Torkin Manes
Barristers & Solicitors

Torkin Manes LegalPoint

Technology, Privacy & Data Management

July 2022

Cybersecurity in M&A Transactions

By Lisa R. Lifshitz and Roland Hung

It's no secret that the world is becoming increasingly data-driven, and the business world is no exception. The ability of a business to effectively store and protect its data is often integral to its value. Buyers in M&A transactions acquire both the assets and liabilities of the target entity and may risk losing immense value if the target entity has a history of poor cybersecurity practices. Buyers would, therefore, be wise to consider the target entity's cybersecurity preparedness in two key contexts: (1) during the due diligence process, and (2) as part of the purchase agreement's preparation and negotiation.

Cybersecurity and Due Diligence

A cyber-attack can quickly and substantially reduce the value of a target entity. It can cause the target to suffer reputational damage, and for public companies, it can negatively affect the target entity's share value. The federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**"), Alberta's *Personal Information Protection Act* ("**PIPA**"), and Québec's *Act respecting the protection of personal information in the private sector* as amended by *Bill 64, An Act to modernize legislative provisions as regards the protection of personal information* ("**QC Act**") require that private sector organizations report any breach of security safeguards involving personal information under their control.[1] PIPEDA and PIPA require organizations to report the breach if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual, while the QC Act requires organizations to report the breach if the breach creates a risk of serious injury. Failure to report the breach can result in fines of up to $100,000 under PIPEDA or PIPA, and ultimately up to $25 million or 4% of worldwide turnover for the preceding year under the QC Act.[2] A Special Committee of the British Columbia legislature published a report in December 2021 recommending that British Columbia implement mandatory breach notification requirements in its private sector privacy law as well.[3]

Given the risks associated with a cyber-attack, buyers should consider the target company's cybersecurity preparedness when engaging in the due diligence of such company. Such diligence should include questions as to whether the target company ever suffered an actual or suspected data/security breach, experienced a cyber-attack, paid any ransoms to third parties in connection with such an occurrence, or was ever required to report a data/security incident to any regulator, government agency or department, third party institution or individual in Canada or elsewhere.

Buyers should review the target entity's cybersecurity practices (including controls) and data governance policies and procedures. They may ask whether the target entity periodically assesses its own cybersecurity risks (and uses a third-party expert to evaluate such risks), and whether the target company's existing security practices are appropriate (and adequate) for the particular industry in which the target entity operates. Specifically, the buyers should review how the target entity controls access, manages data for security and authorization purposes, and monitors the movement of information that is being transferred outside of the organization, including to both related entities and unrelated third parties. Additionally, the buyers should understand the data, assets, and services of the target entity's organization that require the most protection to ensure the target company has met these requirements prior to closing. Buyers should also consider the target entity's incident response policies and procedures, as well as its external and internal privacy policies.

Many businesses also use third-party platforms that process or otherwise have access to the target entity's data. Buyers should, therefore, consider whether the target entity's key third-party partners, suppliers, and vendors have sufficient cybersecurity practices and whether the target company's existing contracts with such entities contain adequate legal language regarding such cybersecurity considerations. Buyers should also determine how the target entity analyzes risk when considering prospective third-party relationships.

Cybersecurity and Contractual Protections

Buyers may also reduce their own cybersecurity risks by negotiating relevant contractual protections in the prospective purchase agreement. If the due diligence process of the target entity revealed critical cyber vulnerabilities or outdated technology and other systems, the buyer should anticipate incurring costs to implement the necessary changes to bring the target entity up to an adequate level of cybersecurity readiness and practices. The buyers may then be able to negotiate a lower purchase price to account for such costs. In addition, the buyers should negotiate a holdback on the purchase price payable to the seller(s) to cover cybersecurity remediation costs post-acquisition.

Buyers may also want to use legal representations and warranties to reduce risk exposure. Buyers rely on representations and warranties to determine the appropriate purchase price. If the sellers breach their representations/warranties, the buyers may have rights to walk away from the deal or recover additional damages for not getting what the buyers bargained for. Even where a buyer conducts robust due diligence, the sellers would be in a position to know the target entity much more intimately than the buyer. The inclusion of carefully drafted representations and warranties in the purchase agreement can act as a backstop, protecting the buyer from cybersecurity issues that the due diligence process may not have uncovered. Ideally, representations and warranties for cybersecurity matters should not have significant materiality or knowledge qualifiers.

As examples, a buyer could request the following representations and warranties:

- That the target entity has not been the subject of a data or security breach, including any breach that required the target entity to report such event to a government entity/regulator, third-party government institution or individual;
- That the target entity's cybersecurity practices comply with certain designated security standards/frameworks and practices (or exceed them, where appropriate); and
- That the target entity has, at all times, conducted its business in compliance with applicable privacy and data security laws, with such laws expressly described in the purchase agreement.

A purchase agreement will usually include a general indemnity that would allow the buyer to recover losses for breach of representations and warranties. We additionally recommend the inclusion of specific privacy and cybersecurity indemnities in larger acquisitions, as appropriate. For example, it may be appropriate to have privacy and cybersecurity representations and warranties survive for a longer period than other representations and warranties, as privacy/cybersecurity deficiencies may not reveal themselves until long after the closing.

Conclusion

There is no question that prospective buyers in an M&A transaction should consider cybersecurity concerns at all stages of the transaction, from the earliest due diligence stage to the drafting of the definitive purchase agreement to final negotiations with the prospective target entity. Depending on what the due diligence process reveals, cybersecurity concerns/inadequacies may impact the final purchase price that the buyer is willing to spend. In certain circumstances, the buyer should consider the inclusion of stand-alone representations, warranties and indemnities for privacy/cybersecurity matters in the purchase agreement. At the end of the day, a seller's representations, warranties and indemnities are only one aspect of the transaction to consider when the buyer wishes to protect itself against the risk of cyber-attacks. Buyers should carefully review all aspects of the target entity's cyber practices to uncover critical cyber vulnerabilities prior to acquisition in order to better understand the target entity's vulnerabilities and formulate a plan to remediate essential cybersecurity deficiencies and build a more comprehensive cybersecurity regime for the target entity post-closing.

For more information about legal considerations around cybersecurity, please contact a member of Torkin Manes' Technology, Privacy & Data Management Group. For more information about the new Bill C-27, please read our article on Bill C-27 here.

[1]*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 at s. 10.1(1) ["**PIPEDA**"]; *Personal Information Protection Act*, R.S.A. 2003, c. P-6.5 at s. 34.1(1) ["**PIPA**"]; *Act respecting the protection of personal information in the private sector*, C.Q.L.R., c. P-39.1 at s. 3.5 ["**QC Act**"], effective September 22, 2022. Note that the exact phrasing and threshold of the reporting requirement varies depending on the applicable Act.

[2]*PIPEDA* at s. 28; *PIPA* at s. 59(2); *QC Act* at s. 91, effective September 22, 2023.

[3] British Columbia, *Modernizing British Columbia's Private Sector Privacy Law*, 42nd Leg, 2nd Sess, December 6, 2021 at p. 27-28 <https://www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/2nd-session/pipa/report/SCPIPA-Report_2021-12-06.pdf>.

Authors

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Roland Hung
Counsel

Tel: 780 914 1786
rhung@torkinmanes.com