NEW YORK LAW SCHOOL

NYLS Law Review

Volume 67 | Issue 2 Article 4

January 2022

Cyberattacks and Material Adverse Effect Clauses in M&A Transactions: A Proposed Hack

Staff Editor

VOLUME 67 | 2022/23

STAFF

Cyberattacks and Material Adverse Effect Clauses in M&A Transactions: A Proposed Hack

67 N.Y.L. Sch. L. Rev. 115 (2022–2023)

ABOUT THE AUTHOR: This Note was written by a Staff Editor of the 2021–2022 *New York Law School Law Review*. They received their J.D. from New York Law School in 2022. The author received editorial assistance from a member of the 2021–2022 *New York Law School Law Review*. They received their J.D. from New York Law School in 2022.

> "*We live in a world where it appears to be a matter of when, not if, an enterprise is breached.*"[1]

I. INTRODUCTION

Computer screen after computer screen went black at Maersk headquarters in Copenhagen on June 27, 2017.[2] With its computer network paralyzed, the world's largest shipping company ground to a halt.[3] Worldwide, chaos ensued across the seventy-six ports and nearly eight hundred ships operated by the company.[4] Maersk had fallen victim to NotPetya.[5] Then the most damaging cyberattack[6] in history, NotPetya had been launched by Russian military intelligence agents to disrupt Ukrainian businesses, but the attack spread around the globe, harming companies in over sixty countries[7] and causing more than $10 billion in damages.[8]

Cyberattacks threaten everyone.[9] From personal laptops to corporate and government networks, no computer is beyond a hacker's[10] reach.[11] And as dependence on computer networks continues to deepen, new opportunities present for cyber attackers to cripple critical infrastructure.[12]

---

1. Gaurav Banga, *How Three Waves of Cybersecurity Innovation Led Us Here*, Forbes (Oct. 10, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/10/10/how-three-waves-of-cyber-security-innovation-led-us-here/?sh=6eb06a8143d7.

2. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

3. *Id.*

4. *Id.*

5. Matteo Crosignani et al., Fed. Rsrv. Bank of N.Y., Pirates Without Borders: The Propagation of Cyberattacks Through Firms' Supply Chains 1–2 (2021).

6. This Note uses the terms "cyberattack," "cyber incident," and "cyber threat" interchangeably, to refer to "an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems." U.S. Dep't of Homeland Sec., Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government (2023).

7. Other corporations afflicted by NotPetya include pharmaceutical company Merck, which was unable to supply vaccines to the Center for Disease Control, and a subsidiary of delivery company FedEx, which could not process shipments. Crosignani et al., *supra* note 5, at 2, 7 tbl.1.

8. Zaheer Merchant, *NotPetya: The Cyberattack that Shook the World*, Econ. Times (Mar. 4, 2022), https://economictimes.indiatimes.com/tech/newsletters/ettech-unwrapped/notpetya-the-cyberattack-that-shook-the-world/articleshow/89997076.cms?from=mdr.

9. *See* Daniel J. Solove & Paul M. Schwartz, Information Privacy Law 1–2 (7th ed. 2021).

10. This Note uses the terms "hacker," "cyber attacker," and "cyber actor" interchangeably, to refer to an entity responsible for a cyberattack. *See What Is a Data Breach?*, IBM, https://www.ibm.com/topics/data-breach (last visited Apr. 19, 2023) (noting that cyber threats come from "outsiders" like organized criminals or state-sponsored actors, as well as from "insiders" like disgruntled employees).

11. *See* Solove & Schwartz, *supra* note 9, at 1–2.

12. Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, Cybercrime Mag. (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Particularly vulnerable to cyberattacks are companies, due to their large-scale reliance on electronic records, digital communications, and computer networks.[13] Hackers exploit this dependence to spread malware[14] quickly and globally.[15] Moreover, companies retain troves of valuable digital assets[16] and Personally Identifiable Information (PII),[17] rendering them highly attractive targets for cyber attackers.[18]

The threat that cyberattacks pose to companies in the merger and acquisition (M&A)[19] context is especially acute.[20] Most M&A deals are not signed and closed simultaneously; instead, a deal may take a year or more to close after the acquisition agreement[21] is executed.[22] This lapse in time, coupled with the increasing frequency of cyberattacks on business enterprises,[23] exposes M&A deal constituents—particularly buyers[24]—to significant risks.[25]

13. *See* Roland L. Trope, *The Importance of Cybersecurity Due Diligence for an M&A Deal*, *in* Guide to Cybersecurity Due Diligence in M&A Transactions 10 (Thomas J. Smedinghoff & Roland L. Trope eds., 2017).

14. "Malware," also known as "malicious software," is intrusive software designed to damage or destroy computers and computer networks. *What Is Malware?*, Cisco, https://www.cisco.com/site/us/en/products/security/what-is-malware.html (last visited Apr. 19, 2023).

15. *See* Crosignani et al., *supra* note 5, at 5.

16. "Digital asset" refers to any electronic file of data that can be owned, transferred, and stored digitally. Matthew Vincent, *What Are Digital Assets and How Does Blockchain Work?*, Fin. Times (Oct. 20, 2021), https://www.ft.com/content/2691366f-d381-40cd-a769-6559779151c2. Examples of digital assets owned by businesses include cryptocurrencies, intellectual property, business plans and strategies, operational and production data, and personal information of customers and employees. *See id.*; Trope, *supra* note 13, at 9–10.

17. "PII" is information that can be used to trace an individual's identity, including their name, home address, telephone number, email address, and the like. 2 C.F.R. § 200.1 (2023).

18. *See* Barracuda, Spear Phishing: Top Threats and Trends 9 (2022).

19. In a "merger," one firm absorbs the assets and liabilities of another firm that merges out of existence, while in an "acquisition," one firm purchases all or substantially all of the assets or the controlling stock of another firm. Dale A. Oesterle & Jeffrey J. Haas, The Law of Mergers and Acquisitions 2–3 (5th ed. 2018).

20. *See* Forescout, The Role of Cybersecurity in Mergers and Acquisitions Diligence 5 (2019) (finding that, of the nearly three thousand information technology and M&A decisionmakers surveyed, 53 percent reported that their firm had experienced a cybersecurity issue that jeopardized an M&A deal).

