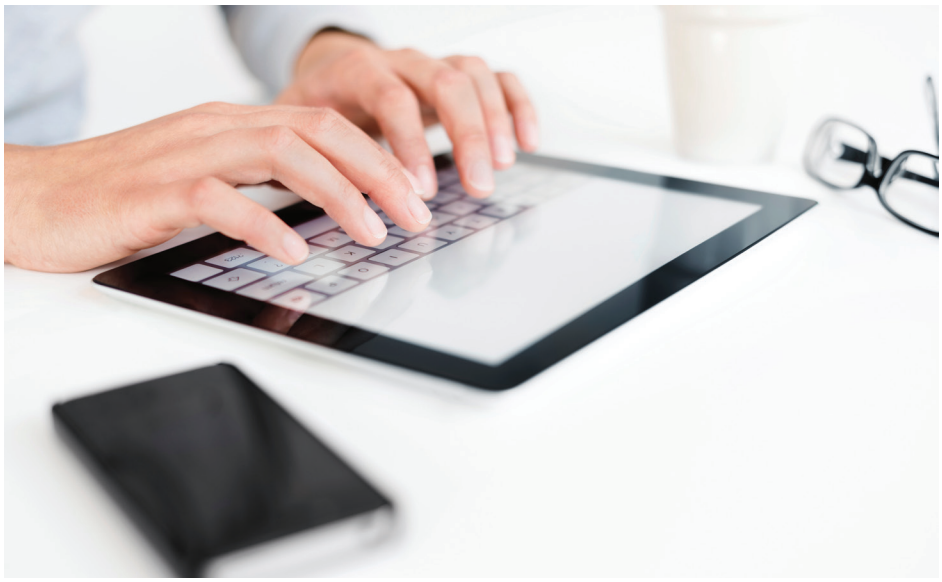
BDO KNOWS:

TRANSACTION ADVISORY SERVICES



CYBER RISKS: THE IMPORTANCE OF THEIR ASSESSMENT IN M&A DUE DILIGENCE

As the recent WannaCry and Petya cyber-attacks have demonstrated, cyber risk continues to pose a significant threat to organizations across the globe. Cybersecurity is a critical business function, yet, paradoxically, cyber risk is often insufficiently examined – or even overlooked – during the merger and acquisition (M&A) due diligence process. This often results in the acquiring company unwittingly assuming risk and placing assets in jeopardy.

The Cyber Risk Landscape and M&A

According to TIME Magazine, businesses stand to lose as much as $400 billion USD from cybercrime globally. Further, the cyber defense, cyber forensics and cyber insurance industries are projected to be worth nearly $200 billion USD annually by the close of 2020. Despite this economic outlay, however, cyber-attacks continue to grow in scale and sophistication, and occur at a rate of almost 4,000 per day.

CONTACT

KRISTIN WINFORD
Managing Director of
Transformation & Growth
kwinford@bdo.com
212-798-4036

The economic impact to companies is a very real one, with a recent Ponemon Institute study indicating ach data breach costs an average of $3.6 million USD. Given these statistics, why isn't cyber playing a more dominant role in the M&A diligence process? Our view is there are a few substantial reasons for this:

- Cyber often is viewed as just one component of the larger Information Technology (IT) diligence, and, as such, there often is a lack of robust diligence criteria around assessing cyber risk, as well as a lack of technical expertise on the due diligence team to assess it.
- IT due diligence sometimes is viewed as a lower priority during the due diligence process, and resources often are scarce given the short timeframe available to conduct diligence.
- The focus on cyber risk, if any, tends to be on compliance and not on the true analysis and assessment of risk.

While acquirers may not be focused on gaining a deep understanding of a target's cybersecurity posture, industry data suggests a high-profile cyber breach would have an immediate cooling effect on the prospects of a deal. According to a recent survey of 276 directors and officers of public companies, 22 percent of the respondents indicated they would not consider acquiring a company that had recently suffered a high-profile data breach, while 52 percent of the respondents indicated they would only consider an acquisition at a significantly lower value. Tangentially, 84 percent of the respondents indicated the likelihood of major cyber security vulnerabilities impacting a transaction was "very likely" (31 percent) and "somewhat likely" (54 percent).

