Westlaw Today

Cyber liabilities are a key aspect of insurance due diligence in any corporate transaction

By Cort T. Malone, Esq., Anderson Kill, Boris Strogach, Esq., World Insurance Associates, and Seán McCabe, Esq., Anderson Kill

NOVEMBER 7, 2025

Insurance due diligence is a critical component of any M&A transaction. As a corporate asset on the balance sheet, insurance warrants as much attention and review as any other company asset in connection with a merger, acquisition, or investment. If the limits of liability, terms and conditions, quality, or types of insurance are inadequate, the asset may be impaired, and risks assumed by the buyer are increased or un/underinsured.

Insurance due diligence involves reviewing and assessing the target company's insurance programs, risk exposures, and potential liabilities, including identifying insurance risks that could derail a deal. This makes it a vital aspect of any corporate transaction. The detailed analysis and recommendations provided through the insurance due diligence process deliver valuable input into the financial modeling process of a transaction.

As a corporate asset on the balance sheet, insurance warrants as much attention and review as any other company asset in connection with a merger, acquisition, or investment.

Failure to maintain insurance for a particular exposure or under-accounting for losses within a large deductible can lead to substantive adjustments to a company's total cost of risk and, ultimately, the purchase price of the transaction.

This is particularly true in the private equity realm where mergers and acquisitions have seen a significant rebound since 2024. Coinciding with this uptick is the increase in cyberattacks on PE firms and their portfolio companies. This is due, in part, to the perception that PE firms have deep pockets.

Since 2021, the FBI has been ringing the bell on the potential for bad actors to target and leverage victim companies for ransomware infections. In particular, bad actors threaten to release non-publicly available information that can negatively impact a company's stock value, mergers and acquisitions, and other announcements.

The secondary effects of a cyberattack can be equally devastating, including fines, legal liabilities, reduction in the target company's value, and reputational loss. Such negative results are contrary to the primary focus of a PE firm — to generate significant returns on investments and sell the acquired company at a high profit.

Due diligence is the best place for PE firms to discover cyber vulnerabilities in the target companies and test their technical capabilities. A key area of discovery will be how well a target company can manage its cyber risks. This is especially true because the PE firm remains exposed throughout the hold period.

Due to the vast amount of sensitive data acquired by PE firms, a key risk to look out for in due diligence is whether the target company has previously suffered a data breach. Data breaches continue to increase annually with nearly 5,000 data breach incidents reported in 2024 and an estimated 1.7 billion breach notices sent to exposed stakeholders, according to Kiteworks (https://bit.ly/4nHWQyR).

Due diligence is the best place for PE firms to discover cyber vulnerabilities in the target companies and test their technical capabilities.

Not only are these incidents increasing in frequency but so too are the costs of responding to data breaches. The cost of responding to a data breach largely depends on the industry. The average cost of a data breach in the healthcare industry, the industry with the highest cost per breach, is almost $11 million, according to IBM (https://bit.ly/43VN9Wi).

In the financial sector, the estimated cost is upwards of $6 million per breach. These costs include operational

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

Thomson Reuters™

downtime, lost customers, post-breach responses, increased staffing, and regulatory notifications, fines, and penalties.

If a breach is disclosed during due diligence, it can have a major impact on the purchase price of the target company and the operational costs going forward.

For instance, in 2016, during the merger between Yahoo and Verizon, Yahoo disclosed to Verizon a data breach that it suffered in 2014. As a result of this breach, Yahoo agreed to lower the purchase price by $350 million (https://nyti.ms/47rtUGy) and agreed to share liabilities and expenses relating to the breach going forward. Ultimately, the purpose of due diligence is to correctly value the target company, and if there is a known risk that affects the value of the company, it must be considered.

If a breach is disclosed during due diligence, it can have a major impact on the purchase price of the target company and the operational costs going forward.

One way a PE firm can account for risks is through the target company's insurance policies. During due diligence, a PE firm must review whether the target company has a stand-alone cyber insurance policy and Commercial General Liability ("CGL") policy, among others, which, taken together, can respond adequately to cyber incidents.

A major concern for policyholders is the potential for gaps in coverage between the CGL policy and cyber policy. For instance, cyber policies typically exclude coverage for bodily injury and property damage whereas CGL policies provide this coverage.

