McGriff | Executive Risk Advisors

Client Advisory

July 2022

Cyber Risks in M&A Transactions and Reps and Warranties Insurance

Cyber attacks have become part of our daily vernacular as we hear news about ransomware gangs, malware, threat actors, phishing attacks, compromised supply chain accounts, data extortion, and even double extortion tactics. We have seen a vast increase in the number of cyber attacks in the past few years, including a significant increase in ransomware attacks. There is no industry that is safe from cyber attacks — threat actors have targeted professional services, technology/telecom, healthcare, government, manufacturing, along with many other industries. In addition, there is no size company that is too small for an attack — being vigilant and proactive in incident response planning is the best offense.

When a company suffers a cyber attack, the expenses can mount rapidly. In addition to a potential ransom payment, the company may need to hire forensics and accounting experts, a public relations firm, legal breach counsel in addition to other costs such as business interruption losses, notification expenses and loss of customers or clients. Businesses can be whipsawed by suffering a first party loss and then receiving third party liability claims further down the road.

Due to the increase in ransomware attacks and active cyber criminals who always seem to be one step ahead, it is critical that strategic buyers, private equity firms, and their outside deal counsel and advisors consider cyber liability when assessing risks tied to M&A transactions, particularly where the acquiring company purchases representations and warranties insurance ("RWI").

Unsurprisingly, RWI underwriters are becoming more conservative in evaluating cyber exposure when structuring deal insurance. This more conservative approach may even lead to broad exclusions for cyber-related loss in a RWI policy when the exposures are not properly diligenced or diligence reveals red flags. To avoid RWI policy restrictions, it is critical to understand how cyber liability impacts a potential transaction and what minimum cyber standards should be in place for the target company. In the following sections, we discuss cyber diligence best practices, cyber considerations in an RWI context, and cyber policies, generally.

Due Diligence Regarding the Target Company's Cyber Hygiene

As part of the due diligence process, the buyer should assess the cyber security strengths and weaknesses of the target company (in addition to asking whether the target company has open and ongoing cyber claims). In order to purchase cyber liability insurance, most cyber underwriters now require that potential Insureds meet minimum security controls. The buyer should inquire about the following during the due diligence process:

- Does the target company have multi-factor authentication ("MFA") in place for remote access to email accounts and to the network, in desktop/laptop logins, and for all privileged accounts and critical applications?
- Does the target company have a formal written and updated Disaster Recovery Plan, Business Continuity Plan, and Incident Response Plan?
- Does the target company have patching policies and procedures in place?
- Does the target company have backup restoration programs that are regularly tested? Do they have backups that are offline?
- Does the target contract with vendors and what are the risks associated with their supply chain operations (supply chain attacks are on the rise, examples include Kaseya, Solar Winds, and Log4j vulnerability)?[1]
- What kind of data, including PHI and PII, does the target company collect and retain and does the target have data retention and destruction policies and procedures in place?
- Has the target company assessed their cyber risks by conducting penetration testing (often referred to as "PEN testing"), vulnerability testing, dark web monitoring, tabletop exercises, and phishing and business email compromise training? Tabletop exercises can identify potential cracks or gaps in the processes and protocols BEFORE a real attack or breach occurs.
- Does the target company regularly train and test their employees on social engineering, phishing, and other cybersecurity topics and pitfalls?

Considerations Related to Cyber Coverage in RWI Policies

As a general matter, RWI insures a buyer's losses from unknown breaches of representations and warranties made by a seller or target company in an acquisition agreement. Typically, RWI is structured to either replace or enhance a seller's indemnity obligation, with the buyer named as the insured. Sellers also may purchase RWI to backstop their contractual indemnity, but that is less common.

Cyber Risks in M&A Transactions and Reps and Warranties Insurance

A standard suite of representations and warranties will typically include representations relating to a target company's information technology systems and data privacy controls. Given the increased frequency and severity of claims arising from cyber breaches, RWI insurers are placing heightened emphasis on underwriting these representations. Accordingly, buyers purchasing RWI should consider the following when negotiating policy terms:

- **Specific Language of Cyber Representations**: While the representations and warranties in an acquisition agreement will vary based on a target company's industry and the relative negotiating positions of the deal parties, we often see three common elements in cyber representations:

  (1) no security incidents have occurred,[2] (2) adequate internal controls are in place,[3] and (3) target company is in compliance with privacy laws (e.g., HIPAA, CCPA, or GDPR).[4] Accordingly, buyers should demonstrate via fulsome due diligence that they have assessed and are comfortable with these risk areas (which will be necessary to provide RWI underwriters the comfort they need to cover the representations). However, even with fulsome diligence, insurers may view certain classes of business as so risky from a cyber-liability perspective that coverage of the representations is either not possible or only possible with certain coverage restrictions. These restrictions may include requiring the purchase of separate cyber coverage, flat or conditional exclusions or other policy limitations.