The Impact of Cyber on M&A

Over the past 12 months the impact of cybersecurity on M&A transactions clearly has been demonstrated. In July 2016, Verizon announced its acquisition of Yahoo for approximately $4.83 billion USD in cash. In September 2016, Yahoo disclosed that in 2014 approximately 500 million user accounts had been hacked by a state-sponsored actor and user account information had been extracted from the company's network. Following this announcement, various news sources reported Verizon was seeking a significant reduction in the purchase price. Later, this was compounded by Yahoo's announcement in December 2016 of a second, subsequent breach. In February 2017, Verizon announced the deal with Yahoo would proceed, but with a purchase price reduction of approximately $350 million USD as a result of the cyber incidents.

Moving from Compliance to Risk Assessment

Once the importance of evaluating the target's cybersecurity posture is understood, the conversation should quickly move from "why" to "what"? If an entity is evaluating cyber risk as a part of the diligence process, the majority tend to focus their efforts on compliance logs and compliance audits. Our view is this approach is problematic for several reasons:

- Compliance audits are conducted against a standardized framework; and they only inform where the organization is non-compliant with pre-set standards. A compliance audit does not provide a snapshot of an organization's current state of assessing cyber risk or identify where issues may exist separate from the compliance framework.
- Compliance audits do not assess who has access to the target's software applications and at what level of security. Understanding which employees have access to which systems – and whether they need that access – is a critical component of assessing cyber risk. Hackers are known to "lie in wait" until they are able to identify the best way to escalate privileges, and thereby gain access to critical systems and sensitive information.
- While compliance audits may capture the existence of certain policies and procedures related to cybersecurity, they do not provide a window into the target's security incident logs, which offer an acquirer a historical and current snapshot into issues that have been identified and remediated…or not.
- Understanding the target's organizational culture is an important component in assessing cyber risk, as it has been estimated 43 percent of all data losses occur at the hands of internal actors. Organizational and cultural components are meaningful insights when determining the targets' cyber risk profile: they should not be overlooked.
- Finally, compliance audits may overlook vendor/ third-party risk, a critical aspect of an organization's cyber risk exposure. This deserves scrutiny in a diligence context as the target's vendors and third-party service providers likely may enter into similar relationships with the acquirer.

Best Practices for Evaluating Cyber Risk in M&A Due Diligence

1. Conduct a cyber risk assessment. In order to better understand how to mitigate risk, acquirers should determine the current state of the target organization's cyber risk profile. Performing a cybersecurity risk assessment is far less expensive than the cost of reacting to a cyber incident after the deal has been closed. This not only may cause reputational harm, but may result in regulatory issues for having not been prepared. By conducting a risk assessment and gap analysis, acquirers may quickly assess current policies and operations, identify gaps and prioritize remediation initiatives.

2. Take inventory of sensitive target company data. Information is often an organization's most valuable asset. It can factor heavily into deal value. Today, more than ever before, that information is at risk. The increased threat of cyberattacks in recent years, along with the creation of new data privacy regulations, only emphasize the need for companies to implement strong policies to achieve compliance and mitigate information-related risks. Understanding what information the target organization has, where it resides, and its purpose, are key factors in identifying the highest risk areas and developing a mitigation strategy. This understanding may protect assets and maximize the value of the deal.

3. Examine insurance plans to ensure adequate levels of cyber coverage. Cyber insurance may be purchased as a stand-alone policy or included as an additional coverage under a professional liability policy. Coverage levels and terms, however, may vary greatly. Acquirers should evaluate current policies and levels of coverage, particularly if cyber coverage is added to another policy form. This may help to ensure the target organization – and subsequently the acquirer - is properly protected from the potential losses in connection with a cyber incident.

4. Perform a thorough analysis of a target entity's IT systems and functions. A thorough analysis of IT systems and functions may reveal optimization opportunities to create additional value. This analysis may result in the identification of areas of underperformance and risk exposures that may serve as critical bargaining chips during deal negotiations. This analysis should include inquiries about policies, processes and services; facilities (data centers and other processing centers); wired and wireless networks; identity and access management; hardware and operating systems; applications and data; third-party risk; business continuity and disaster recovery plans; social media; and big data.