Bulletin | Cybersecurity, Privacy and Data Protection

February 2023

Managing privacy and cyber risks in M&A transactions

Privacy and cyber risks are essential considerations for almost all merger, acquisition and financing ("M&A") transactions. Privacy and cyber risks can affect the viability and value of a transaction, influence the nature and terms of a transaction and, in some circumstances, cause the parties to abandon a transaction. In addition, parties to an M&A transaction and their directors and officers (if applicable) might be legally obligated to address privacy and cyber risks in connection with the transaction and incur potentially significant liabilities if they fail to do so. In Canada, privacy and cyber risks regarding M&A transactions will soon increase significantly as a result of the modernization of Canadian privacy and cybersecurity laws. For those reasons, parties to an M&A transaction should appropriately address privacy and cyber risks throughout the transaction life cycle.

Understanding privacy and cyber risks

Privacy and cyber risks are relevant to every organization, regardless of size, industry or public profile, because all organizations (directly or indirectly through their business partners and service providers) use or depend on information technology systems and data (including personal information) for their day-to-day operations.

Privacy risks are risks of losses and costs/liabilities suffered or incurred by an organization as a result of a failure to comply with privacy laws regarding the personal information in the organization's custody or control (including personal information processed by the organization's service providers). Privacy laws impose restrictions and requirements on organizations regarding their collection, use, disclosure and retention of personal information, including requirements for safeguarding personal information and reporting personal information security incidents. Contraventions of privacy laws can result from various causes, including an organization's failure to establish and effectively implement a legally compliant privacy management framework.

Cyber risks are risks of losses and costs/liabilities suffered or incurred by an organization as a result of a cybersecurity incident (i.e., an incident that adversely affects the information technology systems used by or on behalf of the organization or its business partners and advisors or the confidentiality, integrity or availability of data, including personal information, in the organization's custody or control). Cybersecurity incidents can result from internal sources (e.g., employees, contract workers, and system failures) or external sources (e.g., nation-states, terrorists, competitors, hackers, and fraudsters).

Losses caused by a contravention of privacy laws or a cybersecurity incident can include business disruption loss, loss of (or inability to use) critical data, loss of revenue and other financial loss, brand depreciation, and harm to reputation and customer loyalty. Costs and liabilities resulting from a contravention of privacy laws or a cybersecurity incident can include incident response, remediation and reporting/notification costs, regulatory investigation costs, litigation costs (including privacy class actions), regulatory fines/penalties, and financial liabilities to customers and business partners.

Privacy and cyber risks will soon increase significantly as a result of the modernization of Canadian privacy and cybersecurity laws to give Canadian privacy commissioners and other regulators robust enforcement powers, including the authority to conduct investigations, make binding orders, enter into compliance agreements, and impose or recommend multi-million dollar administrative monetary penalties. In addition, certain statutory contraventions will be quasi-criminal offences punishable by multi-million dollar fines. See BLG bulletins *Québec adopts Bill 64 – Key requirements for businesses*, *Canada's Consumer Privacy Protection Act (Bill C-27): Impact for businesses*, *Special committee recommendations to modernize B.C.'s private sector privacy law*, and *Bill C-26: New Canadian critical infrastructure cyber security law*.

Privacy and cyber risks and M&A transactions

Privacy and cyber risks are relevant to almost all M&A transactions and important to all transacting parties (e.g., buyers, sellers, and lenders/investors) for both business and legal compliance reasons. Well-known M&A transactions that have been adversely affected by privacy/cybersecurity incidents include:

