The Intersection of Cyber Risk and Insurance in M&A Transactions

May 2022

LOCKTON®

AUTHORS

Josh Mikels
Senior Vice President
Private Equity Practice Leader
704.556.4137
jmikels@lockton.com

Maryam Rad
Vice President
Cyber Initiatives & Claims Director
816.960.9744
mrad@lockton.com

Edward Kim
Senior Vice President
Transaction Liability
917.351.2540
ekim@lockton.com

In a world and business environment so dependent on data, systems, and technology, all companies face a host of cyber-related risks. Retail, healthcare, and hospitality are no longer the only industries with operations highly exposed to cyber threats.

Every enterprise now has cyber-related risk exposures — and the successful ones know how to manage those risks effectively and appropriately.

A decade ago, cyber risks typically manifested themselves as breaches of credit card information, personally identifiable information (PII) or personal health information (PHI) and the associated liability, notifications costs, and governmental fines and penalties. While these risks still plague many organizations, cyber threats have also evolved.

Cyberattacks today are more sophisticated than ever before and can cause widespread damage. The expenses to investigate, mitigate, and remediate the damage caused by these new and complex cyber risks can be substantial. Many companies may also face significant brand and reputational damage, business interruption losses, and potential third party liability claims resulting from these incidents. Preventing and defending against cyberattacks requires continuous and conscientious effort. And if that were not enough, organizations must comply with a growing number of privacy protection and cyber risk management regulations.

With the rise of ransomware and other cybercrimes over the past several years seeming to take off at the same feverish pace as M&A activity, the implications for private equity (PE) firms, their portfolio companies, and their target investments are more material now than ever before. Threat actors today do not discriminate based on industry or even company size. Ransomware attacks against relatively small manufacturing firms, engineering firms, and business services operations are just as prevalent as those against global enterprises.

Coveware, a leading ransomware negotiator, reported that in the last quarter of 2021,

82%

of attacks were against companies with fewer than 1,000 employees.

Knowing that the risk is real and that it is at every business's doorstep, what does it mean for PE firms and others looking to acquire in today's robust M&A environment?

Due Diligence

With these evolving risks, reviewing cyber and technology exposures has become a vital part of diligence-related workstreams. It is important to know what systems a target company has in place as well as its cybersecurity safeguards and protocols.

Cyber risk controls, policies, and procedures are a company's first line of defense and are essential to shielding it from the disruption and costs of a breach or malware attack, and any resulting reputational damage. Knowing the risks up front allows a buyer to understand things that may need to be upgraded and implemented post-closing, along with the expense implications of doing so as a means to model those costs into pro formas.

During the due diligence process, a PE firm will be able to thoroughly assess a target's cyber risks and proficiencies.

Among other questions, a PE firm should ask:

- What protocols are in place for the transfer of data between the target and acquiring organization? Are those procedures in compliance with the applicable regulatory framework?
- What is the target's history of cybersecurity incidents?
- Does the target have policies and procedures regarding the storage, retention, and destruction of data?
  Are those policies in procedures in writing?
  How often are they updated?
- What records does the organization collect, store, and maintain?
- What protocols are in place for the use of personal devices?
- What are the target's values regarding information security, data protection, and cybersecurity awareness and education?
- What cybersecurity vulnerabilities exist in the target's supply chain?
- What does the target's cyber insurance program look like?

While a multitude of factors can go into evaluating a company's security posture, the technical cybersecurity areas for buyers to evaluate and understand include whether specific controls have been implemented by the target. Whether these controls are in place can impact the availability and depth of cyber insurance.

Key cybersecurity controls include:

- Multifactor authentication (MFA) for remote access, Office 365, and privileged accounts.
- Maintaining a regular backup schedule and keeping the backups offline.
- Use of endpoint detection and response technology.
- Training and testing employees on phishing scams.
- Implementing 24 x 7 monitoring via a Security Operations Center (SOC) and a Security Incident Event Management (SIEM) system.
- Establishing regular patching cadence with critical patches deployed within 24 hours.
- Removal of end users as local administrators on their machines.
- Implementing and testing business continuity/ disaster recovery and incident response plans.
- Full encryption of all data at rest and in transit.

Collaborating with a reputable cybersecurity firm to conduct a cyber risk assessment during due diligence as a part of a robust cyber and technology diagnostic is now an absolute must in many cases.

