CYBERSECURITY NOW PART OF DUE DILIGENCE PROCESS

By: Imran Ahmad, Gary Volman, and Deven Rath

Given the accelerated pace at which businesses are digitizing their operations and assets, the importance of cybersecurity cannot be underscored enough. In the context of an M&A transaction, implementing appropriate cybersecurity measures is essential given that the buyer is likely paying a premium for the target and any failure to accurately assess cyber risks may result in a reduced value of the acquisition or previously unknown litigation exposure. With the assistance of cybersecurity experts, due diligence can be tailored to ensure that the risks are known and appropriately managed so that there are no unexpected surprises post-transaction.

Hidden Risks

It was recently announced that Yahoo! Inc. ("Yahoo") and Verizon Communications Inc. ("Verizon") had reached an agreement whereby the purchase price was reduced by $350 million. Yahoo will be responsible for evenly splitting the cash liabilities that may arise from non-Securities and Exchange Commission ("SEC") government investigations and third-party litigation related to the breaches. In addition, Yahoo will continue to be responsible for SEC investigations and shareholder lawsuits. The adjustment to the purchase price stems directly from the data breaches Yahoo reported over the summer of 2016. This case serves as a reminder of the importance of a due diligence process that includes an in-depth review of the target's cybersecurity posture.

Avoid Buying A Lemon

Acquiring a business can create a number of advantages for the buyer, but also inherently carries certain risks, such as environmental liabilities or obligations to employees. This is why a thorough due diligence process is essential, since it allows the buyer to identify the level of risk associated with the transaction and ensure that it is comfortable taking on that risk. Failure to identify problems can result in discovering, after the fact, issues and liabilities that may not only diminish the value of the acquisition, but can also result in having to commit significant additional resources to resolve them. Put simply, buyers want to avoid a situation where they have bought a lemon.

As the Yahoo-Verizon case study shows, identifying cybersecurity risks during the due diligence phase of a deal is increasingly important, because if the company does not detect problems before the deal closes, it risks sustaining losses afterwards. The earlier a buyer can identify problems, the more opportunity it will have to manage the associated risks: by resolving them, re-negotiating the purchase price, or delaying the closing date, if necessary.

Broadly speaking, cybersecurity risks include the following:

- Business interruption
- Legal liability, including litigation
- Regulatory investigation and enforcement action
- Failure to meeting contractual obligations
- Loss of critical data (e.g., intellectual property, trade secrets, etc.)
- Reputational harm
- Inconvenience to customers and loss of trust
- Expenses related to recovering the data
- Loss of revenue, etc.

Given the potential impact a cyber-incident can have on an organization, it is no surprise that buyers are increasingly demanding that a cybersecurity due diligence process be undertaken and the findings factor into the negotiation of the purchase agreement.

Covering the Bases

The following elements should be, at a minimum, part of any cybersecurity due diligence process. This is by no means an exhaustive list and it would need to be customized based on the input of cybersecurity experts, depending on the nature of the target's business. Nevertheless, it is a good baseline from which to start.

1. Initial Identification at the Engagement Stage

Buyers should consider performing cybersecurity risk assessments during the initial stages of the transaction, and engage qualified experts as early as possible. The target's key processes and systems should be identified, including the data backup and recovery process. In addition, the buyer should have an understanding of the target's key assets, major threats, and potential vulnerabilities. One of the key objectives during the due diligence stage should be to assess the target's awareness of its operational risks rather than relying on the target's assurances.

2. Assess Target's Security Measures

Due diligence questionnaires based on recognized standards (e.g., NIST, ISO 27001, etc.) should be completed by the target to determine what security controls are in place to protect critical business data. The questionnaires provide buyers with key information on the target's exposure to a potential data breach and these findings may serve as a negotiating point throughout the transaction. The findings will also help the buyer determine whether the target has a crisis management plan in place which has been approved by senior management – awareness at the senior executive/board level is an important indicator of how seriously the target has considered its cyber-related risks.

3. Tailoring Diligence

After reviewing the information obtained from the initial cybersecurity risk assessments, buyers should tailor and focus their follow-up due diligence accordingly. Findings from the initial risk assessment and due diligence questionnaires will better inform the buyer of the information now available to it, the industry it will be operating in, and how important information security is to the target. Buyers should also consider how important data is to the target's business, and how that data is being protected.

4. Engage Cybersecurity Experts

Cybersecurity experts and specialized legal counsel should be engaged at the outset of the transaction to gauge the target's cyber-readiness and potential exposure to serious data breaches. Involving experts is vital, since the parties involved in the transaction process often do not possess the technical background necessary to thoroughly assess cybersecurity risks or to compare the findings with accepted industry-specific benchmarks. Experts may conduct necessary on-site testing and assess the suitability of the programs in place to manage risks to both physical security (access to locations/computers) and technical security (encryption, firewalls, network monitoring). They will also ascertain the costs and consequences of any potential vulnerabilities identified during the engagement stage.

5. Setup Risk Oversight Team

Organizations may also want to establish a risk oversight team to oversee all cybersecurity related matters, including the possible issues that may arise during negotiations and post-closing. The team should be regularly briefed about cyber-risks uncovered during the diligence process and key stakeholders should be informed of these risks. The team should liaise with the target to ensure that security measures are comprehensive: employee contracts and confidentiality/non-disclosure agreements, employee policies/training, access to hardware/software, and should include possible issues in the supply chain. This team should also be responsible for managing the integration process to ensure that the buyer's network is not put at risk as a result of the target's vulnerabilities.

6. Check The Past

Buyers should also ask the target about past cybersecurity incidents, any pending investigations by regulators or litigation, and the target's general response to the any incidents. If the target has suffered numerous cyber incidents, this may be a good indicator that security was not a priority and it may signal that the target's digital assets (e.g. intellectual property, trade secrets, etc.) have been compromised. Buyers must remember that when they are acquiring a company, they are directly acquiring its past, present, and future data security problems.

7. Assessing Cyber Insurance

In addition to insurance and/or indemnities related to the representations and warranties in the purchase agreement, buyers should evaluate the extent to which cyber risks are mitigated by specific coverage, including whether enhancements to the cyber program may be available post-closing. Most cyber insurance policies cover data breaches and the expenses involved in complying with data breach notification laws.

Key Takeaways

- It is vital for buyers to understand the risks associated with the digital assets they are acquiring in transactions. Not understanding the risks can create an unexpected liability post-transaction.
- To help understand the risks, cybersecurity due diligence should always be part of the buyers broader transactional analysis. Buyers should consider potential cyber-related risks in the acquisition process and tailor their diligence to each target's business.
- The results of cybersecurity due diligence, and any issues that are discovered, should inform the negotiation of the purchase agreement. This will possibly be reflected in the purchase price, the indemnification/insurance provisions, or elsewhere in the agreement.
- It is important for a buyer to engage cybersecurity experts in the due diligence process. Engaging experts ensures that individuals with the necessary technical background are assessing the target's exposure to cyber risks.

Contact

Imran Ahmad
Partner
416.597.6031
iahmad@millerthomson.com

Gary Volman
Associate
416.595.7924
gvolman@millerthomson.com

Deven Rath
Articling Student
416.595.8635
drath@millerthomson.com

MILLERTHOMSON.COM

MILLER THOMSON
AVOCATS | LAWYERS