- **Verizon/Yahoo!**: Privacy/cybersecurity incidents at Yahoo! discovered before the completion of Verizon's USD $4.83 billion acquisition of Yahoo! resulted in a USD $350 million reduction in the purchase price and an allocation to Yahoo! of liability for costs resulting from the incidents.
- **PayPal/TIO**: A privacy/cybersecurity incident at TIO discovered after PayPal's CAN $302 million acquisition of TIO resulted in PayPal shutting down TIO's services and winding down TIO.
- **Spirit AeroSystems/Asco**: The terms of Spirit's proposed acquisition of Asco were substantially amended after a ransomware attack disrupted Asco's business. Ultimately, the transaction was cancelled.
- **Marriott/Starwood**: A privacy/cybersecurity incident at Starwood Hotels that began two years before Marriott's USD$13 billion acquisition of Starwood (as a result of a share purchase) and was not discovered until after the acquisition was completed resulted in a £18.4 million fine imposed on Marriott by the U.K. Information Commissioner's Office, an investigation of Marriott's personal information practices by the Office of the Privacy Commissioner of Canada and class-action lawsuits.
- **CafePress/PlanetArt**: A privacy/cybersecurity incident at CafePress that was resolved and reported a year before CafePress' assets were purchased by PlanetArt resulted in a U.S. Federal Trade Commission investigation and consent orders against each of CafePress and PlanetArt more than a year after the transaction.

Business considerations

Privacy and cyber risks can dramatically reduce the present and potential future value of the business or assets that are the subject of an M&A transaction and impose potentially significant costs (e.g., costs of improving privacy practices, correcting cybersecurity deficiencies and responding to regulatory investigations and legal proceedings) and liabilities (e.g., regulatory fines/penalties, settlement payments and litigation judgments) on the transacting parties after the transaction is completed. Certain assets (e.g., brand and customer goodwill) can be particularly vulnerable to harm caused by a privacy or cybersecurity incident. In some circumstances, significant privacy or cyber risks can cause the parties to negotiate substantial changes to the value and structure of a proposed M&A transaction or to abandon the transaction. Privacy and cybersecurity incidents can also impair the transacting parties' ability to negotiate and complete an M&A transaction.

Legal compliance considerations

Failure to appropriately address privacy and cyber risks in connection with an M&A transaction can expose the transacting parties, and in some circumstances their directors and officers, to potentially significant legal compliance costs and liabilities after the transaction is completed. Common legal compliance considerations include obligations under privacy laws, industry-specific cybersecurity laws, corporate directors' and officers' duties of care, reporting issuers' continuous disclosure obligations, and contractual obligations.

Privacy laws

Canadian privacy (personal information protection) laws regulate the collection, use, disclosure, and retention of personal information by private sector organizations in Canada. The laws also impose restrictions and requirements for sharing personal information in connection with a prospective or completed M&A transaction. In addition, the transfer of legal or practical control over personal information in connection with a completed M&A transaction can result in the transfer of accountability for the personal information and expose the transacting parties to potentially significant legal compliance costs (e.g., costs of changing personal information practices and improving personal information

safeguards) and liabilities (e.g., liabilities to individuals and organizations affected by a personal information security incident and administrative monetary penalties and fines imposed under modernized Canadian privacy laws).

Industry-specific cybersecurity laws

Canadian organizations may be subject to industry-specific laws and regulatory requirements regarding cybersecurity. For example, financial industry regulators (e.g., the Office of the Superintendent of Financial Institutions, the British Columbia Financial Services Authority and the Investment Industry Regulatory Organization of Canada) have issued cybersecurity guidance and imposed requirements for reporting cybersecurity incidents. Proposed new Canadian cybersecurity laws will require organizations in certain industries to comply with minimum cybersecurity standards.

Corporate directors' and officers' duties

Under Canadian law, corporate directors are obligated to manage or supervise the management of their corporation's business and affairs, and corporate officers are responsible for their corporation's day-to-day operations. Canadian regulators and authoritative organizations have emphasized that corporate directors must be engaged and take an active role in their corporation's privacy and cyber risk management activities, and must ensure that corporate officers have properly implemented appropriate policies and practices to manage privacy and cyber risks and respond to privacy and cybersecurity incidents. Corporate directors' and officers' responsibilities regarding risk management include managing privacy and cyber risks in connection with M&A transactions. Failure to do so might not only result in harm to the corporation but also expose its directors and officers to potentially significant liability.

