CHAPTER

1

The Challenge

By Roland L. Trope and Thomas J. Smedinghoff

In M&A deals, targets often prefer to postpone disclosures of information that might adversely affect their position in the negotiations and closing. Acquirers attempt to coax out those disclosures as early as practicable. Questions asked early in an acquisition, however, may prompt a denial or be interpreted to facilitate a postponement of a disclosure. Due diligence reviews aim to bring the undisclosed, deal-critical information to light.

Acquirers also seek to know what the target may not know about itself that could be deal-critical information. Due diligence reviews endeavor to identify areas where such unknowns pose a significant risk to the acquirer's deal objectives.

In both cases, deal-critical information that the target is slow to disclose or does not know increasingly tends to relate to the target's cybersecurity profile, practices, and vulnerabilities, and to the condition of its digital assets (*i.e.*, whether, and to what extent, they are not adequately protected and/or have already been compromised and devalued).

Until those unknowns become known, the acquirer cannot assess them and determine whether it should seek a negotiated adjustment in the deal's terms. It is important that an acquirer not close a deal if deal-

critical information remains unidentified, or there has not been sufficient time to evaluate its significance to the deal's objectives. Several examples of M&A deals involving cyber incidents (discussed in Chapter 2) suggest that cybersecurity information about a target and the condition of its digital assets can be among the most elusive and difficult to evaluate when discovered, yet may well be of critical significance to an acquirer's deal objectives.

Thus, this guide to cybersecurity due diligence is intended to help an acquirer's counsel capture both kinds of cybersecurity unknowns about a target: what the target knows and may be reluctant or slow to disclose, and what the target does not know. This guide is also intended to help C-suite officers (especially chief executive officers and chief information security officers) as well as board members quickly grasp the importance of cybersecurity due diligence and the ways in which it can help them in their evaluation of risks that a target's cyber-vulnerability or a compromise of its digital assets can abruptly pose to a deal's objectives.

In the digital era, counsel responsible for preparing a customary due diligence report must contend with the known unknowns about the quality of a target's cybersecurity defenses and its experience with cyber incidents. That poses a challenging risk assessment for an acquirer, and one quite different from other risk assessments in an M&A deal. How does an acquirer's counsel evaluate the target's cybersecurity program or inquire into its probable experience with cyber incidents? How does counsel assess the potential devaluation of the target's high-value digital assets without evidence of what was accessed and exploited? How does counsel determine the "materiality" of apparent cyber incidents without knowing, other than by inference, the nature of the digital assets at risk or the harm that could flow from their compromise?

Customary due diligence reviews might not address such issues. As a result, they might overlook a significant set of known unknowns—the possibility of asset devaluation by undetected cyber incidents. Such reviews might also omit an assessment of such risks and the potential need to factor them into the negotiation of the price the target seeks to place on its high-value digital assets.

Customary due diligence in M&A deals aims at verifying the existence, actual condition, and value of a target's tangible and intangible assets as well as its operations and businesses. Where the condition of the target's assets, operations, and businesses is discovered to be substantially less than initially described or otherwise expected, an acquirer may want to restructure the deal to address the risks identified, negotiate a reduction in

the price, require enhancements in the representations, warranties, covenants, and indemnifications, or, in rare instances, abandon the deal.

However, a customary due diligence review of a target might not adequately identify its high-value digital assets, assess the state of the security program it has in place to protect those assets, or alert the acquirer to risks that the target's high-value digital assets, operations, and businesses may have been (or could be) compromised by cyber incidents. As a result, the acquire might not realize that the target is not worth the price originally negotiated. Thus, the acquirer's counsel may decide to recommend to the client that time and resources be invested in enhancements of the customary due diligence review to identify and address the uncertainties and risks posed by the potential cyber vulnerabilities of the target's digital assets. In that event, M&A lawyers might find it helpful to draw on this guide's suggestions for organizing and planning enhanced cybersecurity due diligence to discover and report on a target's cyber vulnerabilities, whether those have been exploited by cyber incidents, and whether the value of target's assets, operations, and businesses have been reduced or are at risk of becoming impaired.

Cybersecurity due diligence might not yield a precise and exact picture, but it has the capability to provide an acquirer with a far closer approximation of the actual condition of the target's digital assets by revealing the cyber vulnerabilities of those assets, whether the target has been adequately safeguarding and monitoring the control of those assets, and any records of cyber incidents that may have resulted in compromises of those assets. Knowing such facts, the acquirer's counsel will be in a better position to structure the definitive acquisition agreement to mitigate the risks identified (*see generally* Chapters 11 and 12).

During the writing of this guide, two particular M&A deals highlighted the risks of underestimating the need for cybersecurity due diligence: (i) the cyber incident that began shortly before the acquisition of Neiman Marcus and ended just after the closing, but was not discovered until months later during the end-of-year holiday shopping season; and (ii) the agreement by Verizon to acquire Yahoo! where, at this writing, the terms of the deal have been renegotiated to reflect, among other changes, a $350 million reduction in the price as the result of discovery of two cyber incidents that compromised over 500 million and one billion Yahoo! customer records, respectively. The incidents at Neiman Marcus and Yahoo! and their impact on the acquisitions of those companies are discussed later in this guide (*see* Chapter 2, Sections 6, 6.1 and 6.2).

Best practices for cybersecurity due diligence have yet to coalesce, but this guide takes the first step in developing such best practices by outlining a fundamental approach to cybersecurity due diligence and highlighting the areas worthy of focused attention by a cybersecurity due diligence team.

