
MANDIANT
A FireEye® Company
THE BENEFITS OF CYBER SECURITY DILIGENCE IN MERGERS AND ACQUISITIONS
WHITE PAPER
FireEye

EXECUTIVE SUMMARY

THERE IS A GROWING PROBLEM IN THE WAY STANDARD MERGERS AND ACQUISITIONS (M&A) DUE DILIGENCE IS CONDUCTED — THE CYBER SECURITY POSTURE OF A SELLER CAN HAVE A SIGNIFICANT IMPACT ON THE RISKS AND COSTS TO THE BUYER.

However, most buyers do not incorporate cyber security risk into their due diligence activities. According to a global survey of dealmakers, **"78% of respondents believe cyber security is not analyzed in great depth or specifically quantified as part of the M&A due diligence process."**[1] This paper examines the benefits of cyber security due diligence in mergers and acquisitions, and outlines the characteristics of diligence that should be standard practice, but are most often missing in deals today.

[1] Freshfields Bruckhaus Deringer. "Cyber Security in M&A." **www.freshfields.com.**

THE THREAT

M&A activity expands organizations' risk profiles. Mandiant Consulting has helped several companies detect and remediate advanced attacker activity that appeared to be triggered by and focused on the M&A process. One group of financial criminals known as FIN4 targeted the seller, its law firm and even its public relations firm, probably in an attempt to make a profit by trading stocks on what they learned. In another case, an advanced espionage team, which had gone dormant after penetrating the buyer a year earlier, reactivated their illicit access once M&A negotiations were happening. The most classic threat, however, is an intruder using access to a seller's systems to move laterally and compromise the buyer. Day-to-day threats are significant enough, but M&A often presents an opportunity advanced criminals can't ignore.

PRE-ACQUISITION

Cyber security risk assessment should be considered for a stand-alone acquisition or merger as part of the standard due diligence process.

Due Diligence

Due diligence is often conducted to assess the risks that the buyer would assume when closing a potential transaction. Upon completing due diligence the buyer must decide to either accept the risks identified, adjust the terms of the deal to mitigate risks or, potentially, reconsider the purchase. There are many traditional due diligence areas that a potential buyer must consider and analyze. These include:

- Financial
- Legal
- Intellectual property
- Customers/Sales
- Supply chain strength
- Insurance

Missing from the list of customer due diligence categories is cyber security. Why hasn't cyber security been considered a focus of due diligence until recently? There are at least four possible reasons:

- **History of Due Diligence:** Due diligence focuses first on detecting existing liabilities. At a high level, this diligence is performed by examining a company's balance sheet for debt and legal filings for litigation. This documentation is readily available and the review of it is a well established practice. With few exceptions, cyber security (such as a past data breach that has led to ongoing public financial and reputational loss) does not focus on existing liabilities. The focus is on current and future risks. These risks can cascade and affect many parts of the business, but do not lend themselves to historical documentation review and auditing. This is why cyber risk has not been a natural part of the due diligence ecosystem.
- **Lack of Expertise:** Law firms, hedge funds and other due diligence implementers have amassed accounting, legal, business management and other forms of expertise to analyze potential acquisition targets. The skillset, experience and processes to analyze cyber security risk are highly technical and the accompanying law is unsettled. It will take time and focus to build the institutional expertise required to expand due diligence offerings.
- **Regulatory Challenges:** Some areas of due diligence are guided by clear requirements imposed by regulations such as Sarbanes-Oxley and environmental laws that are absorbed into the due diligence process. Cyber security lacks uniform regulatory oversight and so has historically been a "should" rather than a must.
- **Buyer Demand:** Attention to cyber security risk has traditionally lagged in the corporate transaction process, but that is rapidly changing. For example, requests for proposals for legal counsel have begun including clauses to ascertain the data protection and general cyber security program for law firms.

