Preface

By Roland L. Trope and Thomas J. Smedinghoff

This guide is for M&A lawyers. It is designed for use when advising a client that plans to acquire a target whose key assets include high-value digital assets. This guide is also for a broad audience that includes the acquirer's officers, directors, general counsel, and outside counsel who want to improve their grasp of the cyber risks to an M&A deal and the importance of cybersecurity due diligence to the pursuit of the acquirer's deal objectives. In addition, this guide will be useful to security consultants that counsel might engage to assist in the due diligence process, and who may need a quick introduction to why their efforts should not be concentrated solely on technical details and to ways in which they might assist counsel.

Because of the devastating consequences that can result from a cybersecurity breach or other compromise of a target's digital assets, counsel should consider enhancing customary M&A due diligence with a cybersecurity due diligence review to improve the client's awareness of the risk that cyber incidents may devalue (or may already have devalued) the target's digital assets. This guide offers practical guidance on how to conduct such due diligence, as well as information that lawyers can use to persuade clients contemplating an M&A deal to incorporate a cybersecurity due diligence review as part of the tasks to be completed in the diligence process.

This guide grew out of the recognition that customary due diligence reviews in M&A deals often fail to assess the target's cybersecurity program or the risk of damage that may flow from cyber attacks to a target's digital assets, including those that may not have become front-page news or gone viral on the Internet. This omission reflects a long-standing practice: cybersecurity due diligence, where done, tends to be relegated to a subset of the review of a target's information technology assets. As a consequence, enterprise-wide cybersecurity issues might not receive the attention they merit in M&A due diligence reports. And for the same reason, definitive acquisition agreements might not adequately address cybersecurity issues.

In some cases, the limited focus on cybersecurity due diligence also reflects a lack of awareness of cybersecurity risks and their potential impact on M&A transactions. Although boards gradually have begun to recognize the need to add cybersecurity to their oversight of an enterprise's risk management and crisis management, that reasoning often is not applied in the M&A context.

Thus, M&A practice may at times overlook the significance of the cybersecurity risks facing targets, including the risk that cyber attacks could already be devaluing the digital assets of a target without the target's awareness and without the acquirer's knowledge.

Reports of such incidents suggest that officers and directors should anticipate that cyber attacks could extensively damage or modify an enterprise's digital assets, possibly disrupt an enterprise's operations and businesses, and may require disclosures to regulators and affected individuals and entities. By December 2014, such risks had become widely reported as demonstrated by the following bleak recap in *The New York Times*:

> In the last two years, breaches have hit the White House, the State Department, the top federal intelligence agency, the largest American bank, the top hospital operator, energy companies, retailers, and even the Postal Service.[1] In nearly every case, by the time the victims noticed that hackers were inside their systems, their most sensitive government secrets, trade secrets and customer data had already left the building. . . .[2] But the value [of stolen credit cards during this period] . . . which trade freely in underground criminal markets, is eclipsed by the value of the intellectual property that has been siphoned out of the United States corporations, universities and research groups by hackers in China—so much so that security experts now say there are only two types of companies left in the United States: those that have been hacked and those that do not yet know

1. This recap by *The New York Times* immediately preceded the disclosure of the North Korean attack on Sony Corporation in December 2014 and China's massive breach of the U.S. government's Office of Personnel Management in 2015.

2. For example, when Home Depot experienced a cyber intrusion that compromised upwards of 56 million credit cards, the attack reportedly had been going on for *five months*. See Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, Wall St. J., Sept. 18, 2014, *available at* http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

> they have been hacked. . . . Most large organizations have come to the painful recognition that they are already in some state of break-in today.[3]

Two-and-a-half years later, during the final editing of this book, numerous businesses, organizations, and governments found their digital data imperiled by a world-wide dispersal of two waves of malware.

