THE M&A JOURNAL

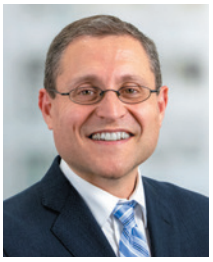
THE INDEPENDENT REPORT ON DEALS AND DEALMAKERS

VOLUME 22 NUMBER 9

Evaluating and Containing Cyber and Data Privacy Risks in Corporate Transactions

Sid Mody
O'Melveny & Myers

Kayla Haran
O'Melveny & Myers



Brian Levine
Ernst & Young

Archana Chintalacharuvu
Ernst & Young

By Sid Mody, Data Security and Privacy partner, O'Melveny & Myers LLP; Kayla Haran, Data Security and Privacy associate, O'Melveny & Myers LLP; Brian Levine, Managing Director, Cybersecurity and Data Privacy, Strategy and Transactions, Ernst & Young LLP; Archana Chintalacharuvu, Director, Transactions Cyber Group, Ernst & Young LLP

Let's wait and see what happens –

Cybercriminals have started playing the long game when targeting certain victims. They breach the little guy and then wait until it is acquired by a bigger fish before showing themselves in the system. As cybercriminals become more organized and sophisticated, so do their strategies. They now have the resources as well as the patience to wait it out in hopes of snagging a bigger slice of the pie. These malicious actors are increasingly targeting companies with cyberattacks and data breaches around the time of high-profile transactions, creating liabilities and risks on both sides of major deals. In this article, we explore the various types of cybersecurity and data privacy risks surrounding transactions and offer strategies and recommendations for mitigating those risks.

I. Cybersecurity & Data Privacy Are Now Top of Mind for Boards

Cybersecurity incidents have become commonplace, and company boards across nearly all industries and sectors are rightly concerned about protecting and mitigating against the risk of data breaches and other cyber incidents. Some recent high-profile incidents have had sprawling effects impacting corporate entities and individuals alike, including SolarWinds in February 2020 (affecting more than 18,000 corporate customers), Microsoft Exchange Server in January 2021 (affecting more than 30,000 U.S. organizations), and LastPass in August 2022 (affecting 30 million users). Other vulnerabilities have threatened millions of corporate entities, such as the vulnerability reported in the popular Java logging package Log4j in January 2022, which affected vendors like Adobe, IBM, Cisco, IWS, and VMWare.

Along with a greater frequency of cyber incidents has come an increased regulatory focus on data privacy and cybersecurity, as well as a sharp increase in proposed and enacted state legislation governing data privacy and biometric privacy. State attorneys general have increasingly brought enforcement actions against companies in the wake of data breaches under state consumer protection laws, state data privacy laws, and state data breach notification laws, and they have secured multi-state assurances of voluntary compliance at high costs to companies: Home Depot entered into a $17.5 million settlement with the attorneys general of 46 states and D.C., as did Anthem, with 42 states and D.C. to the tune of $39.5 million, and Uber with all 50 states and D.C. for $148 million.

In the face of numerous failed efforts in recent years to enact robust federal data-privacy legislation, states have acted on their own: Five states (California, Colorado, Connecticut, Virginia, and Utah) now have broad data privacy statutes, with 18 more introduced and pending so far in 2023. Following in the footsteps of Illinois's 2008

Cybercriminal ➔

Cybercriminal

continued

Biometric Information Privacy Act, Washington and Texas recently enacted similar statutes, and nine other states have introduced similar legislation so far in 2023.

Predictably, cyber insurance prices have soared. Cyber insurance premiums have increased by nearly 400% over the last several years. These hikes have been steep and rapid—for example, premiums increased by 28% on average in the first quarter of 2022 compared with the fourth quarter of 2021. In addition to these increases, underwriters are attempting to mitigate cybersecurity incident-related losses by imposing far stricter underwriting requirements. Altogether, the shifting landscape of cybersecurity and data privacy poses risks to companies from all fronts.

II. Cyber Risks Surround Transactions

Cyber risk peaks during transactions. Transactions present at least two types of cyber risk: "counterparty risk" and "transaction risk."