21. The term "acquisition agreement" refers to the negotiated contract that governs either a merger or acquisition transaction. *See* Oesterle & Haas, *supra* note 19, at 335–36.

22. *See id.* at 15–17.

23. Jim Boehm et al., *Cybersecurity Trends: Looking over the Horizon*, McKinsey & Co. (Mar. 10, 2022), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon.

24. *See* Oesterle & Haas, *supra* note 19, at 17.

The meanings of the terms "buyer" and "seller" in the M&A context depend on the type of transaction at hand. In a merger, the buyer is the surviving company that absorbs the assets and liabilities of another company, the seller, which is merged out of existence. *Id.* at 2–3. In an acquisition, the buyer is the acquirer of all or substantially all of the assets or the controlling stock of another company, the seller. *Id.*

25. *See* Trope, *supra* note 13, at 15–18.

After the parties to an M&A transaction sign the acquisition agreement, a cyberattack on the seller before the deal closes could prove devastating to the seller's business and thus to the transaction. This is because a cyberattack on a targeted company[26] disrupts business operations, reduces revenue, frustrates customer and supplier relationships, and threatens the company's exclusive control over its intellectual property.[27] Further, the PII that a targeted company stores may be compromised, exposing the company to expensive, lengthy litigation and reputational damage.[28]

Drastic deterioration of a seller's business due to a cyberattack raises novel questions in the M&A context: Can the buyer escape the deal? Or can the seller compel the buyer to close notwithstanding the cyberattack? The answer depends on how the parties drafted the Material Adverse Effect (MAE) clause in their acquisition agreement. An MAE clause entitles the buyer to refuse to close the deal should the seller suffer an event that results in a "material adverse effect" on its business.[29]

The issue of whether a cyberattack on a seller gives rise to an MAE has not yet been litigated.[30] But given the prevalence of corporate cyberattacks today, impending litigation is anticipated.[31] Accordingly, this Note delineates factors for a court to consider when confronted with the novel issue of whether a buyer should be excused from closing an M&A deal on the theory that a cyberattack on the seller induced an MAE.

Part II of this Note reviews the purpose and structure of MAE clauses. Part III addresses the traditional analysis courts have applied when determining whether the effects of an event on a seller's business are material enough to constitute an MAE. Part IV illustrates the inadequacies of this traditional approach as applied to cyber incidents and analyzes the dangers such incidents present to M&A activity. Part V responds first by proposing factors to guide a court's MAE analysis when a seller suffers a cyberattack, and then by suggesting a measure parties should take to mitigate the threats that cyberattacks pose to M&A deals. Part VI concludes this Note.

---

26. In this Note, the term "targeted company" means a company subjected to a cyberattack.

27. *See* Deloitte, CFO Insights: Seven Hidden Costs of a Cyberattack 2–3 (2016).

28. *See* Elizabeth Weise, *Yahoo to Pay $35 Million for Leaving Investors in the Dark About 2014 Breach*, USA TODAY (Apr. 24, 2018), https://www.usatoday.com/story/tech/2018/04/24/yahoo-pay-35-million-leaving-investors-dark-2014-breach/546408002/.

29. *See* Oesterle & Haas, *supra* note 19, at 363.

30. Indeed, few MAE-related disputes have reached any court judgment, as most result in settlement or renegotiation of the acquisition agreement. Gail Weinstein et al., *COVID-19 as a Material Adverse Effect (MAC) Under M&A and Financing Agreements*, Harv. L. Sch. F. on Corp. Governance (Apr. 4, 2020), https://corpgov.law.harvard.edu/2020/04/04/covid-19-as-a-material-adverse-effect-mac-under-ma-and-financing-agreements/.

31. *See* Alan S. Wernick, *Mergers & Acquisitions: Cybersecurity Traps for the Seller & Buyer*, Wolters Kluwer: Sec. Regul. Daily (Apr. 5, 2020), https://www.agdglaw.com/FFDBF8/assets/files/lawarticles/M&A_Cybersecurity%20Traps%20for%20the%20Seller%20&%20Buyer_Alan%20S.%20Wernick%208-5-20.pdf.

II. THE PURPOSE AND STRUCTURE OF MAE CLAUSES

Business leaders are conscious of the devastating effects that sudden, harmful events can have on their enterprises.[32] Parties to ordinary commercial transactions therefore build into their contracts such protections as force majeure clauses, which may excuse a party from its contractual obligations when certain events render their performance impossible or impracticable.[33] These contract law doctrines, however, are generally absent from acquisition agreements.[34] This is because adverse effects on a seller's business typically render a buyer's obligation to perform unattractive, though not impossible or impracticable.[35] Instead, the parties to an M&A deal negotiate to allocate risk should a harmful change to the seller's business occur between the signing and closing of the deal.[36] The result of this negotiation is memorialized in the acquisition agreement's MAE clause.

Typically located in the Defined Terms section of an acquisition agreement,[37] an MAE clause identifies the harmful events that excuse a buyer's obligation to acquire a seller that has been materially impacted by such an event.[38] Practically, an MAE clause works as a risk-allocation device that reflects the expectations of a buyer signing an acquisition agreement: that the seller will remain an attractive target until closing and that, if the seller's business falters, the buyer will be afforded some opportunity to renegotiate or terminate the deal.[39] This measure is a prudent one; the lapse of time between the signing and closing of an M&A deal, known as the "executory period," can be lengthy.[40] And the longer the executory period lasts, the greater the risk is that the seller will suffer an MAE.

---

32. *See* Deloitte, M&A Trends Survey: The Future of M&A 13 (2020) (reporting that more than half of the one thousand executives polled considered cybersecurity threats their top concern in executing M&A deals). For example, in 2019 Bob Dudley, then chief executive officer of the major oil and gas company BP Plc, shared that his largest concern aside from the transition away from fossil fuels was the threat of a cyberattack. David Voreacos et al., *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, Bloomberg News (Dec. 3, 2019), https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war.

33. 14 Timothy Murray, Corbin on Contracts § 74.19, LEXIS (database updated Nov. 2022).