On the other hand, since the inception of the stand-alone cyber policy, insurance companies have sought to remove cyber coverage from their CGL policies through exclusions. The insurance companies argue that cyber policies were created to cover such events, including data breaches.

Two recent court decisions illustrate how pursuit of insurance coverage under CGL policies for bodily injury claims stemming from cyberattacks may play out. In each case, the decision hinged primarily on the presence or absence of an electronic data exclusion in the CGL policy.

In *Home Depot, Inc. v. Steadfast Insurance Company*,[1] ("*Home Depot*"), after suffering a data breach, Home Depot sued its insurance company for defense costs and indemnification under its CGL policy. The court held that Steadfast Insurance Company and Great American Assurance Company owed no duty to defend or indemnify Home Depot.

For indemnification, the CGL policy included an "electronic data" exclusion that purported to exclude coverage for "[d]amages arising out of the loss, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[2] The court reasoned that the data breach did trigger that exclusion: "When hackers broke into Home Depot's system, they gained access to payment card data. The hacker's access made that data useless … . When that critical function is affected, the data doesn't work the same as before; it loses its function."

In contrast, in *Landry's, Incorporated v. Insurance Company of the State of Pennsylvania*,[3] ("*Landry's*"), the Fifth Circuit required the insurance company to defend Landry's in the underlying suit. In that case, Landry's suffered a data breach that affected millions of customers' credit cards.

Paymentech, LLC — a branch of JPMorgan Chase Bank that processes Visa and Master Card payments — sued Landry's for over $20 million in data-breach-related losses. The applicable CGL policy did *not* include an "electronic data" exclusion. Therefore, the question before the court was whether the underlying lawsuit sought damages "arising out of … the oral or written publication … of material that violates a person's right of privacy."[4]

A major concern for policyholders is the potential for gaps in coverage between the CGL policy and cyber policy.

The court resolved this question in Landry's favor. First, the court found that the "Paymentech complaint plainly alleges that Landry's published its customers' credit-card information — that is, exposed it to view."

Next, the court found that "it's … undisputed that hackers' theft of credit-card data and use of that data to make fraudulent purchases constitute 'violations' of consumers' privacy rights." Thus, the court found that the CGL insurance company owed Landry's a duty to defend in the underlying suit.

The uncertainty demonstrated by these two decisions underscores the advantage of stand-alone cyber coverage. In today's commercial landscape, stand-alone cyber policies are commonly used to backstop a policyholder's exposure — and cyber insurance companies have made frequent claims payouts over the past five years.

There are relatively few coverage cases interpreting standalone cyber policies. One recent exception, *Kane v. Syndicate 2623-623 Lloyds of London*,[5] ("*Kane*"), hinged on another potential coverage gap: for losses incurred when fraudsters induce company employees to wire money to themselves or allied cyber thieves.

Kane began when a third party posing as a senior account manager of one of NMHC's vendors, OptumRX, emailed a

©2025 Thomson Reuters

fraudulent invoice and requested payment at a fraudulent bank account. In response, NMHC wired over $4.4 million to the fraudulent bank account. OptumRX's legitimate invoice went unpaid and they demanded payment.

NMHC sought indemnification for the claims asserted by OptumRX. Beazley denied coverage, in part, because, as they alleged, Beazley's policy applied only to claims against the policyholder "for" the security breach itself — and not to an unpaid debt arising out of the breach.

While the court construed ambiguity in favor of the policyholder, ambiguity is not a basis on which to purchase coverage — or assess the coverage of a target company.

The New Mexico Court of Appeals determined that the phrase "for a Security Breach" in a standalone cyber insurance policy was ambiguous and therefore must be construed in favor of coverage. The Court of Appeals held that "a reasonable [policyholder] would construe ambiguous coverage terms at issue to afford coverage and would not read the exclusions to apply" and thus affirmed the District Court ruling that the policy covered OptumRX's claim against NMHC.

