Cybersecurity & Data Privacy

In our interconnected era – marked by pervasive cyber-threats and data security concerns – protecting both company and customer information is a foundational requirement for public and private firms.

Cahill advises its clients across all aspects of their electronic security and privacy needs, assessing cyber-risks and consumer protection, as well as addressing compliance and regulatory requirements. We ensure clients understand government standards and industry best practices and then deliver the concrete, actionable solutions best suited to their unique business operations, including the security and privacy aspects of corporate transactions, corporate governance and cross-border data transfers.

Our unparalleled experience is enhanced by our due diligence partnerships with leading global investment banks – advising them with respect to the practices at hundreds of different companies annually. As a result of these comprehensive privacy and cybersecurity audits, our team is uniquely positioned to benchmark strategies across a wide variety of industries and geographies and then develop policies and procedures to secure our clients' protected data in compliance with the latest rules in this fast-evolving area, including the new General Data Protection Directive ("GDPR") regulations relating to EU citizens.

Cahill's information security and privacy team is available to:

- Analyze the jurisdictional and territorial reach of privacy laws and regulations, including the GDPR, to assess the applicability and scope of obligations for companies with a global presence;
- Deliver advice on best practices for security, privacy and breach notification, including through comprehensive privacy and cybersecurity audits;
- Build incident response policies and strategies to manage related activity and resolve concerns;
- Establish processes to permit the transfer of personal data between companies and across international borders;
- Develop corporate governance practices, including advice regarding employee training, the appointment of data protection officers, and lines of reporting and responsibility;
- Provide M&A diligence related to privacy and data protection risks, including drafting of security representations, warranties and other clauses in M&A and other commercial transactions;
- Analyze data processing vendor agreements, and the risks associated with outsourcing data processing tasks;
- Review de-identification and anonymization policies and practices and compliance with evolving regulations and interpretations.