- **Stand-Alone Prior Acts Coverage**: RWI insurers may require that, as a condition to covering cyber-related representations, the buyer purchase cyber coverage in addition to RWI (if the target company does not already hold underlying coverage).

  Such underlying cyber insurance should contemplate coverage for prior acts (i.e., not simply "go forward" coverage) to align with RWI's focus on breaches that occur prior to the inception or closing date. In such cases, buyers should make note of any "Other Insurance" clauses in the RWI policy.[5] The buyer should understand how the Other Insurance clause works vis-a-vis other applicable policies, such as a stand-alone cyber insurance. In the event of a cyberattack or cyber breach, the cyber policy may be the primary policy while the RWI policy sits excess of the cyber insurance. In some cases, the relationship between underlying cyber coverage and RWI will be more clearly defined with RWI specifying that coverage for cyber losses is "excess of and no broader than" a specified cyber insurance policy. In these cases, the particularized "excess of" language will trump a generic "Other Insurance" provision.

- **Exclusions or Partial Coverage**: In situations where a target company's cyber exposure is only partially or inadequately diligenced, or in cases where diligence identifies problem areas, RWI carriers may expressly limit coverage. Limitations such as these can manifest by way of exclusions (i.e., specific carve outs to the coverage offered in the policy), deemed limitations in the representations for purposes of the policy (e.g., deleting specific sentences within the cyber representations for purposes of the policy's coverage or synthetically adding knowledge qualifiers to those representations), or required disclosures against the cyber representations if not already scheduled. Additionally, insurers may also limit risk by applying lower sub-limits or higher sub-retentions applicable to cyber losses.

- **Conditional Exclusions**: What happens if a buyer initiates cyber diligence before RWI policy inception, but certain workstreams remain open or questions unanswered until after coverage is bound?

  In these cases, carriers may impose what are known as "conditional exclusions" – exclusions that will remain in place until the underwriter has received outstanding diligence materials or responses to questions on open points raised in diligence, post-binding. Buyers may appreciate this option as an alternative to a flat exclusion as it provides optionality to broaden coverage under an initially bound by RWI until all diligence "loose ends" are tied.[6]

Understanding the suite of options available to RWI insurers prior to a negotiation can help deal parties get ahead of problem areas that could arise in the course of a transaction.

Cyber Policies

According to a recent Law360 article, 60% of organizations now purchase cyber insurance compared to 47% of organizations that had cyber insurance back in 2019.[7] Accordingly, a buyer's first line of inquiry should relate to whether the target company has purchased cyber insurance. If the target company has not purchased any cyber insurance, the parties should address this exposure early in the diligence process. If the target company has previously purchased stand-alone cyber insurance, the buyer must evaluate the specific terms and conditions of the cyber policy (including the policy's limits of liability, the self-insured retention, and the specific cyber coverages in place). While cyber policies can vary widely in their specific terms and conditions, most cyber policies offer both first-party and third-party coverages.[8]

First Party Coverage, amounts directly incurred by the company, can be broken down into several categories:

- **Incident Response** (costs to respond to a privacy event or security breach): Amounts covered by the policy can include legal breach coach, forensics, notification costs, call centers, crisis management, PR, credit monitoring.

- **Cyber Extortion/Ransomware** (costs to investigate and pay threat actors impairing or threatening to impair access or functionality to computer systems/data): Amounts covered by the policy can include ransom payments (often in cryptocurrency) and forensic investigation.

- **Data Restoration** (costs to restore, recreate, recollect damaged, corrupted, destroyed): Amounts covered by the policy can include costs to make determination re: data visibility, re-creation of data costs, restoration of data costs.

- **Business Interruption** (interruption, degradation or suspension of a company's or its vendor's computer system due to a security breach or system failure): Amounts covered by the policy can include forensics, income loss, extra expenses, special expenses, and in some cases, coverage for forensic accounting services (proof of loss).

Third Party Coverages are coverages for liability alleged by a third party against the company, including related defense costs:

- **Privacy Liability** (costs to defend the company against allegations arising out of a privacy event): Amounts covered by the policy can include defense costs and damages.

- **Security Liability** (costs to defend the company against allegations that the network security failed to prevent an attack): Amounts covered by the policy can include defense costs, damages.

- **Regulatory Costs** (costs to defend the company against allegations by a regulatory body): Amounts covered by the policy can include defense costs, damages, PCI (payment card industry) fines.
- **Media Liability** (costs to defend the company against allegations of trademark infringement, copyright infringement, libel, slander, etc.): Amounts covered by the policy can include defense costs and damages.