Reporting issuers – continuous disclosure obligations

Canadian securities laws require reporting issuers (i.e., corporations whose shares are publicly traded) to make continuous disclosure of material information about their business so that investors have equal access to information that might affect their investment decisions. Continuous disclosure obligations require timely disclosure of material privacy and cyber risks and incidents. Those obligations might require a reporting issuer participating in an M&A transaction to identify and assess the privacy and cyber risks associated with the transaction and accurately describe those risks in the reporting issuer's continuous disclosure documents.

Contractual obligations and quasi-contractual assurances

Commercial agreements (e.g., supplier agreements, service provider agreements, and merchant agreements) often impose contractual obligations to protect personal information and other data (e.g., business data, customer data, and cardholder data) and report data security incidents. Privacy and cybersecurity obligations might also result from quasi-contractual assurances given by an organization in various kinds of published notices and policies (e.g., privacy statements) and promotional communications. The parties to an M&A transaction should consider the privacy and cyber risks resulting from those obligations.

Managing privacy and cyber risks in M&A transactions

There is no one-size-fits-all solution for effectively managing privacy and cyber risks in connection with an M&A transaction. The importance of privacy and cyber risks to an M&A transaction, and how the risks might be addressed and allocated effectively and appropriately, will depend on the circumstances, including:

- the nature of the transacting parties and their business structures;
- the industries and legal jurisdictions in which the parties operate;
- the kind of transaction (e.g., asset or share purchase);
- the nature, amount, and timing of the consideration paid;
- the nature and importance of the parties' respective information technology systems and data (including personal information);
- the parties' post-transaction plans;
- the parties' risk tolerance; and
- whether the parties intend to obtain representation and warranty insurance.

To effectively manage privacy and cyber risks in an M&A transaction, the transacting parties and their advisors should consider privacy and cyber risks throughout the transaction life cycle – deal processes, due diligence, transaction agreement, and post-transaction activities. Following are some comments and recommendations.

Deal processes

The deal processes used by transacting parties and their advisors to negotiate and document an M&A transaction can present potentially significant privacy and cyber risks. For example: (1) technologies used to share confidential documents and information regarding a transaction can be hacked or harmed by malware or ransomware; (2) the security of deal-related communications can be compromised; (3) the parties' representatives and other personnel can be deceived by fraudulent messages; and (4) the documents and information disclosed during negotiations often include personal information of employees, customers and other individuals. For those reasons, the parties to an M&A transaction and their advisors should implement appropriate agreements (e.g., confidentiality agreements that contain provisions prescribed by Canadian privacy laws) and security controls (e.g., secure online data rooms and communication protocols) to mitigate privacy and cyber risks inherent in M&A deal processes.

Due diligence

M&A due diligence refers to investigations and assessments of a transacting party and its business and assets to discover and verify information relevant to a proposed transaction and identify and assess risks associated with the proposed transaction. Customary M&A due diligence will usually identify some privacy and cyber risks. Nevertheless, for most M&A transactions it will be appropriate to engage in due diligence specifically directed to privacy and cyber risks to obtain the information necessary for the transacting parties to make informed decisions about the transaction, negotiate an M&A agreement that appropriately addresses privacy and cyber risks, procure adequate representation and warranty insurance, and comply with applicable law. Privacy and cyber risk due diligence can also help the parties plan important post-transaction activities to maximize the benefits of the transaction and avoid or mitigate business and legal compliance risks.

Effective privacy and cyber risk due diligence is not a simple check-the-box process. It requires a collaborative effort by business, technical, and legal advisors with the experience and expertise necessary to identify and assess privacy and cyber risks material to the transaction and recommend appropriate strategies to mitigate those risks. To the extent practicable, privacy and cyber risk due diligence should be conducted by and under the direction of legal counsel, so the transacting parties can appropriately assert legal privilege over due diligence reports.

The privacy and cyber risk due diligence strategy for an M&A transaction should be tailored to the particular circumstances of the transaction. Privacy and cybersecurity frameworks and best practices guidance for conducting privacy and cybersecurity due diligence should be used with reasonable business judgment based on accurate information and expert advice.

