

# Remember Cybersecurity Due Diligence When Evaluating an Acquisition

Given the ubiquity of electronic data, an acquirer must have a comprehensive understanding of a target company's data privacy and cybersecurity risks. Such an understanding can minimize transactional risks and post closing liabilities.

A key due diligence task is determining the adequacy of the target company's data privacy and cybersecurity practices given its legal obligations and the type and volume of information it collects. As with any due diligence exercise, the goals are to inform, validate and quantify. Accordingly, an acquirer's cybersecurity due diligence should investigate the target company's data privacy practices and procedures, evaluate the risks addressed by those practices and procedures and seek to eliminate (or at least reduce) those risks post closing. The process entails categorizing the type of data collected by the target, identifying its data centric vulnerabilities and reviewing its key technology vendor relationships. As cyberattacks often involve unintentional downloading of malware, a prudent buyer acquirer should also review the target company's employee educational and training programs.

Once the cybersecurity due diligence is completed, an acquirer should consider including a cybersecurity representation (tailored to the target's specific business) in the purchase agreement. Such a cybersecurity representation could read as follows:

Seller has all necessary data security, cybersecurity and physical security systems, policies and procedures in place to meet its legal and contractual obligations. Seller's privacy policy regarding the collection, use, maintenance and disclosure of Sensitive Information is set forth on Schedule. Seller is and has at all times since [insert date] been in compliance with such privacy policy. Seller has complied at all times with all applicable laws regarding the collection, use, storage, transfer or disposal of Sensitive Information. Seller has established and implemented policies, programs and procedures that are in compliance with applicable industry practices to protect the confidentiality, integrity and security of all Sensitive Information in its possession, custody or control against unauthorized access, use, modification, disclosure or other misuse. Seller has not experienced any loss, damage or unauthorized access, disclosure, use, maintenance or breach of security of any Sensitive Information in Seller's possession, custody or control, or

## POSTED:

Sep 12, 2017

## RELATED PRACTICES:

### [Banking and Finance](#)

<https://www.reinhartlaw.com/practices/banking-and-finance>

### [Corporate Law](#)

<https://www.reinhartlaw.com/practices/corporate-law>

## RELATED SERVICES:

### [Corporate Governance](#)

<https://www.reinhartlaw.com/services/corporate-governance>

### [Data Privacy and Cybersecurity](#)

<https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity>

### [Emerging Businesses and Early-Stage Investing](#)

<https://www.reinhartlaw.com/services/emerging-businesses>

### [Mergers and Acquisitions](#)

<https://www.reinhartlaw.com/services/mergers-and-acquisitions>

### [Private Equity](#)

<https://www.reinhartlaw.com/services/private-equity>

### [Software, Technology and Licensing](#)

<https://www.reinhartlaw.com/services/software-technology-and-licensing>

## RELATED PEOPLE:

[Martin J. McLaughlin](#)



otherwise held or processed on Seller's behalf.

<https://www.reinhartlaw.com/people/martin-mclaughlin>

Finally, an acquirer should explore any existing and available insurance policies that may cover losses arising from a cybersecurity or data breach. These policies may cover, in whole or in part, costs incurred due to business interruption, system failure, cyberextortion, breach notification requirements and digital asset restoration.

If you have any questions or concerns regarding cybersecurity within the acquisition context, please contact [Marty McLaughlin](#), Hana Cho, or your personal Reinhart attorney.

*These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.*