Bulletin | Cybersecurity and M&A

May 2021

Managing cyber risks in M&A transactions

Cyber risks are an important consideration regarding all merger, acquisition and financing ("M&A") transactions. Cyber risks can affect the viability and value of an M&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 cyber risks in connection with the transaction and incur potentially significant liabilities if they fail to do so. For those reasons, parties to an M&A transaction should appropriately address cyber risks throughout the transaction life cycle.

Understanding cyber risks

Cyber risks are risks of losses, costs and liabilities suffered or incurred by an organization as a result of a cybersecurity incident (i.e., an incident that adversely affects the confidentiality, integrity or availability of data in the organization's custody or control, or the information technology systems used by or on behalf of the organization or its business partners and advisors). 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 cybersecurity incident can include business interruption loss, loss of critical data, trade secret disclosure, loss of revenue and other financial loss, loss to stakeholder value, brand depreciation, and harm to reputation and customer loyalty. Costs and liabilities resulting from a cybersecurity incident can include incident response and remediation costs, regulatory investigation costs, litigation costs, fines, and financial liabilities to stakeholders, business partners, and customers.

Cyber risks are relevant to every organization, regardless of size, industry or public profile, because all organizations (directly or indirectly through their business partners) use or depend on information technology systems and data for their day-to-day operations. While large, high-profile organizations might be the most obvious targets for cyber attacks, cybercriminals are increasingly targeting small and medium sized organizations to obtain information about their customers and as a way to access the information technology systems and data of their business partners.

Effective cyber risk management is an enterprise-wide risk management and compliance challenge that requires a comprehensive, multidisciplinary approach based on three pillars – people, processes and technology. Appropriate cybersecurity controls – processes and technologies designed to prevent, detect, and respond to cybersecurity incidents – are of fundamental importance.

Cyber risks and M&A transactions

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 cybersecurity incidents include:

- **Verizon/Yahoo!:** Data security incidents at Yahoo! discovered before the completion of Verizon's USD $4.83 billion acquisition of Yahoo! resulted in a $350 million reduction in the purchase price and an allocation to Yahoo! of liability for costs resulting from the incidents.
- **PayPal/TIO:** A data security 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 Asco's business was disrupted by a ransomware attack. Ultimately, the transaction was cancelled.
- **Marriott/Starwood:** A data security incident at Starwood Hotels that began two years before Marriott's acquisition of Starwood 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.

According to an October 2020 *M&A Trends Survey* conducted by Deloitte, cybersecurity threats are the top concern for more than half (51%) of respondents as they manage M&A transactions virtually.

Business considerations

Cybersecurity incidents 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 and liabilities on the transacting parties after the transaction is completed. Certain assets (e.g., brand, reputation, and customer goodwill) can be particularly vulnerable to harm caused by a cybersecurity incident. In some circumstances, significant 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. Cybersecurity incidents can also impair the transacting parties' ability to negotiate and complete an M&A transaction.

Legal compliance considerations

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

Personal information protection laws

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

Corporate directors' and officers' duties

Under Canadian law, corporate directors are obligated to manage or supervise the management of the business and affairs of their corporation 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 cyber risk management activities and must ensure that corporate management has properly implemented appropriate policies and practices to manage cyber risks and respond to cybersecurity incidents. Corporate directors' and officers' responsibilities regarding risk management include managing 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 cybersecurity risks and cybersecurity incidents. Those obligations might require a reporting issuer participating in an M&A transaction to identify and assess the 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 data (e.g., business data, customer data, and cardholder data) and report data security incidents. Cybersecurity obligations might also result from quasi-contractual assurances given by an organization in various kinds of published policies (e.g., privacy policies) and promotional communications. The parties to an M&A transaction should consider the cyber risks resulting from those kinds of obligations.

Managing cyber risks in M&A transactions

There is no one-size-fits-all solution for effectively managing cyber risks in connection with an M&A transaction. The importance of cyber risks to an M&A transaction, and how those 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 sale or share sale);
- the nature, amount, and timing of the consideration paid;
- the nature and importance of the parties' respective information technology systems and data;
- the parties' post-transaction plans;
- each party's risk tolerance; and
- applicable representation/warranty insurance.

To effectively manage cyber risks in an M&A transaction, the transacting parties and their advisors should consider 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 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; and (3) participating individuals can be deceived by fraudulent messages. For those reasons, the parties to an M&A transaction and their advisors should implement appropriate agreements and security controls (e.g., secure online data rooms and communication protocols) to mitigate cyber risks inherent in M&A deal processes.

Cyber risk 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 cyber risks. Nevertheless, for most M&A transactions it will be appropriate to engage in due diligence specifically directed to cyber risks to obtain the information necessary for the transacting parties to make informed decisions about the transaction and post-transaction activities, negotiate an M&A agreement that appropriately addresses cyber risks, procure adequate representation/warranty insurance, and comply with applicable law.

Effective 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 cyber risks material to the transaction and recommend appropriate strategies to mitigate those risks. To the extent practicable, 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 cyber risk due diligence strategy for an M&A transaction should be tailored to the particular circumstances of the transaction. Cybersecurity frameworks and best practices guidance for conducting cyber 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 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 cyber risks, including:

- representations and warranties about cyber risks, including risks identified during due diligence and issues relevant to representation/warranty insurance;
- covenants that impose obligations, before and after the transaction is completed, regarding cyber risks;
- special indemnities, holdbacks and insurance obligations regarding cyber risks; and
- specific remedies if a 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 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 cyber risks (e.g., compliance with personal information protection laws, continuous disclosure obligations for reporting issuers, and corporate risk management generally) and costs associated with remediating both known and unknown cybersecurity problems. Transacting parties should also determine whether an M&A transaction affects their existing cyber insurance coverage or results in a need for additional cyber insurance.

Key takeaways

The importance of 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 cyber threats, evolving cybersecurity best practices, and new legal compliance obligations and liabilities. For those reasons, parties to an M&A transaction should obtain appropriate business, technical, and legal advice about cyber risks to properly inform their risk-based business decisions about the transaction and help address cyber risks throughout the transaction life cycle.

Following is a summary of key steps for managing 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 to be 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.
- Implement a strategy to help assert legal privilege over cyber risk due diligence results.
- Conduct appropriate cyber risk due diligence of each relevant transacting party to identify and assess cyber risks relevant to the transaction and post-transaction activities.
- Document the use of cyber risk due diligence results by or at the direction of transaction decision-makers (e.g., corporate directors and officers) to evidence 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 cyber risks before the transaction is completed and plan to address cyber risks after the transaction is completed.

- Consider cyber risk due diligence results when negotiating the nature and terms of the transaction, and include in transaction agreements appropriate risk allocation provisions – representations and warranties, covenants, indemnities and remedies – to address cyber risks.
- After the transaction is completed, implement cybersecurity controls to address cyber risks identified during due diligence and additional or increased cyber risks resulting from the transaction, and consider procuring additional cyber insurance. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's national Cybersecurity, Privacy and Data Protection Group offers comprehensive advice on compliance with privacy laws at the federal and provincial levels as well as with European data protection legislation. We provide both proactive compliance advice and legal advice to help respond to a contravention of privacy laws.

BLG's national Mergers & Acquisitions team handles domestic and cross-border M&A transactions across a broad range of industries involving listed and other public entities, as well as the acquisition and disposition of closely-held businesses. We leverage a broad range of combined expertise to offer responsive, targeted advice.