These assessments could include:

- Vulnerability scans
- Penetration testing
- Dark web searches
- Red team/blue team exercises

This process is very similar to hiring environmental consultants to conduct a Phase 1 or ESA for a target business with environmental risks. The main difference, however, is that every company has at least some type of cyber risk exposure.

Cyber Insurance

In addition to understanding a target company's existing cybersecurity strategies, the buyer's due diligence process should include an evaluation of any cyber liability insurance coverage in place at the target.

Given the current cyber threat environment, the cyber insurance market remains strained. Insurability itself is now an issue as some companies do not meet current underwriting standards for the existence and strength of cybersecurity controls. Cyber insurers are also limiting policy terms, lowering limits, and placing conditions on coverage.

If a target company has cyber insurance coverage, the buyer should review the following:

THE CURRENT LIMITS IN PLACE AND THEIR ADEQUACY. If higher limits are recommended based on benchmarking and risk profile, the cost of those higher limits should be quantified so they can be included in the QoE analysis. Acquiring companies should review not only aggregate policy limits, but sublimited coverages as well; some insurers are hesitant to make a full policy limit available for some risks, such as cyber extortion and dependent business interruption.

COVERAGE TERMS AND CONDITIONS. Not all cyber policy forms are created equal. Insurance policies are legal contracts, and the devil is in the details. The robustness of policy language should be carefully examined.

RETROACTIVE DATE (PRIOR ACTS). Cyber policies generally are written on claims-made and reported forms and will cover claims made and reported during the policy period. Therefore, it is critical to have a clear understanding of how far back coverage goes based on the retroactive date.

PREMIUM COST. Over the last 12 months, premiums for cyber insurance policies have increased 50-200%. Depending on when a particular company last renewed its cyber coverage, it's possible that additional cost increases may need to be modeled into pro formas.

PORTABILITY. Most cyber insurance policies have a change in control provision that would be triggered by an acquisition. While these can typically be waived for a cyber policy, buyer should confirm this during the diligence process.

...or the lack of cyber insurance

What if the target does not carry any cyber insurance? This, of course, is something that needs to be identified during diligence — but buyers must do more than just uncover this fact.

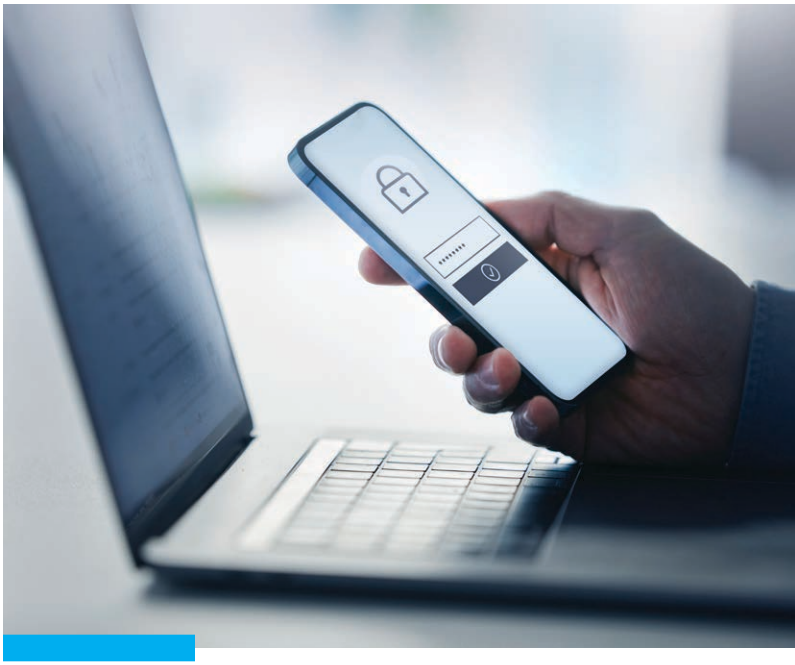
If a target company has no cyber insurance, an acquiring company should determine if the target is even insurable. The lack of coverage may foretell uninsurability, but a company's chances of qualifying for cyber insurance can be determined by reviewing a completed application and ransomware supplemental application and getting the advice of an experienced cyber insurance broker. Policy applications will provide great insight into the company's cybersecurity controls and cyber hygiene.