34. Benjamin Horney, *Why Force Majeure Isn't a Golden Ticket Out of M&A Deals*, Law360 (Apr. 20, 2020), https://www.law360.com/articles/1265259/why-force-majeure-isn-t-a-golden-ticket-out-of-m-a-deals.

35. *See id.*

36. *See* Oesterle & Haas, *supra* note 19, at 337–38.

37. The Defined Terms section, typically found at the beginning of an acquisition agreement, delineates the meanings of particular words or phrases as they are to be used throughout the agreement. *Id.* at 336.

38. *Id.* at 337–38.

39. *See id.* at 363.

40. *See id.* at 15–17 (noting that an executory period can be especially long if the deal involves a publicly traded company subject to extensive pre-closing regulatory approvals); Grace Maral Burnett, *Analysis: Over $2.5T in Signed 2020–2021 M&A Deals Await Closing*, Bloomberg L. (Oct. 5, 2021), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-over-2-5t-in-signed-2020-2021-m-a-deals-await-closing ("[M]ore than 21,000 global deals announced since the start of 2020, valued at a total $2.5 trillion, remain pending in the period between signing and closing.").

Nearly all acquisition agreements contain an MAE clause divided into three components that allocate risk between the buyer and seller.[41] The first component defines an "MAE" broadly;[42] the second component serves a carve-out function, exempting certain events from the broad definition in the first component; and the third component, somewhat circularly, establishes exceptions to the carve-outs set forth in the second component.[43] This Note focuses on the first two components.

Little debate arises over the first component of an MAE clause. Rather, negotiations center on the second component, which limits the broad scope of an MAE by enumerating certain events that will not excuse a buyer's performance.[44] The parties have competing priorities here. While the seller favors an extensive carve-out list, the buyer prefers a narrow one.[45]

III. THE TRADITIONAL MAE APPROACH

An MAE clause is typically referenced in multiple locations throughout an acquisition agreement.[46] It is featured most prominently, though, in the General MAE Condition, the operative provision conditioning the parties' obligation to close the deal on the seller not suffering an MAE.[47] Accordingly, if during the executory period the seller sustains an MAE as defined in the MAE clause, the buyer's duty to purchase the seller is excused under the General MAE Condition.

When determining whether an event meets the General MAE Condition, courts apply a tripartite burden-shifting framework that tracks the three-part structure of

---

41. *See* Robert T. Miller, *Pandemic Risk and the Interpretation of Exceptions in MAE Clauses*, 46 J. Corp. L. 681, 685–87 tbl.1 (2021).

42. The typical practice is to define "MAE" self-referentially, as an event that has a "material adverse effect" on a seller's business. Akorn, Inc. v. Fresenius Kabi AG, No. 2018-0300, 2018 WL 4719347, at *52 (Del. Ch. Oct. 1), *aff'd*, 198 A.3d 724 (Del. 2018).

43. *See, e.g.*, *id.* at *50–51.

44. Andrew M. Herman & Bernardo L. Piereck, *Revisiting the MAC Clause in Transaction*, Bus. L. Today, Aug. 2, 2010, at 1.

45. Carl L. Reisner et al., *Material Adverse Clauses: Practice in an Uncertain World*, 10 M&A Law. 1, 1 (2006).
Generally, the seller accepts company-specific risks, while the buyer assumes general market or industry risks. *Akorn, Inc.*, 2018 WL 4719347, at *50. Company-specific risks typically include events over which the company has control, including issues related to ordinary business operations such as the loss of a critical customer or a products liability lawsuit arising from defective products. *See* Robert T. Miller, *The Economics of Deal Risk: Allocating Risk Through MAC Clauses in Business Combination Agreements*, 50 Wm. & Mary L. Rev. 2007, 2073 (2009); *see, e.g.*, *Akorn, Inc.*, 2018 WL 4719347, at *51. General market or industry risks, on the other hand, stem from events affecting the financial markets, including natural disasters, acts of war, military activity, sabotage, and terrorism. Miller, *supra*, at 2071; *see, e.g.*, *Akorn, Inc.*, 2018 WL 4719347, at *51.

46. *See Akorn, Inc.*, 2018 WL 4719347, at *46. Usually, the MAE clause is cited "(i) in the General MAE Condition, (ii) in various representations for purposes of evaluating any inaccuracies in those representations at the time of signing, and (iii) in the Bring-Down Condition." *Id.* This multilocation deployment of the MAE clause gives a buyer several grounds on which to argue that an adverse change in the seller's business entitles the buyer to escape the deal. *See id.*

47. *See id.* at *45 & n.514.

the MAE clause. First, the buyer bears the burden of proof to show that the event caused the seller to endure an MAE as defined in component one of the MAE clause.[48] The burden then shifts to the seller to prove that the event falls within a carve-out enumerated in component two.[49] Last, the burden of proof shifts back to the buyer to counter that, under component three of the MAE clause, the event is excluded from the carve-out provision.[50]

A. Component One: Buyer to Show that Seller Suffered an MAE

To meet its initial burden under the General MAE Condition analysis, the buyer must show that an event materially harmed the seller's business.[51] Most MAE clauses do not define the term "material."[52] But under Delaware law,[53] the materiality threshold is satisfied if an adverse change in the seller's business "substantially threaten[s] the overall earnings potential of the [seller] in a durationally-significant manner."[54] A two-part showing is thus required to prove materiality: The buyer must establish that the adverse effect on the seller's business is one of (1) substantial magnitude and (2) durational significance.[55] This is a high threshold—one that is "difficult, if not impossible," for a buyer to meet.[56]

Taking each requirement in turn, first, to determine whether an adverse effect on the seller's business is one of substantial magnitude, courts assess the value and overall earnings potential of the seller, and consider the extent to which either is compromised by the event.[57] Delaware courts have routinely found the substantial

48. Bardy Diagnostics, Inc. v. Hill-Rom, Inc., No. 2021-0175, 2021 WL 2886188, at *22 (Del. Ch. July 9, 2021).

49. *Id.*

50. *Id.*

51. *See Akorn, Inc.*, 2018 WL 4719347, at *47–48.