The first wave, a ransomware attack dubbed "WannaCry," started on May 12, 2017. It infected "230,000 computers in 48 hours."[4] *WannaCry* locked down the computers it infected, and encrypted and rendered all of their stored data inaccessible. The malware then displayed a demand to each victim: either pay a ransom "into a particular account, of a sum in bitcoin, an electronic currency,"[5] or the data would be destroyed. The WannaCry worm caused kinetic effects—"paralyzing hospitals, disrupting transport networks, and immobilizing businesses."[6]

The second wave of malware, called "Petya," began on June 27, 2017. Although *Petya* demanded a ransom of $300 in Bitcoin to decrypt the victim's data, "the mechanisms ... to collect this money from victims in exchange for decryption keys quickly disintegrate[d]."[7] As it spread, *Petya* proved to have been "built to destroy, not extort."[8]

In fact, the emerging analyses revealed that, unlike ransomware, "[*Petya*] does not just encrypt files, which a company can back up, but affects a machine's ability to operate."[9] As one commentator noted, "'Petya [has] ... an evil twist: instead of encrypting files on disk, it will lock the

3. Nicole Perlroth, *Hacked vs. Hackers: Game On*, N.Y. Times, Dec. 3, 2014, at F-1, F-7.

4. *Id.*

5. *WonnaCry should make people treat cyber-crime seriously,* The Economist, May 20, 2017, *accessible at* http://www.economist.com/news/science-and-technology/21722158-it-has-been-neglected-tooMong-wannacry-should-rnake-people-treat-cyber-crime.

6. Sam Jones and Tim Bradshaw, *Global alert to prepare for fresh cyber attacks*, Financial Times, May 14, 2017, *accessible at* https://www.ft.com/content/bb4dda38-389f-11e7-821a-6027b8a20f23?mhq5j=e2.

7. Iain Thomson, *Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide,* The Register, June 28, 2017, *accessible at* https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/.

8. *Id.*

9. FT Reporters, *Security experts track initial infection*, Financial Times, June 29, 2017, p. 12.

entire disk, rendering it pretty much useless"[10] *Petya* severely disrupted operations of "some of the world's largest companies, including WPP, Roseneft,[11] Merck, ... AP Moller-Maersk[12] ... Saint-Bobain[13] and DLA Piper, the law firm."[14] For example:

- One day into the *Petya* attack, integrated transport and logistics company A.P. Moller-Maersk "tweeted" that the malware had brought down its "IT systems ... across multiple sites and select business units."[15] By the second day, Maersk had "shuttered many of its ports around the world."[16]
- Three days after the attack, thousands of lawyers at law firm DLA Piper "still couldn't access firm computer systems or emails and were mostly 'doing their best' from home computers ... DLA Piper's data blackout ... [had started] to disrupt active litigation ...[I]n at least five different civil cases in the U.S., including a patent dispute involving Apple, firm lawyers ... sought deadline extensions."[17]

Petya vividly demonstrated the cyber vulnerability of the operations of global enterprises. And it suggests that directors and officers of many sophisticated enterprises may have overestimated the resilience of their companies to cyberattacks, or that improvements in malware had rendered obsolete their previous estimates of sufficient resilience. Moreover, *Petya* showed the potential for hackers to interdict the progress of M&A transactions by making key documents inaccessible to clients and counsel.

---

10. Matt Burgess, *What is the Petya ransomware spreading across Europe? WIRED explains*, WIRED, June 29, 2017, *accessible at* http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017.
11. Russia's largest oil company.
12. The Danish shipping firm.
13. The large French construction firm.
14. FT Reporters, *Global groups hit by fresh ransomware cyber attack*, Financial Times, June 28, 2017, p. 11.
15. A.P. Moller-Maersk, *Twitter Post*, June 27, 2017, *accessible at* https://twitter.com/Maersk.
16. Nick Kostov and Costas Paris, *Companies Try to Contain Fallout From Global Cyberattack*, The Wall Street Journal, June 28, 2017, 5:27 p.m. ET, *accessible at* https://www.wsj.com/articles/fallout-from-global-cyberattack-extends-into-second-day-1498639146.
17. Jacob Gershman and Kate Fazzini, *Global Law Firm DLA Piper Faces Disruptions After Cyberattack*, The Wall Street Journal, June 29, 2017, 3:16 p.m. ET, *accessible at* https://www.wsj.com/articles/global-law-firm-dla-piper-faces-disruptions-after-cyberattack-1498763817.

