LEGAL ADVISOR

A PilieroMazza Update for Federal Contractors and Commercial Businesses

Cybersecurity Concerns in M&A Due Diligence

By Kimi Murakami and Jonathan Bush

Prominent news stories in the last couple of years have highlighted the increasing regulatory and commercial risks that businesses across industries are confronting related to cybersecurity attacks (e.g, Yahoo!, Home Depot, Sony, and Target). These attacks have underlined the key point that most businesses today are dependent to one degree or another on data and network systems. The consequences of such attacks can result in significant litigation, remediation and other costs in response, not to mention loss of consumer or industry goodwill and trust.

The federal market reflects these broader realities. To combat threats and shift responsibility and potential liability to contractors, the government has been busy adding cybersecurity requirements to the FAR and DFARS. A very recent example that has affected many of our clients was the requirement for certain defense contractors to comply with NIST SP 800-171 as of the start of this year.

Given the increased focus on cybersecurity requirements for both commercial firms and government contractors, it is not surprising that we have started to see more attention paid to cybersecurity in some M&A transactions. However, in many M&A transactions, the parties are still not paying sufficient attention to the efforts of the target company to prepare for future attacks, especially considering how the target company's value proposition may be significantly impacted by such attacks.

Given the dependency of businesses across almost every industry upon digital data and systems, acquirers of businesses must include at the beginning of every due diligence investigation, an evaluation of whether a target has been or is the victim of a digital attack and, if not, whether it is vulnerable or unprepared for such an attack. If this is not done, then the acquirer will potentially assume unknown damages and liabilities and may be acquiring assets that are substantially devalued. This is not the only risk, however. Integration of the target's data and computer systems with the acquirer's may allow attackers to exploit vulnerabilities across the whole enterprise.

Acquirers in an M&A transaction must, therefore, approach due diligence surrounding cyberattacks and cybersecurity with the same level of thoroughness undertaken with respect to other commercial and legal due diligence. The following is just an introductory list of topics that should be addressed in undertaking any cybersecurity review of a target company.

1 Identification of the key digital assets of a target company.

This review must begin by identifying critical digital assets that need protection as well as analyzing which digital assets are vital to the operation of the company and its business. This will allow an acquirer to begin to assess the potential impact of a cyberattack on a target company. This review should not only examine the target's data, but all the surrounding systems that relate to such assets such as computer systems and servers, software, and communications infrastructure. The acquirer should ascertain not only what the digital assets are, but where they are stored, on what they are stored, and whether or not the target has control of

Continued on page 2

PILIERO MAZZA

such assets (i.e., does it own the location where they are stored and control access to their use).

2 Evaluation of the target company's internal cybersecurity program.

The due diligence evaluation must assess whether the target has an appropriate cybersecurity program in place. This evaluation should be made by the business and legal members of the acquirer's team as a supplement to a technical cybersecurity review undertaken by IT security professionals. Evaluating a target's cybersecurity program includes addressing issues such as:

- ☑ Is there a written system security plan or program in place? If so, how recent is it and is it regularly updated?
- ☑ How involved is senior management and the board of directors in overseeing and monitoring the program?
- ☑ Who is responsible for day to day operations of the program? Does the company have or need to have a chief information officer?
- ☑ Has the target conducted a risk assessment and tailored the program to its particular business?
- ☑ Has the target had a third party firm analyze its security program?

3 Is the target a defense contractor?

Failure to comply with defense regulations requiring that certain cybersecurity controls be in place can jeopardize the target company's ability to bid on and perform work as a defense contractor. Due diligence inquiries and investigation must be conducted to ensure no violation of this additional layer of cybersecurity requirements for contractors performing work for the Department of Defense.

4 Evaluation of target's program with respect to third parties upon which it is dependent.

Cybersecurity of a target company also relies on whether there is an effective program to manage the security risks relating to its third party vendors, outsource providers, contractors, cloud service providers, and others that have access to the target's digital assets. It is essential in a due diligence evaluation to identify vendors that are critical to a target's operations as well as those that pose the greatest threat to the target if said vendor was the victim of a cyberattack.

5 Assessing past cybersecurity attacks and breaches.

Since the effects of prior attacks can linger long after a breach has been addressed, it is critical to understand the scope of past breaches, the history of the target's response to such breaches, and changes in its cybersecurity program to prevent/respond to future attacks.

6 Evaluation of compliance cybersecurity with regulatory obligations.

Cybersecurity laws and other legal obligations are extensive and vary widely across jurisdictions at the federal and state levels as well as internationally. Even if a target company is not directly governed by the laws of a specific jurisdiction, relationships between the target and its business partners can result in the laws of other jurisdictions being imposed on a target company via contract. Additionally, a target company may have imposed cybersecurity related obligations upon itself through statements in privacy policies on its website or in advertising. Failure to comply with such obligations risks not only regulatory penalties, but such failure could also be used against a target company in future litigation with a concomitant increase in exposure.

Once the cybersecurity due diligence assessment is completed, corporate attorneys must flag problem areas for the acquirer's transaction team and assist the team in discussing such risks and implementing solutions to address them including, for example, additional representations and warranties, conditions to closing, covenants, purchase price adjustments, line-item indemnification.

About the Authors: Kimi Murakami is counsel with PilieroMazza and focuses her practice in the business and corporate and government contracts groups. She may be reached at kmurakami@pilieromazza.com. Jonathan Bush is counsel with PilieroMazza and focuses his practice in the business and corporate group. He may be reached at jbush@pilieromazza.com.