ENCOMPASS

Cybersecurity & Data Breach Response

Integrated tactics address preventive & responsive measures

Whether you are seeking to

- develop or assess data security and governance practices
- implement investigative and response measures in response to a cyber attack
- communicate with law enforcement or regulators regarding a data breach, or navigating lawsuits relating to cybersecurity

our team can guide you step by step.

We help clients manage

- Business and reputational risks
- A changing regulatory landscape
- Sensitive internal investigations
- Board-level and customer communications
- Law enforcement and government relations
- The interplay with a data breach and related litigation

A wide level of experience and diverse perspectives

- Former senior in-house counsel (including individuals in compliance and privacy roles)
- Government prosecutor
- Military service
- Enterprise-wide electronic discovery counsel for clients with global operations — Class action and multidistrict litigation defense counsel
- Insights from internal investigations on behalf of the company and the Board

Related Capabilities

Data Collection, Processing & Production

E-Discovery & Review Counsel – Investigations

E-Discovery & Review Counsel – Litigation

Enterprise Data & Mobile Device

Enterprise E-Discovery Counsel

Hosting & Migration

Litigation Readiness

Predictive Coding & Analytics

Records & Information Governance

Review

Second Requests

Strategic Advocacy

ENCOMPASS

Our clients span industry sectors

- Fortune 50
- Privately held companies
- Businesses with global operations
- Heavily regulated companies

Some clients have in-house multidisciplinary information governance teams, and others have a designated professional leading information security and data protection efforts.

Make careful, timely, and informed decisions

Develop defensible strategies regarding internal investigations, response and data protection, preservation and litigation readiness measures, and communications with the Board, regulators, customers, and law enforcement.

Our cybersecurity and data breach response services allow you to:

- **Assess risks** in connection with ongoing operations, acquisitions, and new service offerings and technology platforms
- **Complete transactions** by setting information lifecycle governance systems
- **Coordinate communications** with the Board, law enforcement, regulators, and customers
- **Define insurance coverage solutions** that match your exposure and analyze cyber-insurance coverage after a breach
- **Design data security structures,** policies, and practices
- **Integrate response measures** when it is time-sensitive to contain breaches, investigate incidents and notify customers, communicate with law enforcement and governments
- **Launch internal investigations**
- **Manage crises** when faced with breach-related government investigations
- **Mitigate the problem** with risk assessment and litigation readiness practices
- **Preserve data correctly** after cyber attack or in the face of breach-related government subpoenas, investigations and related litigation
- **Report to regulators**
- **Retain a security consultant** and also your client privilege

Why Nelson Mullins Encompass?

- A practical business mindset
- Integrated information governance services
- Multi-disciplinary team
- Predictability and cost efficiency
- Relationships with law enforcement, public relations and government professionals, and the communities in which we do business

Experience

Following is a selected sampling of matters and is provided for informational purposes only. Past success does not indicate the likelihood of success in any future matter.

Discovery Counsel in a data breach MDL for a number of companies facing hundreds of putative class actions related to a large cyberattack with extensive concurrent federal, state, and congressional inquiries. Our representation includes advising clients on all phases of discovery; handling the complex, large-scale review and production; 30(b)(6) deposition preparation and defense; and coordination with law enforcement.

- Counseled financial institution and payment processing vendor through all stages of data breach incident involving the loss of sensitive customer data, including incident analysis and breach containment, incident disclosure (i.e., notification in compliance with all regulatory requirements), loss mitigation, and remediation customized to meet each client's specific business and industry requirements
- Counseled major national retailer through a security incident investigation involving the discovery of malware potentially compromising all credit card processing of the company, compliance, risk assessment, and remediation
- Counseled an international construction company and hotel portfolio management company through a breach investigation, response and notification involving the theft of employee W-2 tax information obtained as a result of phishing scheme
- Counseled the domestic subsidiary of a major international company through a security incident investigation involving employee theft and misappropriation of customer credit card information
- Counseled a small accounting firm through a data breach investigation involving the release of sensitive customer information to unauthorized recipients and customer notification