AHT INSURANCE
A BALDWIN RISK PARTNER

MERGERS & ACQUISITIONS:
THE IMPORTANCE OF CYBER DUE DILIGENCE

The merger and acquisition (M&A) due diligence process is comprised of a seemingly never ending list of tasks. Assessing a target company's financial records, operations, processes, growth roadmap, and legal issues are just some of the activities that happen during the M&A process. Though it might be easier to see the business benefits and opportunities that come from merging two companies' data and digital ecosystems, **identifying the cyber risk of technology assets can prove to be extremely challenging.**

Cybersecurity due diligence is the process of identifying, anticipating, and addressing cyber risk across a company's digital ecosystem. The goal of cybersecurity due diligence is to mitigate the cyber risks that a company and its stakeholders face. Successful cybersecurity due diligence should result in a road map of remediation items with the cost and timeline to resolve issues. Revealing deal changers or breakers allow the acquirer to identify and quantify issues so the target can address the issues before closing or so that there is room to renegotiate pricing and terms for the deal.

MORE THAN

1/3

of executives responsible for M&A transactions report that they have experienced data breaches that can be attributed to M&A activity during integration

IBM Benchmark Insights

POTENTIAL PITFALLS OF NOT CONDUCTING CYBERSECURITY DUE DILIGENCE:

Because the majority of businesses today rely on technology in some way and store large amounts of information, cybersecurity due diligence needs to be a top priority in the M&A process. Failure to obtain a comprehensive inventory of digital assets and conduct the proper cybersecurity due diligence process can make an acquirer vulnerable to cyber risks which could lead to significant financial losses, jeopardize the deal, or negatively impact the valuation of a target company.

When exploited, cyber vulnerabilities acquired through M&A could pose a significant risk for the following reasons:

- Potential loss of revenue, legal repercussions, or regulatory fines
- Reputational damage to the business
- Compromised intellectual property
- Breached systems are unavailable - impacts operations of the merged entity
- Damaged morale of new and existing employees
- Stunted short and long-term growth in the marke

More than a third of executives responsible for M&A transactions report that they have experienced data breaches that can be attributed to M&A activity during integration, and about one in five reported experiencing a breach after integration.

Though we are more likely to hear about attacks on larger targets in news headlines, malicious actors will prey on any vulnerable organization, regardless of its size. Alarmingly, bad actors have begun to turn their attention to targets in the middle of an acquisition. Once M&As become public, this signals to attackers that there will be available funds that they can pursue.

Once M&As become public, this signals to attackers that there will be available funds that they can pursue.

They also see companies in the midst of the acquisition process as easier targets because the convergence of IT systems of the involved companies can leave them more susceptible to attacks. Since the M&A process is complex, organizations are preoccupied with competing priorities that likely strain available resources and human capital. This makes it more difficult to stop an attack and may also increase the time it takes to detect a breach.

CHALLENGES OF CONDUCTING CYBERSECURITY DUE DILIGENCE:

Unfortunately, there are a number of challenges that firms may face while trying to conduct a thorough cybersecurity due diligence process, including:

Fast-paced environment:
When there is competition from multiple buyers for high-value deals, there might be a limited amount of time to conduct cybersecurity due diligence.

Target company may be uncooperative:
A target company might be hesitant to provide access and documentation regarding its cybersecurity posture because it could reduce the value of the acquisition or imperil the deal altogether.

Unknown breach history:
Buyers might not discover past cyber incidents.

Insufficient documentation:
If a target company has not prioritized cybersecurity, they likely will not have documented processes that they can share with the buyer. The buyer will have to rely on discussions to obtain this information.

Navigating cybersecurity laws and regulations:
The target company's geographic location, industry, and business type determine which cybersecurity and data privacy laws and regulations it needs to comply with. These requirements can impact a transaction in ways that are not immediately obvious.

Difficulty performing assessments:
Though there are many tools that can identify cybersecurity vulnerabilities, a target company might restrict access to use these tools due to confidentiality reasons.

Level of interest:
When a target company is not as interested in selling, they might be less willing to disclose information regarding their cybersecurity posture.

Quantifying risk:
Every company uses technology in different ways, and the target organization's adoption of technology determines how the cybersecurity due diligence process plays out. Because cyber risk is dynamic, quantifying it can feel a lot like chasing a moving target. Buyers need to tailor the cybersecurity due diligence process to the target organization and should not assume that one size fits all.

MANAGING CYBERSECURITY DURING M&A TRANSACTIONS

The earlier on you evaluate cyber risk in the M&A process, the better you can evaluate the total cost of assets and liabilities. **Here are the key steps you should take:**

Include cybersecurity experts on your team:
Having a cyber aware M&A team makes the cybersecurity due diligence process much easier to navigate. Cybersecurity experts can provide guidance about creating metrics for measuring cybersecurity and aligning the risk with overarching business strategy, as well as help you understand your cyber risk tolerance.

Create an asset inventory:
An asset inventory should account for physical, virtual, and logical assets. Physical assets may include data rooms, laptops, servers, and cellphones. Virtual and logical assets to account for may include software, data, and applications. Also determine to which extent the target company relies on managed services.

Review plans and protocols:
Does the target company have an incident response plan and a disaster recovery plan? How often are these plans tested and improved? Do employees participate in cybersecurity awareness trainings?

Assess vendor risk:
If the target company has contractual obligations, you need to assess the cyber risk in these agreements.

Audit virtual and physical systems:
Conduct cybersecurity audits of the target company's physical infrastructure (data servers, facility access, security measures on laptops and cellphones, etc.), as well as systems within the company that have internet access.

Understand integration:
Determine how your companies' respective physical infrastructures and technology stacks will integrate with one another, and any issues that may arise in the integration process.

Know who has access to what:
The leading cause of cyber breaches is human error, which is why you need to know who has access to which systems and how this can create risk.

HOW DOES INSURANCE FIT INTO THE PICTURE?

Cyber attacks are more sophisticated today than ever before, and the cost of recovering from attacks quickly adds up. Threat actors do not discriminate based on industry or company size, making all enterprises vulnerable to malicious actors. All organizations need to understand how their cybersecurity correlates to financial consequences and have the right risk mitigation strategies in place so that they are able to rebound from cyberattacks. This is why, in addition to assessing a target company's cybersecurity posture, the cybersecurity due diligence process needs to evaluate if the target company has cyber insurance coverage in place that can provide financial protection should a cyber event happen.

Buyers should evaluate a target company's cyber policy and review limits, coverage terms, premium cost, and exclusions to determine if the existing policy is well aligned with the organization's cyber risk so that the company is not on the wrong side of insurance in the event of a claim. And if the target company does not have cyber insurance, the buyer needs to determine what is required to get coverage.

An experienced and knowledgeable broker can help you navigate the intricacies of cyber insurance in the context of the M&A due diligence process and recommend actionable steps to help ensure you find cyber coverage, even as carriers are increasingly stringent in their requirements for coverage.

Our team has proven experience helping clients implement cyber controls that make risks more attractive to cyber liability underwriters, as well as navigating cybersecurity in the context of due diligence to help you make sound investment decisions.

Contact us to learn how we can help.