During due diligence, the buyer and their advisors should also contemplate the following:

- **Cyber Claims History and Active, Ongoing Cyber Claims**: The buyer will want to conduct diligence on whether the target company has suffered any cyberattacks or cyber incidents, obtain detailed summaries of those events (particularly if the events are ongoing, active claims and have not resolved), and if the exposures exceeded policy retentions and led to carrier reimbursement, if covered under the cyber policy. In addition to first-party losses, the buyer should inquire about third-party claims and class action lawsuits.
- **Timing Considerations are Key**: Cyber policies are nearly always claims-made and reported policies. This means that coverage applies only to claims first made against the Insured during the policy period and reported to the underwriters or carriers pursuant to the terms of the policy.

Oftentimes, hackers or bad actors can be present in a company's systems or networks many months before they are first detected. If the target has suffered a cyberattack, they will have to determine when the bad actor was first "discovered" in the company network or system and how timing considerations of discovery will impact the M&A transaction prior to the closing date.

- **Tail Insurance Coverage and Retroactive Dates**: The buyer and the target company may need to determine if tail coverage should be purchased for the target company's cyber policy with the policy inception date as the transaction closing date. The buyer could also consider extending the reporting period for pre-closing cyber breaches and/or purchasing cyber coverage with a retroactive date that would extend coverage back to pre-closing cyber events.
- **Change in Control Provisions:** The buyer will also need to review if the target's cyber insurance policy has "change in control" language.[9] A "change in control" provision may terminate coverage for the target company for any cyber incidents that occur after the closing date. This means there would effectively be no cyber coverage for the target for first-party losses or third-party claims after the closing date. Buyer and target may want to investigate whether the carrier would agree to waiving the "change in control" provision at the time of acquisition. Additionally, there may be the option for the Insured to provide written notice to the carrier of the "change in control" and agree to additional premium and terms of coverage required by the carrier in order to extend coverage under the policy.

Conclusion

Unfortunately, cyberattacks have increased in both severity and frequency as threat actors constantly evolve their tactics and techniques. It is critical for organizations to prepare ahead of time for a potential attack or breach. As demonstrated above, understanding the impact of cyber liability is key to prudent risk management, generally, and vital to managing risk in M&A transactions. We expect that this trend will continue given the financial incentive and increasing ease with which bad actors can access the tools needed to breach the systems of operating businesses.

If you have questions about this advisory, please contact:

Lisa Frist, JD
Vice President, Executive Risk Advisors
LFrist@McGriff.com
(404) 497-7590

Andrew Belisle, JD
Sr. Vice President, Executive Risk Advisors
Andrew.Belisle@McGriff.com
(404) 497-7511

[1] Supply chain attacks impacted 3 out of 5 companies in 2021. CSO online, https://www.csoonline.com/article/3650034/software-supply-chain-attacks-hit-three-out-of-five-companies-in-2021.html

[2] Sample language may read as follows: "*there have been no security incidents, intrusions, outages, successful ransomware attacks, or breaches with respect to any Systems, nor any accidental, unlawful, or unauthorized access to, or loss, destruction, acquisition, alteration, or other Processing of, Company Data maintained or otherwise Processed by or for the Company, in each case, other than as would not reasonably be expected to be material to the Company*."

[3] Sample language may read as follows: "*the Company has implemented and maintained reasonable disaster recovery and business continuity plans, procedures and facilities, including with respect to all Systems*."

[4] Sample language may read as follows: "*the Company is and at all times has been in compliance in all material respects with all applicable Laws, Orders and Permits*."

[5] Sample language may read as follows: "*The coverage provided under this Policy shall be excess to any other valid and collectible insurance coverage applicable to Loss*."

[6] For example, a conditional exclusion relating to failure to purchase underlying cyber coverage might read as follows: *for any data breach, phishing attack, malware attack, ransomware attack, or other unauthorized access to the computer systems of the Acquired Company; At the Insurers' or Claim Representative's sole discretion, the conditional exclusion may be removed upon receipt of evidence of prior acts coverage (for a period of no less than XX years prior to the Closing Date) for an amount of cyber coverage as stated in the term sheet or third party benchmarking study prepared for the Insured.*

[7] 61% Of Organizations Have Cyberinsurance, Survey Finds - Law360 (Law 360 article by Ben Zigterman, May 27, 2022).

[8] Always check the specific policy terms and conditions of your policy as each policy is different. McGriff policyholders should consult with their brokerage service team to address policy terms and conditions, current exclusions, and to consider various loss scenarios.

[9] Sample language may read as follows: *"In the event of the Insured's acquisition or merger into another entity, or the Insured's liquidation or dissolution, or the sale or disposition of substantially all of the Insured's assets that results in the loss of management control by the Named Insured, all of which collectively and individually constitute a 'change of control', this policy shall remain in full force and effect, but only with respect to any act, error, omission, incident or event which occurred prior to the date of the 'change of control'. No coverage shall be provided by this policy for any claim or first party loss which occurs on or after the date of the 'change of control' unless the Named Insured provides written notice to the Underwriters of such 'change of control' within [XX] days after the date of the 'change of control' and they have agreed to any additional premium and terms of coverage required by the Underwriters and the Underwriters have issued an endorsement extending coverage under this policy.*