In reaching this conclusion, the Court first noted that the policy did not define the word "for."[6] Next, the Court noted that the word "for" has multiple commonplace definitions, which "tend[s] to demonstrate the ambiguity of a term."[7] The Court concluded that "there is a lack of an interpretive consensus among courts, and take this as an indicator of ambiguity."[8]

Finally, the Court noted that: "[p]urchasers of a cyber insurance policy often have little knowledge about the breadth and sophistication of the cybersecurity risk they face. The insurers are far more knowledgeable. This imbalance is exacerbated by the lack of standard policy language among insurers to define or limit coverage. … it is another indication that the phrase 'for a security breach' would not have a single, obvious meaning to an insured."[9]

While the court construed ambiguity in favor of the policyholder, ambiguity is not a basis on which to purchase coverage — or assess the coverage of a target company. As cyber frauds inducing payments to the fraudsters grow ever more sophisticated (sometimes now faking the actual video presence of a company executive), private equity firms should assess whether a target company has purchased adequate coverage for such fraud.

In this case, the policyholder had funds transfer fraud coverage with a sublimit of $250,000. That claim was paid, but the coverage was inadequate to the purpose. While the litigation seeking coverage on other grounds was successful, M&A due diligence requires seeking adequate coverage for fraud on a less "ambiguous" basis.

Insurance companies advertise their cyber insurance policies as covering, among other scenarios, social engineering (that is, fraud that induces employees to transfer money, securities or other property), as well as cyber extortion and ransomware, privacy and security liability, data breach response and crises management, data recovery, and dependent business interruption.

In addition, insurance companies purport to provide or offer, for an additional price, risk mitigation resources such as incident response planning, privacy awareness training, social engineering and phishing campaigns, and cyber security compliance assistance.

As *Kane* indicates, whether a given purported coverage is likely to respond to an actual claim — e.g., for "social engineering" — requires an expert eye. Private equity executives need to access expert assessment of target companies' coverages.

Those performing insurance due diligence also must be aware of how cyber insurance policies operate. Typically, cyber policies are claims-made policies, which, in general terms, means that the policy is triggered by a claim made during the policy period and, depending on the policy, noticed during the policy period.

As cyber frauds inducing payments to the fraudsters grow ever more sophisticated, private equity firms should assess whether a target company has purchased adequate coverage for such fraud.

Policyholders can often purchase "tail" coverage that can extend the reporting period during which a policyholder can give notice of a claim made after the end of the policy period where the claim alleges a wrongful act that occurred during the policy period.

CGL policies, on the other hand, are "occurrence" based policies that cover incidents that occur during the policy's active period, regardless of when the claim is filed. Policyholders must be keenly aware of the reporting requirements of their cyber policies and should consider purchasing tail coverage when possible.

If an acquired company lacks sufficient insurance coverage, including for past and future cyber claims, the acquiring PE firm may be on the hook for the costs and expenses resulting from the breach, which will erode potential profits and hurt forecasted projections. Accordingly, proper insurance due

©2025 Thomson Reuters

diligence — including cyber insurance coverage — is a key analytical component of any corporate transaction.

Notes:

[1] 125 F.4th 769 (6th Cir. 2025).

[2] *See Home Depot*, 125 F.4th at 776.

[3] 4 F.4th 366 (5th Cir. 2021).

[4] *See Landry's*, 4 F.4th at 369.

[5] No. A-1-CA-41254, 2025 WL 1733046 (N.M. App. 2025).

[6] *See Kane*, 2025 WL 1733046, at *5.

[7] *See Kane*, 2025 WL 1733046, at *6.

[8] *See Kane*, 2025 WL 1733046, at *7.

[9] *See Kane*, 2025 WL 1733046, at *7.

About the authors



Cort T. Malone (L) is a shareholder in **Anderson Kill**'s New York and Stamford offices and co-chair of the firm's biometric liability insurance recovery group. He can be reached at cmalone@andersonkill.com. **Boris Strogach** (C) is a senior vice president and practice leader at **World Insurance Associates**, specializing in private equity insurance. He advises clients on merger and acquisition due diligence, program integration, and risk transfer strategies across traditional and alternative insurance lines. He can be reached at borisstrogach@worldinsurance.com. **Seán McCabe** (R) is an attorney in Anderson Kill's New York office and a member of the firm's insurance recovery and white-collar defense groups. He counsels individual and corporate policyholders on a wide variety of coverage disputes, cybercrimes and general liability. He can be reached at smccabe@andersonkill.com.

This article was first published on Westlaw Today on November 7, 2025.

© 2025 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional. For subscription information, please visit legalsolutions.thomsonreuters.com.