Expert Insights: Insurance for Cyber Risks in M&A Transactions

A Lexis Practice Advisor® Practice Note by
Jeffrey J. Meagher and Jennifer H. Thiem, K&L Gates


Jeffrey Meagher


Jennifer Thiem

INTRODUCTION

Data breaches, ransomware attacks and other cyber security incidents are quickly becoming the "new normal" for businesses operating in the internet age. As a result, cyber due diligence is quickly becoming the "new normal" for buyers in M&A transactions as they seek to protect themselves against cyber risks. Cyber due diligence, however, is only part of the solution. Many sophisticated buyers are also relying on insurance, including representations and warranties insurance (R&W insurance) and cyber insurance, to protect themselves against cyber risks. This practice note discusses insurance for cyber risks in M&A transactions, including best practices and potential pitfalls for acquiring companies.

R&W Insurance

R&W insurance can provide buyers with some protection against cyber risks arising out of M&A transactions. R&W insurance is, generally speaking, insurance that provides coverage for breaches of representations or warranties in the purchase agreement. It can be purchased by either the buyer or the seller, but buy-side policies are more common because they generally provide broader coverage and allow the seller to exit the deal with greater certainty by limiting or eliminating the need for seller indemnity. R&W insurance is also attractive to buyers because the policy period for an R&W policy is typically more generous than the indemnification period offered by a seller. Most R&W policies offer three years of coverage for "general" representations and six years of coverage for "fundamental" representations. R&W insurance has become more common in recent years as more insurers have entered the market and premiums have dropped (premiums are now often less than 3 percent of coverage limits).

Cyber Exclusions in R&W Policies

Unlike many other types of insurance policies, R&W policies generally do not contain broad cyber exclusions, i.e., policy provisions that broadly exclude coverage for cyber risks. Instead, most R&W insurers evaluate the target company's cyber exposure during the underwriting process and add exclusions based on information learned during that process. While the underwriting process is necessarily tailored to the specifics of an individual transaction, underwriters typically focus on whether the target organization has a history of cyber incidents, as well as on the existence and adequacy of the target's existing cyber insurance program. In evaluating the cyber risks associated with a transaction, underwriters typically rely on the buyer's due diligence. As a result, underwriters may be reluctant to provide broad coverage for cyber risks if the buyer's cyber due diligence is substandard. Underwriters may also propose specific cyber exclusions in response to information learned during the underwriting process. If an R&W insurer proposes a cyber-related exclusion during the underwriting process,

the buyer should first try to eliminate or narrow the exclusion through negotiation. If that proves impossible, the insurer may be willing to provide cyber coverage (as part of the R&W policy) excess of existing cyber insurance (i.e., after the policyholder exhausts existing cyber insurance).

Cyber Coverage in R&W Policies

The trigger for coverage under an R&W policy is the breach of a representation or warranty in the acquisition agreement. The traditional representations and warranties found in most purchase agreements cover some cyber risks. For example, most purchase agreements contain a representation or warranty that the target company has been conducting its business in compliance with all applicable laws. If that turns out not to be true and the target company has violated a law that implicates a cyber risk (e.g., the Digital Privacy Act or the Health Insurance Portability and Accountability Act), then the buyer's R&W insurance policy should provide coverage for losses that arise out of the target company's failure to comply with that particular law.

Cyber Reps and Warranties

A buyer may also insist on cyber-specific representations and warranties. For example, a buyer may insist on a representation or warranty related to the target company's compliance with certain industry standards for cybersecurity. If, for example, the target company stores credit card information, the buyer may ask for a specific representation or warranty that the target has complied with Payment Card Industry Data Security Standards (an information security standard for organizations that collect credit card data). Finally, a buyer may also ask its insurer to treat cyber-specific representations or warranties as "fundamental" representations or warranties in order to extend the coverage period to six years for cyber risks.

CYBER INSURANCE

Stand-alone cyber insurance can provide buyers with additional protection against unknown cyber risks. Cyber insurance, very generally, is insurance that provides coverage for some of the many risks that arise out of the use of computers and other digital devices or networks, such as data breaches and ransomware attacks. Although the specific coverage provided by a cyber insurance policy varies from policy to policy, cyber policies generally provide coverage for both first-party claims (claims seeking coverage for losses sustained by the policyholder) and third-party claims (claims seeking coverage for liability to a third party). Thus, for example, a cyber policy typically provides coverage for certain expenses incurred by the policyholder as a result of a data breach, including costs incurred to investigate and remedy the breach, as well as costs incurred to notify potential victims of the breach. A cyber insurance policy also generally provides coverage for a policyholder's liability to third parties arising out of the data breach. In addition, many cyber policies provide coverage for business interruption losses and cyber extortion payments (among other things).

Cyber Due Diligence and Change in Control Provisions

As part of the due diligence process, an acquiring company will likely want to review any cyber insurance policies maintained by the target company, assess whether those policies are adequate given the target company's cyber exposure, and consider any "change of control" provisions to ensure that it can access the policies post-acquisition. Many cyber policies contain "change in control" provisions that effectively terminate coverage for cyber incidents that occur after an acquisition. These provisions typically state that such coverage as existed before the acquisition will continue in full force and effect for cyber incidents that occurred before the acquisition, but coverage will cease with respect to incidents that occur after the acquisition. Buyers faced with this type of provision will likely want to make sure they have cyber coverage in place that picks up where the target company's cyber policy leaves off to ensure seamless coverage.