52. *Id.* at *48. The benefits of not defining "material" in the MAE clause are twofold. First, leaving the term undefined provides parties the option to renegotiate the deal price should conditions change during the executory period, before litigating whether the materiality threshold is met. *Id.* Second, without a materiality definition, the MAE clause applies broadly and is not limited to a set of specific quantitative thresholds that may not be applicable to all potential events. *Id.*

53. This Note focuses on case law from Delaware: the most common forum for M&A disputes. John Coates, *M&A Contracts: Purposes, Types, Regulation, and Patterns of Practice* 20 (Eur. Corp. Governance Inst., L. Working Paper No. 292/2015, 2015).

54. *In re* IBP, Inc. S'holders Litig., 789 A.2d 14, 68 (Del. Ch. 2001).

55. *See Akorn, Inc.*, 2018 WL 4719347, at *52–57.

56. Lewis H. Lazarus & Jason Jowers, '*Material Adverse Change*' *Clauses Protect Against Loss of Customers and Suppliers*, 25 Westlaw J. Del. Corp. 1, 1 (2011). Indeed, at the time this Note was written and edited for this publication, the 2018 case *Akorn, Inc. v. Fresenius Kabi AG* was the only instance in history of a Delaware court permitting a buyer to terminate an acquisition agreement because the seller experienced an MAE. Robert Malionek & Jon Weichselbaum, *Five Keys to Analyzing a Material Adverse Effect*, N.Y.L.J. (Mar. 6, 2019), https://www.law.com/newyorklawjournal/2019/03/05/five-keys-to-analyzing-a-material-adverse-effect/?slreturn=20230226155111.

57. *See Akorn, Inc.*, 2018 WL 4719347, at *53–56.

magnitude prong satisfied when the event in question causes the seller's profits to decrease by at least 40 percent,[58] though no one metric is dispositive.[59]

Illustrative of this standard is the Delaware Court of Chancery's 2018 landmark decision *Akorn, Inc. v. Fresenius Kabi AG*.[60] There, the court concluded that the seller's pre-closing business decline was of substantial magnitude based on the aggregate evidence presented by the buyer, which included the seller's year-over-year declines of 25 percent in revenue; 86 percent in earnings before interest, taxes, depreciation, and amortization (EBITDA);[61] 113 percent in earnings per share (EPS);[62] and 105 percent in operating income.[63]

As to the second requirement for materiality, an adverse effect is of durational significance when the harm to the seller's long-term earnings power has lasted or is expected to last for a "commercially reasonable period."[64] Although such a period is typically "measured in years rather than months,"[65] the threshold is not fixed.[66]

---

58. Lou R. Kling et al., Negotiated Acquisitions of Companies, Subsidiaries and Divisions § 11.04[9] (2022); *see, e.g.*, Raskin v. Birmingham Steel Corp., No. 11365, 1990 WL 193326, at *5 (Del. Ch. Dec. 4, 1990) (observing that a 50 percent decline in the seller's earnings over two consecutive quarters would likely constitute an MAE); Hexion Specialty Chems., Inc. v. Huntsman Corp., 965 A.2d 715, 742 (Del. Ch. 2008) (holding that the substantial magnitude prong was not met when the seller's earnings in 2007, following the event, were only 3 percent below its 2006 earnings, while its projected earnings for 2008 fell only 7 percent below the 2007 figure).

59. *Akorn, Inc.*, 2018 WL 4719347, at *53 (noting that precedent such as *Raskin* neither "foreclose[s] the possibility that a buyer could show that percentage changes of a lesser magnitude constituted an MAE" nor "exclude[s] the possibility that a buyer might fail to prove that percentage changes of a greater magnitude constituted an MAE"); *see, e.g.*, *In re IBP, Inc. S'holders Litig.*, 789 A.2d at 69–71 (concluding that the substantial magnitude prong was not satisfied even though the seller experienced a 64 percent drop in first-quarter earnings compared to the previous year).

60. 2018 WL 4719347.

61. "EBITDA" measures a company's overall financial performance by considering the company's earnings without the influence of certain accounting and financial deductions. *EBITDA*, Black's Law Dictionary (11th ed. 2019).

62. "EPS" gauges a company's profitability by viewing its net income in relation to the outstanding shares of its common stock. *Earnings Per Share*, Black's Law Dictionary (11th ed. 2019).

63. *Akorn, Inc.*, 2018 WL 4719347, at *54–55.

64. *Id.* at *53 (quoting Hexion Specialty Chems., Inc. v. Huntsman Corp., 965 A.2d 715, 738 (Del. Ch. 2008)). The adverse effect must be material from the long-term perspective of a prudent buyer. *In re IBP, Inc. S'holders Litig.*, 789 A.2d at 68. Indeed, absent evidence indicating otherwise, courts assume that a buyer seeks to acquire a seller with a view toward long-term strategy. *Hexion Specialty Chems., Inc.*, 965 A.2d at 738.

65. *In re IBP, Inc. S'holders Litig.*, 789 A.2d at 67–68 ("A short-term hiccup in earnings should not suffice . . . .").

66. *Compare id.* at 65–71 (holding that the materiality requirement was not satisfied when the buyer failed to show that a short-term drop in the seller's earnings would translate into a continued decline in the company's value), *with* Frontier Oil Corp. v. Holly Corp., No. 20502, 2005 WL 1039027, at *37 (Del. Ch. Apr. 29, 2005) (concluding that the materiality threshold was not met because the parties' "forward-looking basis for evaluating an MAE . . . d[id] not allow the [c]ourt to look at just one year" of the effect on the seller's business), *and Akorn, Inc.*, 2018 WL 4719347, at *53 n.551 (positing that the durational significance requirement "may not apply when the buyer is a financial investor with an eye to a short-

Rather, it depends on the context of the transaction, the characteristics of the parties, and the expectations of the buyer.[67]

For example, in the 2021 case *Bardy Diagnostics, Inc. v. Hill-Rom, Inc.*, the Delaware Court of Chancery held that an adverse effect on the seller, forecast to last two years, was not durationally material.[68] Because the buyer had agreed to acquire the seller, a startup company projected to generate no profit for at least three years, the court determined that the two-year lag was insufficient to affect the continued viability of the purchase agreement.[69]

B. Component Two: Seller to Show that the Event Is Carved Out

If the buyer establishes that the event caused the seller's business an adverse effect of both substantial magnitude and durational significance, the court will find the materiality requirement satisfied and conclude that the seller suffered an MAE as defined in component one of the MAE clause.[70] The burden then shifts to the seller, who must show that the triggering event is carved out from this definition by component two of the MAE clause.[71]

IV. CYBERATTACKS ON SELLERS: INADEQUACIES OF THE TRADITIONAL MAE APPROACH AND NARROW MAE CLAUSES

Most buyers do not conduct cybersecurity assessments in the early stages of their due diligence[72] efforts.[73] There are several reasons for this. Some buyers are inexperienced with the complexities of M&A deals or are unfamiliar with the risks that cyberattacks pose during the executory period, while others wish to restrict the number of parties with knowledge of a forthcoming deal.[74]

---

term gain" (quoting Albert Choi & George Triantis, *Strategic Vagueness in Contract Design: The Case of Corporate Acquisitions*, 119 Yale L.J. 848, 877 (2010))).

