MAYER·BROWN

Cybersecurity & Data Privacy

STRATEGIC THINKING AND PRACTICAL LEGAL ADVICE

Five Questions for General Counsels Regarding Cybersecurity Due Diligence

Whether it comes in the form of a cyber attack to your network or a consumer privacy enforcement action brought by a state regulator, no organization is immune from the risks that come from processing and securing sensitive personal and commercial data. Conducting a due diligence process that addresses privacy and security risks is necessary for acquirers and should be expected by target companies. Here are five considerations for General Counsels to help them do it right.

1. **It matters.** Cyber and privacy due diligence is necessary to identify and understand potential risks in a transaction –and this matters for companies on both the buy and sell side of a transaction. The value of a company can be affected by such regulatory and security risks, which can result not only in legal impacts but damaged reputations. One recent example is that during the Yahoo acquisition, the public disclosure of significant data breaches ultimately led to a $350 million reduction in purchase price.
2. **It's complicated.** General Counsels should understand the full range of cyber and privacy laws, regulations and best practices that could apply to the target company. This means starting with a detailed map of the company's data that describes the types of data collected, how it is collected, how it is stored, and how and to whom it is transferred. This map will assist the General Counsel in understanding the complicated patchwork of regulations from around the globe that may apply to the target.
3. **It's surprising.** A thorough due diligence process will certainly include a request for information on any inquiries from law enforcement and regulatory agencies, or any known security or privacy breach or violation, but sometimes the biggest threats are unknown to the target and can come as a surprise to both parties to the transaction. Diligence can assess unknown breaches by testing the target's systems and obtaining a third party review for any of the target company's data for sale on the dark web.
4. **It's evolving**. Around the world, regulatory requirements affecting data are increasing and evolving at a rapid clip, and with the development of new and emerging technologies, acquiring companies may find that they will be subject to new obligations as a result of the transaction. This may mean that the acquiring company has to get up to speed and understand a wide range of potentially new obligations – which could range from strict state laws governing biometric collection to new data protection requirements in Brazil, to name just a few examples.

5. **It requires experts.** Proper due diligence requires expertise, and counsel with expertise in cybersecurity and data privacy should be involved early and extensively in the process. Depending on where the data is located or the technology involved, this may mean working with specific counsel with the appropriate background in the regulations at issue. Additionally, in order to understand unreported threats or attacks, diligence should involve forensic experts who can perform the necessary testing of the target's systems.

General Counsels of companies currently, or expecting to be, involved in a merger or acquisition should plan on conducting proper cyber and privacy due diligence. While in the past, this may have been a priority primarily for companies where data was at the core of their business model, such diligence matters now for nearly any type of company, regardless of industry.

For more information about the topics raised in this Q&A piece, please contact any of the following lawyers.

Kendall C. Burman
+1 202 263 3210
kburman@mayerbrown.com

Joseph A. Castelluccio
+1 212 506 2285
jcastelluccio@mayerbrown.com

Nina L. Flax
+1 650 331 2070
nflax@mayerbrown.com

Benjamin A. Shoemaker
+1 202 263 3463
bshoemaker@mayerbrown.com