Tail Coverage

Acquiring companies should also consider purchasing "tail" coverage. Almost all cyber policies are written on a claims-made basis, *i.e.*, the policyholder must make a claim under the policy during the policy period or within a defined period thereafter. Cyber incidents, however, may go undiscovered for months or even years. If a pre-closing cyber incident is discovered outside the target company's policy period (and any extended reporting period that may apply), there may be a gap in the acquiring company's cyber coverage. Tail coverage can help close this potential coverage gap by extending the reporting period for pre-closing cyber incidents. Alternatively, an acquiring company may be able to purchase cyber coverage with a retroactive date, *i.e.*, the date on which the policy begins providing coverage for cyber incidents, that provides coverage for pre-closing cyber incidents.

Change in Operations Provisions

An acquiring company will also likely want to review its own cyber insurance policies, assess whether those policies are adequate in light of the company's post-acquisition cyber exposure, and consider any "change in operations" provisions to ensure that it can access the policies in connection with a post-acquisition cyber incident at the target company. Many cyber policies contain "change in operations" provisions that require the policyholder to provide the insurer with notice of an acquisition (and potentially an additional premium payment) under certain circumstances. For example, some policies require notice of the acquisition if the target company's revenues represent more than a certain percentage, e.g., 15 percent, of the acquiring company's revenues. Other policies require notice if the target company has sustained cyber-related losses in excess of some threshold, *e.g.*, $1 million, that would be covered under the acquiring company's cyber policy within the past three years. Once the acquiring company provides notice of such an acquisition, its insurer may require additional information about the target company's exposure, additional premium or both. Again, acquiring companies will want to make sure they have cyber coverage in place that picks up where the target company's cyber policy leaves off to ensure seamless coverage.

CONCLUSION

With cyber incidents on the rise, more and more companies are relying on insurance to protect themselves against cyber risks arising out of M&A transactions. R&W insurance and cyber insurance both have important roles to play in these transactions, but only if acquiring companies understand how these policies work and what pitfalls to avoid.

Jeffrey J. Meagher
Partner at K&L Gates LLP

Mr. Meagher is a partner in the Pittsburgh office. He concentrates his practice on insurance coverage and complex commercial litigation. He has broad litigation and arbitration experience.

In the insurance coverage area, Mr. Meagher represents corporate policyholders seeking coverage under many different types of insurance policies. His recent insurance coverage experience includes cases involving commercial general liability policies, "Bermuda Form" excess liability policies, pollution liability policies, professional liability policies, directors and officers (D&O) policies, corporate-owned life insurance (COLI) policies, property policies, cyber policies and energy package policies. He also counsels clients regarding their insurance coverage programs outside of litigation.

In the commercial litigation area, Mr. Meagher represents both plaintiffs and defendants in disputes arising out of a wide variety of commercial transactions. His recent commercial litigation experience includes representing energy sector clients in oil and gas lease disputes, title disputes and an appeal before the Pennsylvania Supreme Court.

In addition to his core practice areas, Mr. Meagher represents pro bono clients seeking Protection From Abuse orders, and has represented the Rails-to-Trails Conservancy in an appeal before the Pennsylvania Supreme Court.

Mr. Meagher's primary practice is Insurance Coverage. His secondary practices are Complex Commercial Litigation and Disputes, Environment, Land and Natural Resources, International Arbitration, Oil, Gas & Resources, Power, Renewable Energy.

Jennifer H. Thiem
Partner at K&L Gates LLP

Ms. Thiem is a Partner in the Firm's Charleston office. Her practice focuses on complex commercial litigation and insurance and risk management counseling.

In her commercial litigation practice, Ms. Thiem has represented a diverse group of clients as plaintiffs and defendants in both state and federal courts. Ms. Thiem has represented clients with a variety of cases, including claims for fraud, negligent misrepresentation, trademark infringement, breach of contract, breach of fiduciary duty, tortuous interference with contract, deceptive trade practices and trade secret misappropriation. She also regularly represents consumer financial services institutions in litigation matters in state and federal courts in South Carolina.

Ms. Thiem also provides insurance and risk management counseling for commercial policyholders. Ms. Thiem has counseled clients with respect to coverage or potential claims under a variety of insurance policies, including general liability, directors and officers liability, professional liability, employers liability, representations and warranties and commercial property. With respect to representations and warranties insurance, Ms. Thiem works collaboratively with deal counsel to represent publicly and privately-held companies in the placement and negotiation of representations and warranties insurance policies. Ms. Thiem also works with real estate counsel in drafting and reviewing insurance and indemnification provisions.

Ms. Thiem's primary practice is Complex Commercial Litigation and Disputes. Her secondary practices are Cyber Law and Cybersecurity, Financial Institutions and Services Litigation, Insurance Coverage, Product Liability.