense
- Education
- Energy
- Finance
- Health Care
- High-Tech
- Hospitality
- Insurance
- Manufacturing
- Municipalities

The multi-disciplinary group has experience with counseling clients on compliance with federal and state privacy laws, including HIPAA, FERPA and the Gramm-Leach-Bliley Act, as well as federal and state data breach notification laws. The members of the practice also assist clients in navigating cyber threats and on-going challenges by:

- Developing tailored policies and guidelines for client cyber governance, data breach preparedness, and compliance with federal and state notification and accountability laws;
- Advising clients of potential and actual liabilities for data breaches, security failures, and counteroffensive measures; and
- Assessing clients' vulnerabilities and risks, auditing existing incident response plans, procedures and protocols, and recommending improvements.

### Primary Office Contacts

#### Buffalo, NY

Joseph P. Kubarek

#### New York, NY

Tracy E. Miller

#### Rochester, NY

Edward P. Hourihan, Jr.

#### Syracuse, NY

Philip J. Zaccheo

- Social Services
- Software
- Retail
- Transportation
- Utilities