67. *See* Bardy Diagnostics, Inc., v. Hill-Rom, Inc., No. 2021-0175, 2021 WL 2886188, at *27 (Del. Ch. July 9, 2021).

68. *Id.*

69. *Id.*

70. *See Akorn, Inc.*, 2018 WL 4719347, at *52–58.

71. *See id.* at *58–60.

72. "Due diligence" refers to the buyer's investigation of the seller's business to audit and confirm the accuracy of factual representations made by the seller about its business. *See* Oesterle & Haas, *supra* note 19, at 14.

73. Julian Meyrick et al., IBM, Benchmark Insights: Assessing Cyber Risk in M&A 4 fig.2 (2020) (reporting that, of the 720 buyers that participated in the study, more than half did not conduct cybersecurity assessments until after due diligence had been completed).

74. *Id.* at 3.

In lieu of pre-negotiation cybersecurity assessments, some buyers seek specific representations and warranties[75] allocating liability for cyber incidents to sellers.[76] But sellers do not always agree to this.[77] Consequently, when a cyberattack affects an M&A deal governed by an acquisition agreement silent as to liability for cyber incidents, the parties must fall back on the General MAE Condition.

Despite the frequency of corporate cyber incidents today,[78] the issue of whether a cyberattack on a seller causes an MAE has not been litigated. Likely, this is because buyers use the General MAE Condition as leverage to renegotiate the purchase price of a deal, rather than as a means to terminate an acquisition agreement.[79] Practically speaking, renegotiation is preferred by both parties over costly, lengthy, and unpredictable litigation.[80] But when negotiations fail and litigation ensues, the court presiding over the case of first impression will have little precedent to guide its analysis.

Though the traditional MAE approach would control such an analysis, challenges present when applying it to cyberattacks. In particular, the materiality inquiry is frustrated by a "lack of effective metrics, tools and frameworks" to measure the adverse effects of a cyberattack on a seller's business.[81]

To evaluate the magnitude of an event, the traditional approach contemplates the effect on the seller's value and overall earnings potential—an inquiry that has historically focused on the tangible costs flowing from the event.[82] But these traditional metrics fail to appreciate the cascade of effects that a cyberattack inflicts on a seller's business,

75. A "representation" is a statement of fact that a party to an M&A transaction asserts about its business, while a "warranty" is a guarantee from that party that its representation is true and correct. Oesterle & Haas, *supra* note 19, at 350. Should a party's representations and warranties not remain true and correct until closing, the other party can elect to escape the deal or renegotiate the purchase price downward. *Id.* at 351.

76. *See* Jessica C. Pearlman et al., Am. Bar Ass'n, Private Target Mergers & Acquisitions Deal Points Study 46 (2019) (reporting that 70 percent of the acquisition agreements reviewed for the study contained a cybersecurity representation favoring the buyer).

77. *See id.*

78. Boehm et al., *supra* note 23; *see also* Etay Maor, *Cyberattacks 2022: Key Observations and Takeaways*, Forbes (Oct. 28, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/10/28/cyberattacks-2022-key-observations-and-takeaways/?sh=40b72c31f055 (reporting that cyberattacks in the first six months of 2022 increased by 42 percent compared to the first half of 2021).

79. *See* Weinstein et al., *supra* note 30.

80. *See* Damian McNair, PricewaterhouseCoopers, Material Adverse Change Clauses 5 (2016).

For example, in 2016, Verizon signed an acquisition agreement to purchase most of Yahoo!'s assets for more than $4.8 billion. Natalie M. Jersak, Article, *"Can You Buy Me Now?": The Erratic Closing of the Verizon-Yahoo Merger*, 36 Rev. Banking & Fin. L. 544, 544 (2017). Before the deal closed, Yahoo! disclosed that it had endured two massive data breaches in 2013 and 2014 that compromised well over one billion accounts. *Id.* The acquisition agreement's MAE clause was Verizon's best option to exit the deal, yet Verizon chose to leverage the MAE provision to renegotiate and lower the purchase price by $350 million. *Id.* at 544–45.

81. *See* Ioannis Agrafiotis et al., *A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate*, 4 J. Cybersecurity 1, 5 (2018).

82. *See, e.g.*, Raskin v. Birmingham Steel Corp., No. 11365, 1990 WL 193326, at *5 (Del. Ch. Dec. 4, 1990); *In re* IBP, Inc. S'holders Litig., 789 A.2d 14, 65–71 (Del. Ch. 2001); Hexion Specialty Chems.,

including the many intangible ramifications difficult to quantify in dollars but nonetheless harmful.[83] Moreover, determining the durational significance of a cyberattack requires an acute understanding of both short- and long-term consequences.[84] Yet the court lacks any precedent for defining a "commercially reasonable period" in the cyberattack context.

These challenges are amplified by the unique nature of each cyberattack. The effects of a given cyberattack depend on the mélange of many factors: the sophistication and motive of the cyber actor,[85] the lapse of time between the unauthorized intrusion and its detection,[86] the targeted company's existing cybersecurity,[87] the industry in which the targeted company operates,[88] and the data and digital assets exposed.[89] Thus, the nature and severity of a cyberattack will fluctuate based on the variables at play, necessitating the need for a flexible, fact-intensive approach to determine whether the adverse effects of a cyberattack on a seller are material.