A. Counterparty Risk

"Counterparty risk" is the risk that the target company is already compromised or noncompliant with security or privacy regulations or that its security program is so immature that a compromise or regulatory action is highly likely. For example, when one large internet service provider (ISP) acquired another in 2017, the acquirer learned that its target had experienced a significant breach prior to close. As a result, the acquirer was able to reduce the acquisition price by $350 million and required the target to create a surviving entity that would be sufficiently capitalized to cover 50% of any exposure resulting from the breach. The Delaware Chancery Court recently indicated that the total exposure from the target's breach could exceed $3 billion.

In contrast, when one large hospitality company acquired another in 2016, it apparently did not uncover that its target had been breached prior to close, so it did not build appropriate protections into the deal. The breach may have cost the acquirer hundreds of millions in exposure, and the ensuing multiple class action lawsuits have yet to be resolved.

These are two high-profile examples of what cyber transaction professionals see regularly: transactions that create significant counterparty risk, which can significantly erode deal value and create an unwanted narrative that overshadows what was supposed to be a time of celebration.

B. Transaction Risk

"Transaction risk" refers to the fact that the transaction itself increases the risk to both parties. Transactions can be highly visible events that draw the attention of cybercriminals. Indeed, in November 2021, the FBI warned that cybercriminals were increasingly targeting companies involved in mergers and acquisitions and leveraging these high-profile events for ransomware attacks. Four months later, a *Wall Street Journal* headline noted: "Ransomware Attackers Begin to Eye Midmarket Acquisition Targets." Indeed, one acquisitive private equity client recently confided that one target was hit with ransomware on the day of announcement, and another was attacked within a month of the acquisition.

Transactions are a target for cybercriminals not only because they are large, high-profile events but also because they are distracting, and distracted employees are more likely to fall for a phishing email or other social engineering attack. A merger or acquisition often involves new and unfamiliar voices and communication channels, so employees may not be on guard when they receive an email or phone call from someone they don't recognize. Distracted by concerns about whether the transaction will impact their jobs, employees may be less cautious—or may become insider threats themselves, attempting to download anything that is not secured, such as trade secrets or other proprietary information.

III. Mitigating the Risk

A. Proper Cyber Diligence

In general, a key goal for cybersecurity and data privacy in transactions is to "shift risk to the left"—identify and mitigate risks as early in the transaction lifecycle as possible. Like financial, accounting, and tax, cyber due diligence should be a standard part of every transaction. Internal and outside cyber teams should be engaged as early as possible, ideally at the letter of intent (LOI) stage, to most effectively identify, assess, and plan for cybersecurity risks. The buyer's and seller's chief information security officers should be pulled into the transaction early to give the parties sufficient time to identify and mitigate risks prior to announcement and close.

The earlier cyber diligence is conducted, the more options the buyer will have to respond to findings (e.g., price reductions, holdbacks, targeted conditions to close, specific representations

and warranties, technical testing, etc.).

While cyber diligence may historically have been a "check box" exercise that involved a buyer's internal team submitting a questionnaire and/or addressing the topic in 30 minutes of a broader diligence call, the requirements of a "standard" cyber diligence have changed significantly. Today, a standard cyber diligence should generally include both "inside out" and "outside in" diligence. "Inside out" diligence involves a thorough review of the target's documents and typically at least a two-hour interview with the target's cybersecurity and data privacy lead. "Outside in" diligence involves using open-source intelligence and technical tools to identify vulnerabilities, detect hidden risks, and challenge the information received during "inside out" cyber diligence. The buyer's team should also understand the maturity of the target's compliance program and the degree to which it is compliant with an ever-expanding array of cybersecurity and data privacy regulations.

It has also become common to conduct technical testing during the diligence phase or immediately after. Early technical testing may be particularly appropriate for acquisitions in highly regulated entities and acquisitions of entities with relatively immature security programs or those that have experienced recent security incidents. Technical testing might include a compromise assessment (to identify active compromises and critical vulnerabilities), code scans (to identify vulnerabilities and licensing issues with proprietary software), cloud or operational technology security scans, Office 365 configuration reviews, and even penetration testing.