M&A agreements

M&A agreements invariably contain provisions that allocate among the transacting parties various risks arising from the transaction, including circumstances occurring before or after the transaction is completed. Many of those provisions will apply to privacy and cyber risks and related losses and liabilities. Nevertheless, for many M&A transactions, it will be appropriate to include in the M&A agreement provisions that specifically address privacy and cyber risks, including:

- representations and warranties about privacy and cyber risks, including risks identified during due diligence and issues relevant to representation and warranty insurance;
- covenants that impose obligations, before and after the transaction is completed, regarding privacy and cyber risks;
- special indemnities, holdbacks and insurance obligations for privacy and cyber risks; and
- specific remedies if a privacy or cybersecurity incident occurs or is discovered before or after the transaction is completed.

Post-transaction issues

Parties to an M&A transaction should plan and prepare for additional or increased privacy and cyber risks after the transaction is completed, including risks relating to the integration of the parties' business operations and information technology systems, the sharing of data between the parties, and innocent errors and intentional misconduct by the parties' personnel. Transacting parties should be mindful of post-transaction legal compliance obligations relating to privacy and cyber risks (e.g., compliance with privacy laws, continuous disclosure obligations for reporting issuers, and corporate risk management generally) and costs associated with remediating both known and unknown privacy and cybersecurity problems. Transacting parties should also determine whether an M&A transaction affects their existing privacy and cyber insurance coverage or results in a need for additional insurance.

Key takeaways

The importance of privacy and cyber risks to an M&A transaction, and how those risks can be addressed effectively and appropriately, will depend on the circumstances and might require the transacting parties to contend with, and sometimes anticipate, rapid changes in privacy and cyber threats, evolving privacy and cybersecurity best practices, and new legal compliance obligations and liabilities under modernized privacy and cybersecurity laws. For those reasons, parties to an M&A transaction should obtain appropriate business, technical, and legal advice about privacy and cyber risks to properly inform their risk-based business decisions about the transaction and help address privacy and cyber risks throughout the transaction life cycle and after the transaction is completed.

Following is a summary of key steps for managing privacy and cyber risks in connection with an M&A transaction:

- Implement cybersecurity controls (e.g., data confidentiality/security agreements, secure online data rooms, and communication protocols) for the deal processes used by the transacting parties and their advisors and to protect commercially sensitive and regulated information (e.g., personal information) disclosed during negotiations and due diligence.
- Ensure non-disclosure agreements and transaction agreements include provisions required by privacy laws for the disclosure and use of personal information in connection with the transaction (e.g., for due diligence purposes) without the consent of affected individuals.
- Implement a strategy to help assert legal privilege over privacy/cybersecurity due diligence findings and risk assessments.
- Conduct appropriate privacy/cybersecurity due diligence of each relevant transacting party to identify and assess risks (including residual risks from pre-transaction privacy or cybersecurity incidents and risks arising from modernized privacy and cybersecurity laws) relevant to the transaction and post-transaction activities and to support applications for representation and warranty insurance (if applicable) and post-transaction privacy/cybersecurity insurance.
- Document the decisions and actions by or at the direction of transaction decision-makers (e.g., corporate directors and officers), based on consideration of due diligence findings and risk assessments, to establish their compliance with legal obligations (e.g., corporate directors' and officers' risk management duties and continuous disclosure obligations, if applicable).
- To the extent appropriate and practicable, mitigate identified privacy/cyber risks before the transaction is completed (e.g., by implementing the data minimization principle) and plan to avoid/mitigate risks after the transaction is completed (e.g., by establishing corporate structures and practices/procedures to avoid/mitigate unnecessary transfers of risk from seller to buyer).
- Consider privacy/cybersecurity due diligence findings and risk assessments when negotiating the nature, structure and terms of the transaction, and include in transaction agreements appropriate risk allocation provisions – representations and warranties, covenants, indemnities and remedies – to address privacy/cyber risks for a reasonable period after the transaction is completed.
- After the transaction is completed, promptly implement privacy practices and cybersecurity controls to address privacy/cyber risks identified during due diligence and additional or increased privacy/cyber risks resulting from the transaction, and consider procuring additional privacy/cyber insurance. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity, Privacy & Data Protection Group has extensive expertise and experience in cyber risk management and crisis management legal services. Find out more at **blg.com/cybersecurity**.