Understanding the cybersecurity posture of the target company via third-party cyber assessments and specific questions from the insurance diligence process is critical to ensuring the depth and strength of the target's cybersecurity posture. If, for example, the target has no MFA in place, it likely won't be able to obtain any cyber insurance until it does; if any coverage is available, it will likely include an absolute ransomware/cyber extortion exclusion.

This can even be the case for a bolt-on transaction. If the target add-on does not have the minimum controls in place, the platform company's insurer may be unwilling to add the target to the platform's existing policy at the close of the transaction.

Oftentimes, the bolt-on entity will not immediately integrate into the platform company's technology and systems, and until it does or until it beefs up its standalone systems and security, that specific operating entity may not be insurable.

If the target company is insurable, the cost to insure based on the recommended limits should be identified during the diligence process and modeled for accordingly in the pro forma.



Representations and Warranties (R&W) Insurance

Cyber-related issues have become more significant in the underwriting of representations and warranties (R&W) insurance in M&A transactions. R&W insurance underwriters now want to understand what cyber diligence has been conducted, similar to QoE, legal, insurance, and other traditional diligence workstreams. Conducting cyber diligence provides underwriters with more comfort around cyber risks and the representations being made by sellers.

In addition to information about cyber diligence around the target company, R&W underwriters also want to understand what, if any, cyber insurance is in place, given that the R&W insurance policy is intended to sit in excess of such underlying coverage. In the absence of any underlying cyber insurance in place, underwriters may look to exclude cyber- and technology-related representations from the R&W policy.

If there is no underlying cyber insurance in place, there are two ways to address the absence of coverage:

1 *Obtain cyber insurance at or before closing.*

This solution assumes the target has sufficient controls in place to be insurable. Purchasing a cyber policy requires a fully completed application and time — generally, three weeks from when the application is fully completed to obtain quotes and bind.

R&W insurers are focused on coverage for prior periods (given the "look back" nature of the representations in the transaction agreement), and less concerned about "go forward" coverage. As such, having a cyber insurance policy include "prior acts" coverage is important to ensuring R&W underwriters are comfortable with underlying cyber coverage. Given current market conditions, obtaining prior acts is increasingly more difficult — in some cases, not possible — and comes with heightened underwriting scrutiny.

2 *Include a synthetic retention in a R&W policy.*

If a target has no cyber insurance and cannot secure a policy with prior acts coverage at the time of the transaction, a "synthetic retention" can be negotiated and structured into a R&W policy such that cyber and technology representations are still covered. The synthetic retention acts as a separate, standalone retention (specific to cyber and technology representations and warranties), typically in an amount equal to the limit of cyber insurance that should have been in place at the target.

For example, if a cyber insurance limit of $3 million was recommended based on the target company's industry and size, the R&W insurer may consider a separate $3 million retention/deductible on the policy specific to these representations.

Even if a R&W insurer does not require any underlying cyber insurance, the procurement of R&W insurance with no cyber/technology exclusions does not mean coverage exists for any and all cyber-related issues. R&W insurance traditionally covers a breach of a representation or warranty; if the seller does not make a particular representation, there can be no breach. The most appropriate protection is always a combination of R&W insurance and cyber liability insurance.

What should you do?

IT ALL BEGINS WITH AWARENESS FOLLOWED BY UNDERSTANDING, EVALUATION, AND TAKING ACTION. Understanding the new world of cyber risks that we live in is a start, but the cyber and technology risk must be reviewed in the same manner diligence is conducted for business, legal, QoE and other traditional areas of M&A due diligence.

DILIGENCE MUST GO BEYOND SIMPLY CONDUCTING CYBER ASSESSMENTS. It must include a holistic understanding of the target's cybersecurity controls and cyber risk management strategies. This can be the difference between a successful deal and investment and one that goes awry.

INFORMED DECISION-MAKING AND GOOD CYBER HYGIENE WILL ALSO COME INTO PLAY DURING THE INSURANCE PROCESS. When R&W insurance is being considered on a particular transaction, it is also important to understand how a R&W insurance policy interplays with underlying cyber insurance and any limitations the R&W insurer may look to impose around cyber-related representations.

Every deal should account for these factors to provide maximum protection for the initial transaction and during the hold period.

UNCOMMONLY INDEPENDENT

SE: 1499694