An additional complication arises concerning the second component of the traditional MAE approach. Today, the frequency of corporate cyber incidents significantly increases the probability of a cyber-related MAE on a seller. Indeed, U.S. executives contemplating M&A deals rank cyberattacks among their greatest concerns.[90] Without a well-negotiated carve-out provision, a buyer risks acquiring a

Inc. v. Huntsman Corp., 965 A.2d 715, 740–43 (Del. Ch. 2008); Akorn, Inc. v. Fresenius Kabi AG, No. 2018-0300, 2018 WL 4719347, at *54–56 (Del. Ch. Oct. 1), *aff'd*, 198 A.3d 724 (Del. 2018).

83. *See generally* Deloitte, *supra* note 27.

84. *See* Emily Mossburg et al., Deloitte, Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts 14 (2016); *Businesses Underestimate Long-Term Effects of Cyber Attacks: Lloyd's Report*, Ins. J. (June 28, 2017), https://www.insurancejournal.com/news/international/2017/06/28/455973.htm.

85. *See* David Carmiel, *5 Trends Shaping the Future of Cybercrime Threat Intelligence*, Forbes (Dec. 19, 2022), https://www.forbes.com/sites/forbestechcouncil/2022/12/19/5-trends-shaping-the-future-of-cybercrime-threat-intelligence/?sh=54b7425530a6.

86. For example, a 2021 study of data breaches revealed that those not identified and contained within two hundred days cost the targeted company $4.87 million on average, while those taking less than two hundred days to identify and contain cost an average of $3.61 million. IBM, Cost of a Data Breach Report 6 (2021). Moreover, the average time it took targeted companies to identify and contain a data breach averaged 287 days: a timeframe longer than most executory periods for M&A deals. *Compare id.*, *with* Grace Maral Burnett & Eleanor Tyler, *Analysis: As Reviews Stretch, M&A Deals Keep Shorter Deadlines*, Bloomberg L. (Oct. 21, 2021), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-as-reviews-stretch-m-a-deals-keep-shorter-deadlines (studying eighty-one public M&A deals valued at $1 billion or greater and finding that the average time to close was 278 days).

87. *See* Carmiel, *supra* note 85 (noting that businesses lacking tools to guard against cyberattacks are "easier target[s]" for cyber actors to prey upon).

88. Some industries are more vulnerable to cyber incidents than others. Abdul Subhani, *Industries at Risk of Cyberattacks*, Forbes (Feb. 28, 2023), https://www.forbes.com/sites/forbestechcouncil/2023/02/28/industries-at-risk-of-cyberattacks/?sh=69b9b89b49e1. For example, in 2021, the average cost of a data breach in the healthcare industry was $9.23 million, while the average cost of a data breach in the public sector was $1.93 million. IBM, *supra* note 86, at 15 fig.4.

89. *See* IBM, *supra* note 86, at 17 fig.6, 18 fig.7 (finding customer PII to be the most common, and costliest, type of record attacked in cyber incidents).

90. *See* Deloitte, *supra* note 32, at 13.

company so suddenly deteriorated by a cyberattack that the "fundamentals of the deal" are undermined.[91] Still, some carve-out provisions include cyberattacks among the events to be assumed by the buyer.[92] And as the prevalence of cyberattacks continues to mount, buyers will face even more pressure to bear the risk of cyber incidents through narrow MAE clauses.[93]

A narrow MAE clause together with buyers' historic failure to meet the materiality threshold, undermine a buyer's expectations and afford little comfort in the event of a cyberattack on the seller. And a minimum level of comfort is necessary to do business—particularly M&A business, where millions or billions of dollars are at stake. As the frequency of cyber incidents increases, so too will buyers' hesitancy to sign acquisition agreements absent sufficient safeguards. This reluctance could dampen M&A activity or result in lower purchase prices that reflect the cyber-related risks buyers assume at signing and until closing.

The traditional MAE approach leaves courts ill-equipped to evaluate the novel issue of whether a cyberattack on a seller meets the General MAE Condition. Meanwhile, the ubiquity of cyberattacks threatens M&A activity, particularly when buyers lack leverage to negotiate broad MAE clauses. Thus, to better appreciate the potential risks and harms that cyberattacks pose to M&A deals, the traditional MAE approach should be tailored and the parties to such transactions should abandon narrow MAE clauses.

V. PROPOSED SOLUTION: CYBERATTACK-SPECIFIC GUIDANCE FOR COURTS AND PROTECTIONS FOR M&A DEAL CONSTITUENTS

A. The Traditional MAE Approach Tailored to Cyber Incidents

Whether a cyberattack constitutes an MAE should be determined on a per-case basis, by applying an adjusted version of the traditional MAE approach. This Note proposes a set of factors, informed by the nuances of cyberattacks, that a court should consider when assessing whether a cyberattack has caused a material adverse change in a seller's business.

---

91. *See* Akorn, Inc. v. Fresenius Kabi AG, No. 2018-0300, 2018 WL 4719347, at *47 (Del. Ch. Oct. 1), *aff'd*, 198 A.3d 724 (Del. 2018).

92. *See, e.g.*, Twitter, Inc., Current Report Exhibit 2.1 at 5 (Form 8-K) (Apr. 26, 2022) (acquisition agreement executed by Elon Musk and Twitter, which carved out cyberattacks from the MAE definition).

93. A creative sell-side litigator could argue that, absent explicit mention, a cyberattack is covered by the "war exclusion clause," that is, the customary carve-out for warlike situations. *See, e.g.*, *Akorn, Inc.*, 2018 WL 4719347, at *51 (carving out from the MAE definition "acts of war (whether or not declared), military activity, sabotage, civil disobedience or terrorism, or any escalation or worsening of any such acts"). But this novel argument was recently rejected in the context of insurance policy agreements, which are structurally similar to MAE clauses. Merck & Co. v. Ace Am. Ins. Co., No. UNN-L-002682-18, 2022 WL 951154, at *6 (N.J. Super. Ct. Law Div. Jan. 13, 2022) ("[B]oth parties to this contract [we]re aware that cyber attacks of various forms . . . have become more common. Despite this, [the] [i]nsurers did nothing to change the language of the exemption to reasonably put th[e] insured on notice that it intended to exclude cyber attacks.").

