



Cyber Diligence and Resilience: Understanding Risk Involved with A Company's Data

Sep 08, 2019

Categories:

[Blogs](#)

[Private Equity Industry](#)

[Blog](#)

Background

The due diligence process in private equity transactions require that you as a buyer or seller conduct proper investigations into a prospective target's data security. Data breaches are inevitable. According to bitglass.com, data breaches of the three largest publicly traded companies over the past three years have resulted an average of \$347 million in legal fees, penalties, remediation costs, and other expenses for each of these companies. In addition, these three large companies suffered an average of a 7.5% decrease in stock price leading to a market cap loss of \$5.4 billion per company. Thus, there is a direct link between a company's valuation and the occurrence of a data breach.

Private equity firms are increasingly assessing the cyber health of their target companies as an essential component of the due diligence process. Key to this assessment is understanding what personal data the target collects and the systems it utilizes, the security processes it employs, the security incidents it has experienced, the responses to those incidents, and the programs it has in place for security, both internally for employees and externally for third party contractors.

Data Management

The types of personal data that a company maintains is important because it will help you determine what regulations apply to its business. More importantly, you will want to understand what kind of networks and systems are being used by the company and where the data is located on those systems (i.e. cloud).

- What types of data does the company maintain (e.g. financial, health, children's)? Where is the data located? What systems are the data located on?

- What networks and systems are being used by the company? Who maintains and has control over these networks and systems?

This knowledge will help you put into context the associated legal, technical, forensic, and administrative costs associated with complying with regulations in this industry, both to prevent data breaches and in dealing with a breach when it occurs.

Breach and Disaster Response

Next, you will want to request information on any data breaches that have occurred and evaluate the target's breach response and business continuity plans.

- Does the target have a robust written information security program and breach response plan? Does the target conduct tabletop exercises to test its plan and its resilience in the event of a data breach?
- Does the target maintain a disaster recovery plan and business continuity plan? If so, have personnel been trained regarding their responsibilities?

Employee Training and Third-Party Contracts

A plan is only as good as the people who are implementing it. _

Employees: You will want to know whether the target adequately trains its employees regarding data management and security.

- Does the company have a comprehensive data management and security program? Are the proper personnel knowledgeable about the program?
- How does the company train its employees regarding data security? Are exercises conducted annually to determine employees' knowledge of potential security threats (e.g. simulated phishing email)?

Third-Party Contractors: Companies should properly vet their vendors and other contractors that have access to the target's data.

- Does the contractor employ proper security measures for data that it exports from the target to its own systems?
- Do the service agreements indemnify the target in the event of a breach of the contractor's network?

Takeaways

Proper diligence regarding cybersecurity is crucial to assess the need for remediation of an acquired company's past data and security practices. And at the extremes this due diligence may help the PE firm avoid a potentially unwise and costly investment.

For more information, please contact any attorney on our [Privacy & Data Security team](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.