

Data Security & Privacy

Cyber intrusion and attacks have increased at an alarming rate in recent years. Twenty-first century data breaches involve sophisticated attacks on the network and information systems that form the infrastructural foundation of modern commercial and corporate activities for companies of all sizes and across industries. It's no longer a question if a data breach will occur, but when.

Bracewell works with energy companies and utilities, retail companies, financial institutions, investment advisors, and local and state municipalities on developing and implement information security plans to mitigate and minimize risks. We also help insulate senior management from the regulatory and shareholder scrutiny that inevitably follows a breach.

Our team — which includes former prosecutors, seasoned civil litigators and strategic communications veterans — puts an emphasis on preemptive planning to streamline the time and expense of a response effort. We help companies put a response plan in place that can be implemented on a moment's notice, including media and governmental outreach to reduce financial, regulatory and reputational repercussions.

Key Contacts



Seth

Partner

NEW YORK +1.212.508.6165

seth.ducharme@bracewell.com

Experience

We have represented a variety of clients on sensitive and confidential matters involving data security and privacy.

Global asset firm

- on its information security policy and incident response plan

International energy company

- after it was victimized by an email compromise scheme

Oil and gas exploration and production company

- on cyber preparedness matters, including an incident response plan and information security policy

Privately owned real estate firm

- on its information security policy and managing the fallout after the loss of personally identifiable information

Public water and waste water services district

- after it was victimized by an email compromise scheme

Real estate investment firm

- on notice obligations after it was victimized by a cyberattack

Retailer

- in government relations and strategic communications after the detection of an external data breach