When analyzing whether a cyberattack on a seller has given rise to adverse effects of substantial magnitude, a court should recognize that the costs of a cyberattack take many forms. Some of these costs are tangible and easily translated into dollar amounts; others are intangible and difficult to quantify.[94] Both tangible and intangible costs are imperative to the analysis and should be weighed considering the following factors.

Regarding tangible costs, unique to a cyberattack are the expenses flowing from forensic investigations to identify the cause and source of an incident, and remedial measures to contain and remove the malware from a seller's computer systems.[95] A seller afflicted by a cyberattack also incurs the costs of notifying customers and affected third parties, particularly if PII is breached.[96] These costs include breach-related litigation expenses like legal fees, court costs, expert witness fees, settlement payments, and fines imposed by government agencies.[97] Further, as it purchases or renews cyber insurance after a cyberattack, a seller faces increased premiums.[98] A seller is also saddled with costs arising from the disruption of its normal business operations as a result of any system downtime caused by a cyberattack.[99]

Apart from these cyberattack-specific costs, the traditional metrics courts have used to assess the tangible impacts of non-cyber events remain important to the analysis. These considerations include loss of revenue, decline in stock price and market value,[100] loss of future opportunity associated with contracts terminated,[101] and increased costs to raise debt.[102]

---

94. Mossburg et al., *supra* note 84, at 2.

95. *See* Sasha Romanosky, *Examining the Costs and Causes of Cyber Incident*s, 2 J. Cybersecurity 121, 129 (2016).

96. *See id.*

97. *See* Solove & Schwartz, *supra* note 9, at 1013 (noting that Equifax reached a settlement of at least $575 million with the Federal Trade Commission, the Consumer Finance Protection Board, and all fifty states after enduring a cyber incident).

98. Deloitte, *supra* note 27, at 2 (finding that it is common for a cyber insurance policyholder to face a premium increase of 200 percent after suffering a cyberattack).

99. *Id.*

100. Brian Cashell et al., Cong. Rsch. Serv., RL32331, The Economic Impact of Cyber-Attacks 4–6 (2004); *see also* Matthew Heller, *Cyber Attacks Can Cause Major Stock Drops*, CFO (Apr. 12, 2017), https://www.cfo.com/technology/2017/04/cyber-attacks-stock-drops/ ("[B]reaches have wiped as much as 15% off companies' stock market valuations.").

101. Deloitte, *supra* note 27, at 2; *see, e.g.*, Akorn, Inc. v. Fresenius Kabi AG, No. 2018-0300, 2018 WL 4719347, at *55 (Del. Ch. Oct. 1) (holding that the seller endured an MAE and noting that the seller "unexpectedly lost a key contract to sell [a product], resulting in a loss of revenue where [it] had been forecasting growth"), *aff'd*, 198 A.3d 724 (Del. 2018).

102. Deloitte, *supra* note 27, at 2 (explaining that increased costs to raise debt are expected because a targeted company is perceived as a higher-risk borrower and is consequently charged higher interest rates to borrow capital).

The intangible costs of a cyberattack are often concealed from the public because they are not readily quantifiable, yet they can prove devastating.[103] In particular, a seller's loss of exclusive control over its intellectual property upon a data breach weakens its competitive advantage.[104] Furthermore, productivity suffers as a seller shifts focus from ordinary business operations to mitigating the effects of a cyberattack.[105] In addition, a seller's relationships with valued customers and business partners could sour following a cyberattack,[106] while increased customer support efforts could prove costly.[107] Most importantly, though, a cyberattack tarnishes a seller's brand and public perception.[108] The negative press coverage and distrust of a seller's data protection practices stemming from a breach render customers and business partners less inclined to provide a seller with the PII crucial to everyday transactions.[109]

Moreover, when evaluating the durational materiality of a cyber incident, an astute understanding of both the short- and long-term effects of such an incident is essential. The following considerations specific to cyberattacks should be incorporated into the traditional durational significance inquiry.

Short-term effects are those flowing directly and immediately from a cyberattack, and primarily concern damaged or destroyed data.[110] When evaluating the short-term impacts of a cyberattack, a court should consider the length and breadth of a seller's near-term response, which may include conducting forensic investigations to assess the damage and identify the cyber actor; detecting and deleting malware; restoring corrupted systems; notifying affected customers and third parties; and recovering stolen digital assets, like intellectual property and PII.[111] Also probative of short-term effects is the extent of a cyberattack's immediate disruption to a seller's business operations, including the diminished productivity that results when a company shifts focus toward minimizing the effects of a cyberattack.[112]

---

103. *See* Mossburg et al., *supra* note 84, at 2–3.

104. Deloitte, *supra* note 27, at 3 (noting that loss of control over intellectual property like trade secrets, copyrights, and investments strategies is particularly damaging to companies that rely on such assets for their competitive advantage).

105. Morgan, *supra* note 12; *see also* Romanosky, *supra* note 95, at 129 (stating that the intangible costs of a cyber incident include those resulting from lost time when executives are fired in the aftermath of such an incident).

106. Deloitte, *supra* note 27, at 2.

107. Romanosky, *supra* note 95, at 129.

108. Deloitte, *supra* note 27, at 2 (listing the "[d]evaluation of [a targeted company's] trade name" as one of the "seven hidden costs" of a cyberattack).

109. *See* Agrafiotis et al., *supra* note 81, at 12.

110. *See* Lloyd's, Closing the Gap: Insuring Your Business Against Evolving Cyber Threats 22 (2017).

111. *See id.* at 22–24.

112. *See* Cashell et al., *supra* note 100, at 15.

