OSLER

SERVICE

Cybersecurity and Security Incident Response

Navigate data security incidents with confidence.

Related Expertise

- Class Action Defence
- Corporate and Commercial Disputes
- Privacy and Data Management
- Privacy and Data Security Disputes

Recent high profile security breaches have served as a wake-up call for organizations. The increasing breadth and sophistication of cyber attacks have led companies from across the full spectrum of industries to place a renewed emphasis on protecting confidential data such as credit card information, health care data and social insurance numbers.

Data breaches can have significant consequences for an organization – including reputational damage and potential class action lawsuits as well as the associated financial costs of both – leaving senior executives and boards of directors justifiably concerned about their company's level of cybersecurity preparedness. The ongoing threat of a data breach has opened the door to a series of questions for these organizations: Do we have safeguards in place to prevent a data breach? Are we prepared if we have one? How will the company survive an incident?

Osler has the answers companies need. Our industry-leading Privacy and Data Management team has extensive experience dealing with security incidents arising from a broad range of circumstances, and regularly helps organizations to prepare for security incidents and, in particular, to develop the security incident response protocols they need to protect their confidential and private data.

Security Incident Management

When a company experiences a cyber attack, it's critical to engage a team of experts that can provide the support and guidance necessary to manage the security incident and the subsequent consequences. Osler's lawyers have acted on many of the largest and most significant Canadian security incidents and regulatory investigations to date, assisting with breaches related to a variety of situations, including

- state sponsored and politically motivated (e.g., Anonymous) cyber attacks
- misplaced or stolen devices (e.g., laptops, USB keys) containing personal information
- data extortion
- misdirected mail and email
- rogue employees or contractors

Security Incident Support

Dealing with security incidents effectively typically requires support on multiple fronts. Osler's experienced team can assist with

- providing direction for internal and external forensic investigations
- advising on private sector and health sector statutory reporting and notification obligations and best practices, including an assessment of "real risk of significant harm" in the circumstances and the new security breach notification regime under the *Personal Information Protection and Electronic Documents Act*
- offering guidance on privacy regulatory authority expectations and liaising with privacy authorities
- crafting the narrative for verbal and written reports to applicable privacy regulatory authorities
- drafting notifications to affected individuals
- liaising with credit monitoring, forensic experts and other key service providers
- drafting FAQ and other public facing statements
- managing any privacy regulatory authority investigations
- acting on litigation proceedings

Security Incident Readiness

Adopting a proactive approach to security incident response can be invaluable to organizations and will ensure they are prepared in the event of a breach. Members of Osler's Privacy and Data Management team work regularly with organizations to develop, test and otherwise enhance their security incident response protocols, and assist with integrating security incident response into companies' broader data governance frameworks.

Litigation Management

Osler's Privacy and Data Management lawyers work closely with our National Litigation Group and our Class Actions specialty group. Our litigation group has wide-ranging experience on privacy-related proceedings and Osler's team is currently acting for a number of high profile clients on privacy class actions that have been filed in Canada.

Representative Mandates

Our Privacy and Data Management team's representative security incident mandates include acting for

- a large American retailer in connection with a security incident involving millions of credit card records and email addresses
- a multinational financial services company in a cybersecurity incident involving millions of email addresses
- an American retailer regarding the joint investigation by the Office of the Privacy Commissioner of Canada (OPC) and the Alberta privacy regulatory authority in connection

with the cybersecurity incident involving millions of payment card records
- a global technology and entertainment company in connection with the joint queries by the OPC, Alberta, BC and Québec privacy regulatory authorities in connection with the cybersecurity incident involving millions of customer records
- a social networking site in connection with the joint queries of the above-noted Canadian privacy regulatory authorities relating to the cybersecurity incident involving the theft of millions of member passwords
- an online company in connection with the cybersecurity incident involving millions of member passwords and other data
- a multinational software company regarding the joint investigation of the OPC and the Irish Data protection authority in connection with the cybersecurity incident involving millions of user accounts
- a social networking site on numerous investigations (including an investigation involving a security incident) by the OPC

Key Contacts

Adam Kardash
Partner, Privacy and Data Management, Toronto

Tina Saban, CIPP/C
Associate, Privacy and Data Management, Toronto