As Columbia Law School professor John Coffee observed: "Suddenly encrypting deal documents in a merger essential freezes it."[18]

Despite the ubiquity of cyber incidents, the capacity of attackers to hit specific targeted enterprises, and the sophistication, speed, global reach, and disruptive impact of cyberattacks, such risks appear to remain "below the radar," be underestimated, or belatedly addressed, in M&A deals. Denial of cyber risks and a denial of the imminence and magnitude of those risks appears to persist in boardrooms and C-suite offices, notwithstanding the fact that the costs to respond and remediate a damaging cyber incident and the amounts reserved to cover potential data breach liability can be prodigious. For example, in 2014, Target Corp experienced a breach of its networks affecting 40 million credit- and debit-card numbers and personal identifiable information for up to 70 million individuals. The remediation costs had a material impact on the company. Target eventually reported that it "incurred $252 million of cumulative Data Breach-related expenses, partially offset by $90 million of expected insurance recoveries, for net cumulative expenses of $162 million."[19]

A cautionary premise of this guide is that, if a target's digital assets can be accessed through the target's computer networks (whether via an internal port, a wireless signal, or an Internet link), those digital assets are cyber-vulnerable. There is a strong likelihood that the target has experienced multiple cyber incidents. Some of the incidents will have originated inside the enterprise, some from outside, and some may have involved coordinated inside and outside access to the target's high-value digital assets. If a cyber attack succeeds in gaining access to such assets, its perpetrators will seek to misuse, modify, or damage the data.

With the value of so many enterprises dependent upon the condition of their high-value digital assets, and with so many of those assets cyber-vulnerable, consideration of adding a cybersecurity due diligence review would seem a good and prudent precaution at the start of any proposed M&A deal.

In this guide, practicing lawyers, including those who advise clients in M&A transactions on a regular basis, offer their insights into how to conduct cybersecurity due diligence reviews. Each chapter addresses a

18. Stu Sjouwerman, *NotPetyya 'ransomware' Froze Business At Global Law Firm DLA Piper*, KnowBe4, [undated], *accessible at* https://blog.knowbe4.com/notpetya-froze-business-at-global-law-firm-dla-piper.

19. Target Corp. 10K—2014 Annual Report 77 (filed March 13, 2015, p. 17, *available at* https://corporate.target.com/_media/TargetCorp/annualreports/2014/pdf/10K-Target-2014-Annual-Report-5.pdf.

different aspect of the cybersecurity due diligence process. The Introduction includes a summary of the contents of each chapter and the tasks that each chapter can help counsel undertake. For clarity, the authors have made limited use of technical vocabulary in this guide.

This guide comes with three crucial caveats. First, the resources contained herein are not intended to prepare an M&A lawyer to function as a cybersecurity consultant. Instead, it is assumed that counsel will work with cybersecurity professionals as needed to structure the due diligence process and interpret its results.

Second, this guide is a resource, not a manual. It can be used to improve an M&A due diligence review, but it will not help counsel determine whether and where an enterprise may be experiencing a cyber incident. Proper use of this guide should significantly improve a due diligence team's ability to identify and report cybersecurity issues that may be significant enough to warrant consideration when negotiating the definitive acquisition agreement, but it will not reduce the uncertainties that the cyber threats and cyber incidents pose to M&A deals in the digital era. Early awareness of those uncertainties and of their potential impact on the value of the target's digital assets puts the client in a position to decide whether, and how, to address them.

Third, this guide does not offer examples of M&A provisions that address cybersecurity risks. The ABA Business Law Section and the ABA's Cybersecurity Legal Task Force publish several outstanding guides that discuss representative M&A provisions.[20] To venture into such discussions would take this guide beyond its objectives. Moreover, given that M&A deals tend to be unique and that cyber incidents add complexities to the deal, it is doubtful that attempting a general discussion of cybersecurity provisions would be a helpful or welcome resource to counsel.

The editors wish to thank each of the other contributing authors for their dedication, time, and efforts:

Jonathan P. Adams, Senior Privacy Counsel, LinkedIn Corporation, San Francisco, CA

Robert Bond, Partner, Bristows LLP, London, England

William R. Denny, Partner, Potter Anderson & Corroon LLP, Wilmington, DE

David Flint, Senior Partner, MacRoberts LLP, Glasgow, Scotland

20. *See, e.g.*, ABA Sec. of Bus. Law Negotiated Acquisitions Comm., Model Stock Purchase Agreement With Commentary, Second Edition (2010); Jill Rhodes & Robert S. Litt, The ABA Cybersecurity Handbook, Second Edition (2017).

CANDACE JONES, Counsel and Vice President, Federal Reserve Bank of New York, New York City

STUART D. LEVI, Partner, Skadden, Arps, Slate, Meagher & Flom LLP, New York City

MATTHEW STAPLES, Of Counsel, Wilson Sonsini Goodrich & Rosati PC, Seattle, WA

By volunteering, they made it possible to embark on this endeavor. By writing well, they made this guide worth reading. We hope it proves a useful resource.