Long-term effects, on the other hand, continue to impact a seller long after its immediate reactionary efforts have expelled a cyber threat from its system.[113] A court should analyze the length and breadth of the impacts on a seller's business stemming from a cyberattack in the long term, such as legal expenses; regulatory fines and penalties; costs of reimbursing victims; and continued loss of revenue, reputation, competitive advantage, and management focus.[114]

Particularly onerous here are the long-term consequences flowing from legal costs and reputational damage.[115] A seller impacted by a cyber incident will continue to accrue significant expenses to litigate or settle lawsuits for years following such an incident, both because regulatory investigations into a data breach can take more than a year to complete and because data privacy law is still evolving.[116] Additionally, for years after a cyberattack occurs, a seller will suffer a depressed stock price, struggle to regain lost business and restore public confidence in its data protection practices, be subjected to higher interest rates to raise capital and increased premiums for cyber insurance, and continue to lose both revenue and future opportunities.[117]

Ultimately, a seller's immediate response to a cyber threat is costly but accounts for only a small fragment of the total cyber incident-related costs it will expend over a five-year period.[118] The effects of a cyber incident "reverberate over a multiyear timeline," and the short-term recovery efforts are quickly overshadowed by the process of fighting breach-related lawsuits and repairing damaged relationships with customers, suppliers, and the public.[119] Thus, unless a court considers the temporal effects of a cyber incident in a holistic rather than short-sighted manner, a significant portion of the detrimental effects will go unaccounted for, rendering the durational significance analysis deficient.

The approach proposed in this Note provides guidance to a court determining, in the first instance, whether a cyberattack has given rise to an MAE on a seller's

113. *See* Lloyd's, *supra* note 110, at 5.

114. *See id.* at 22–24; Mossburg et al., *supra* note 84, at 2.

115. *See* Deborah Pretty, Pentland Analytics & AON, Reputation Risk in the Cyber Age 5 (2018).

116. *See* Ins. J., *supra* note 84.

The cyberattack experienced by major retailer Target in 2013 illustrates how a targeted company incurs costs in the aftermath of a cyberattack. *See* Lloyd's, *supra* note 110, at 23. At first, the brand paid $60 million in short-term costs toward incident response, investigations to identify the cyber threat, efforts to secure internal systems, increased staffing to field customer complaints, and customer support services. *Id.* Target subsequently paid more than $219 million in long-term expenses, including $100 million to upgrade payment terminals at stores and $5 million toward customer education and awareness. *Id.* Over forty million credit card details and seventy million pieces of PII were stolen from Target. *Id.* And nearly $100 million of its long-term costs were legal expenses and settlement fees stemming from the 140 legal actions brought against the company. *Id.* The last settlement was not reached until 2017, over four years after the cyber incident had occurred. *Id.*

117. *See* Deloitte, *supra* note 27, at 2–3.

118. *See, e.g.*, Mossburg et al., *supra* note 84, at 7, 11; *see also* Ins. J., *supra* note 84 (describing the immediate business impact of a cyberattack on a corporation as just the "tip of the iceberg").

119. Mossburg et al., *supra* note 84, at 14.

business. Because every cyberattack is different, whether any one constitutes such an MAE will hinge on the specific circumstances involved. This Note equips a court with an understanding of the nuances of cyberattacks and a suggested framework for how those characteristics should factor into the traditional MAE approach. This proposed solution, however, is relevant only if parties agree not to exclude cyberattacks from their MAE definitions.

B. Protecting the Buyer to Benefit the Seller

The threat that a cyberattack will decimate a seller's business during the executory period increases buyer risk, thereby chilling M&A activity. To factor this reality into dealmaking, buyers and sellers should embrace broad MAE definitions that allocate the risk of cyber incidents to sellers. Excluding cyber incidents from the list of carve-outs in the MAE clause, and thus conditioning the buyer's obligation to close on the seller not experiencing a cyber incident, mitigates the buyer's risk between signing and closing. At first blush, this practice seems contrary to the seller's interest. But a closer look, revealing how broad MAE definitions can enhance M&A transactions, suggests otherwise.

Notably, broad MAE definitions facilitate more M&A activity. Today, the prevalence of cyberattacks and the seller-friendly MAE approach followed by the Delaware courts[120] leave buyers with few protections when they invest in M&A transactions. But if sellers would appeal to buyers with broad MAE clauses minimizing buyer exposure to cyber-related risks, buyers would be more willing to sign acquisition agreements. Furthermore, by decreasing buyer risk, broad MAE definitions render sellers more attractive to buyers, who will consequently pay higher purchase prices.[121]

Additionally, incidental benefits accrue when sellers bearing the risk of cyber incidents are incentivized to invest in comprehensive cybersecurity, a measure that decreases the likelihood of cyberattacks. A decrease in cyber incidents between signing and closing makes it more likely that buyers will close and less likely that sellers will be forced to accept less lucrative consideration from buyers with the leverage to renegotiate purchase prices downward. Lastly, by encouraging sellers to maintain effective cybersecurity practices, broad MAE definitions enable the public to place greater trust in those companies.

---

120. This approach continues in the post-*Akorn* era. For example, in *Channel Medsystems, Inc. v. Boston Scientific Corporation*, the first MAE clause-related decision rendered by the Delaware Court of Chancery after *Akorn, Inc.*, the court reverted to its longstanding practice, refusing to release the buyer from its obligation to close under the MAE clause. No. 2018-0673, 2019 WL 6896462 (Del. Ch. Dec. 18, 2019).

121. *See* Oesterle & Haas, *supra* note 19, at 17 ("The risk is reflected in the price the buyer is willing to offer, as the buyer will discount the price to account for the risk.").

VI. CONCLUSION

Digitalization exposes companies to exploitation by sophisticated hackers who wreak havoc on corporate digital assets and business operations. Despite the pervasiveness of cyberattacks, some acquisition agreements still fail to allocate the risk of a cyber incident during the executory period to the seller.

Courts must prepare to evaluate whether a cyberattack constitutes an MAE: an issue of first impression for which the traditional MAE approach is inadequate. This Note offers initial guidance. By injecting the nuances of cyberattacks into the traditional MAE approach, this Note proposes a framework that acknowledges the costs and effects historically contemplated by the Delaware courts while appreciating the unique harms that flow from cyberattacks. Meanwhile, to facilitate M&A transactions in the digital age, this Note contends that deal constituents should negotiate broad carve-out provisions allocating the risk of cyberattacks to sellers—a measure that protects all parties against the threats posed by cyberattacks between signing and closing.

As technology continues to develop, hackers' tactics will grow more insidious. Cyberattacks, consequently, will become easier and cheaper to execute, harder to avoid, and costlier to clean up. The dangers that cyberattacks pose to M&A transactions are both potent and sweeping. Confronting this shifting battleground requires that attention be paid to the issues and potential solutions raised in this Note.