While organizations can be found to have been negligent with respect to breaches outside of the transaction context, courts and regulators may have greater expectations for acquirers given the general expectation that they engage in appropriate due diligence as part of the acquisition. *See, e.g., In re Sols. Liquidation LLC*, 608 B.R. 384, 399 (Bankr. D. Del. 2019) ("a complaint pleading facts including, for example, that a 'board undertook a major acquisition without conducting due diligence, without retaining experienced advisors, and after holding a single meeting ...' would be sufficient to plead a claim for gross negligence") (internal citations omitted). For example, in *Springmeyer v. Marriot*, the court dismissed a class action complaint based on a breach that did not arise out of a transaction, finding plaintiff's allegations of negligence to be conclusory. *See* 2021 WL 809894, at *4 (D. Md. Mar. 3, 2021). In contrast, the same court had recently allowed a similar class action against the same defendant arising out of the acquisition of a breached company to proceed, in part, because of the expectations that "a reasonable due diligence would have uncovered the breach." *Id.* (citing *In re Marriott Int'l, Inc., Customer Data Security Breach Litig.*, 440 F. Supp. 3d 447, 454 (D. Md. 2020)). Similarly, in *In re Ambry Genetics Data Breach Litigation*, the court permitted a class action to proceed against a successor to the acquirer "on the theory that it failed to take appropriate and necessary measures in response to due diligence after it was founded." *See* 567 F. Supp. 3d 1130 (C.D. Cal. 2021). Shareholders have even brought derivative lawsuits against directors of companies that acquired breached companies, alleging that the board breached its fiduciary duties by failing to "undertake cybersecurity and technology due diligence." *See e.g., Firemen's Retirement System of St. Louis v. Sorenson*, 46 Del. J. Corp. L. 107, 115-16 (2021).

B. Preparing for Attacks Upon Announcement

Given the increased risk of attacks upon announcement, it is important to take steps to increase the target's resiliency as soon as practical. Many of these steps, such as creating and testing immutable backups to improve the target's ability to recover from a ransomware attack, are inexpensive and can be done in days, if not hours.

But it is not always enough to simply harden the target's shell. Some acquirers and cybersecurity experts have hypothesized that cybercriminals were attacking targets after hearing news reports about acquisitions. While that is sometimes the case, cybercriminals are highly specialized. Some make their living compromising entities and then selling access to those compromised entities on the dark web, in criminal forums, or directly to their criminal associates. New threat intelligence suggests that in some "transaction attacks," the target has been compromised long before the announcement, but the announcement triggers a different cybercriminal to purchase access to the compromised target to launch a cyberattack at a particularly vulnerable time for the target.

Given this new threat intelligence, it is important to attempt to identify and remediate any compromise before (or as soon as possible after) announcement. One of the most effective ways to do this is by conducting a "compromise assessment" in which software is installed on all of the target's desktops, laptops, and servers. The software gives expert threat-hunters access to iden-

Cybercriminal ➔

Cybercriminal

continued

tify and respond to a compromise, critical vulnerability, or other security gap. While this type of assessment does require at least "read-only" access to the target's systems, targets and acquirers share a strong interest in wanting to be free of ransomware upon announcement. Sellers who are educated about cyberthreats will often happily cooperate with such threat hunts, and if both parties agree, there is generally no legal obstacle to a third-party expert threat hunting on the target's systems prior to sign or close. *See, e.g.*, 6 U.S.C. § 1505; Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information (Apr. 10, 2014), available at https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

Conclusion

While there is no shortage of cybersecurity and data privacy risks surrounding transactions, with thorough diligence, technical testing, and appropriate preparation for increased attacks, these risks are navigable. Don't go it alone—engage your legal and technical advisors as early as possible in the transaction.

~~MA~~

THE M&A JOURNAL
the independent report on deals and dealmakers

Editor/Publisher	**John Close**
Design and Production	**John Boudreau**
Senior Writers	**Gay Jervey, R. L. Weiner**
Writing/Research	**Frank Coffee**, **Jeff Gurner**, **Terry Lefton**
Circulation	**Dan Matisa**
Web Production	**John Boudreau**

The M&A Journal, 1008 Spruce Street, Suite 2R, Philadelphia, PA 19107