One guiding principle deserves mention at the outset: acquirers should treat as a rebuttable presumption that a target's high-value digital assets are increasingly at risk of becoming cyber-vulnerable assets. The more iconic the target, or the more renown its trove of digital assets (whether customer data, intellectual property, automated process controls, encryption keys, or infrastructure operational details), the greater the probability that it will, or already has, become a victim of reconnaissance probes and damaging cyber attacks.

As a consequence, cybersecurity due diligence is critical to the M&A process. To the extent that the M&A due diligence process fails specifically to assess cyber risks—and particularly the cyber vulnerability of a target's high-value digital assets and the potential for acquisition of the target to expose the acquirer to the target's cybersecurity deficiencies and secreted malware—the more the acquirer may end up misinformed by its own answers to basic questions, such as: "What are the risks involved in this acquisition? What is the value of this business . . .?"[1]

A key premise of this guide is that the cyber vulnerabilities of a target's high-value digital assets should be viewed as potential *material* risks to an M&A deal's objectives. Accordingly, this guide is intended to provide attorneys representing clients in M&A transactions with the tools needed to conduct effective cybersecurity due diligence reviews of the target company's business and, specifically, to help identify and illuminate cybersecurity risks inherent in the proposed deal.[2] It focuses on issues to be identified and questions to be asked during the M&A due diligence process. It is designed to assist in getting the target to fully disclose any known existing cybersecurity issues. It assumes that, where appropriate, M&A attorneys will work with security professionals to review, analyze, and explain the results of the cybersecurity due diligence review.

This guide is organized to help M&A counsel plan and implement a cybersecurity due diligence review. It will help an acquirer's officers and

1. ABA Bus. Law Section, Comm. on Negotiated Acquisitions, The M&A Process: A Practical Guide for the Business Lawyer 179 (2005).

2. It is not intended as a guide to cybersecurity best practice or an explanation of applicable cybersecurity law. Those issues are adequately addressed in numerous other publications.

directors understand the process and its potential to illuminate unsuspected risks to the target's digital assets. It will also facilitate the interactions between counsel and cybersecurity personnel engaged to assist in the due diligence review so that, instead of focusing on the minutia of technical details, the consultants will realize the need to focus on risks to the target's digital assets, its brand, and the acquirer's deal objectives. Each chapter addresses steps in that process.

Chapter 2 explains the need for cybersecurity due diligence and illustrates that need with a discussion of the impact of cyber incidents on acquisitions. Two illustrations are provided: the acquisition of Neiman Marcus that closed without discovery of an ongoing cyber incident, which led to class-action lawsuits by the retailer's customers; and the acquisition of Yahoo! by Verizon where, before the originally scheduled closing, Yahoo! disclosed two cyber incidents that compromised records containing personal information of over 500 million and one billion users, respectively. Other illustrations highlight reported cyber incidents that a cybersecurity due diligence team will find worth remembering as cautionary guidance.

Chapter 3 explains certain kinds of cybersecurity risks that may be material to an M&A deal. The chapter concludes with a list of a target's potential cybersecurity risks.

Chapter 4 explains the basic cybersecurity concepts that a due diligence team should understand and make use of in its cybersecurity due diligence review of a target. This chapter also describes the basic categories of information security controls that a due diligence team should review.

Chapter 5 focuses on the first stage of cybersecurity due diligence and outlines the due diligence process necessary to identify the target's high-value digital assets and to evaluate the relative importance of those assets to the target's business.

Chapter 6 focuses on the second stage of cybersecurity due diligence and discusses the due diligence process necessary to understand and evaluate the target's cybersecurity program.

Chapter 7 focuses on the third stage of cybersecurity due diligence and explains how to assess the target's cyber risk management efforts as they relate to third parties on which the target depends for goods, services, data, outsourced business functions, and joint business initiatives.

Chapter 8 addresses the fourth stage of cybersecurity due diligence and focuses on breaches a target experienced and its incident response capabilities. This chapter will help a due diligence team determine whether prior and ongoing cyber incidents have had a significant impact on the target's assets or operations.

Chapter 9 focuses on the fifth stage of cybersecurity due diligence: determining whether the target is in compliance with its cybersecurity legal obligations. This chapter will help a due diligence team identify applicable compliance requirements and evaluate the risks posed by any failure of such compliance.

Chapter 10 discusses "special issues" that, at first glance, may appear relevant only to a limited subset of M&A deals. However, a closer look illuminates practices that are important to cybersecurity due diligence in almost all M&A deals. The "special issues" include resilience of targets in regulated industries or critical infrastructure sectors, adoption of new communications technologies produced by a target that may contain undisclosed or unidentified cyber vulnerabilities, and reviews by the Committee on Foreign Investment in the United States.

Chapter 11 discusses how the results of the cybersecurity due diligence process may be used to identify risks to the transaction and the manners in which parties to a transaction may choose to allocate those cybersecurity risks as part of the transaction.

Chapter 12 reviews the representations and warranties the parties should consider for their M&A agreement to address cybersecurity and data privacy practices and compliance with related laws. It thus focuses on translating the results of M&A due diligence into representations and warranties that address any applicable cybersecurity risk.

Chapter 13 presents concluding observations that summarize some best practices in cybersecurity due diligence and emerging challenges to cybersecurity due diligence teams.