Contract language between companies and third-party providers now typically includes specific cyber security obligations and the right to audit corporate cyber security programs. This in turn generates demand for cyber security due diligence. If these trends continue, the due diligence firms that can't provide cyber security risk assessment will begin to be passed over for those that can.

BENEFITS OF INCLUDING CYBER SECURITY IN M&A DUE DILIGENCE

Cyber security due diligence gives a buyer a better understanding of the cyber security capability of the company to be acquired, as well as any risks the acquisition might incur. This knowledge has several benefits to both the purchase and future integration processes.

REDUCE RISK OF CYBER SECURITY THREATS

Cyber threats come in many forms, with many posing serious direct and indirect financial risks to companies. For instance, the global average cost of a data breach in 2015 was $3.79 million.[2] That's a mere pittance when compared to millions in lost sales resulting from intellectual property stolen by hackers. Meanwhile the emergence of ransomware has highlighted how easy it is for cyber criminals to halt business operations for days or weeks at a time, resulting in unrecoverable lost revenue.

TripAdvisor purchased Viator for $200 million in 2014. Soon after, it became apparent Viator was breached – a breach that affected 1.4 million users.[3] In addition to the direct costs of remediating, the acquisition was considered largely responsible for a 4% decline in TripAdvisor's stock price.[4]

A $40 thousand assessment that discovers a $4 million cyber risk exposure can provide a 100-fold return on investment (ROI).

Scale Insurance Appropriately

Cyber insurance continues to grow in popularity, but how much insurance covers the risk the buyer is accepting? There is little on which to base this number unless cyber risk is assessed. In addition, if due diligence is performed and is provided to the insurance company, a lower premium could be offered to the buyer, thus providing an additional return on investment.

Estimated Costs for Security Re-baselining

For mergers, being able to gauge the cost and effort of integrating IT infrastructure is critical. When the cost is high, it could affect the terms of the acquisition. A cyber risk assessment provides focused and actionable insight that the buyer would not normally get from traditional due diligence.

Cyber security due diligence gives a buyer a better understanding of the cyber security capability of the company to be acquired, as well as any risks the acquisition might incur.

[2] Ponemon Institute. 2015 Cost of Data Breach Study: Global Analysis. May 2015.
[3] Goldman, Jeff. "Data Breach at TripAdvisor's Viator Impacts 1.4 Million Users." eSecurity Planet. 24 September 2011.
[4] Zacks Equity Research. "TripAdvisor (TRIP) Down on Viator Data Breach Concerns." Zacks. 23 September 2014.

A $40 thousand assessment that discovers a $4 million cyber risk exposure can provide a 100-fold ROI.

Protect Intellectual Property

In many M&A deals, the intellectual property of the target acquisition is a large component for the basis of the deal. When intellectual property is at stake, the buyer should look for potential prior or ongoing data theft.

Advantages for the Seller

Performing due diligence before becoming acquired can provide distinct advantages for the seller.

- Identify and fix problems before they are made issues by the buyer's due diligence (similar to fixing up a house before putting it on the market)
- Improve the Offering Memorandum through third-party endorsement ("Our cyber security posture has been rated as Low Risk by.....")
- Provide greater confidence in valuation calculations

COMBINATION VS. STAND ALONE

Given the potential of cyber security breaches and security program gaps to harm a company's bottom line and reputation, M&A due diligence teams must incorporate cyber security into their overall risk assessment. There are several factors that impact mergers and acquisitions.

Mergers

1. Merging two separate infrastructures creates challenges:

   a. Maintaining adequate security posture of both networks while integration occurs. There is a higher risk of exposing new vulnerabilities when changes are made, especially in access management. When companies merge, there are "new employees" that are being assimilated into the environment, and constantly changing roles.

   b. Level of effort to ensure that network monitoring and detection is absorbed into the acquirers existing security operations, net new assets to understand traffic patterns and baseline activity, insert distributed denial-of-service (DDoS) attack protections etc.

   c. Possibility of the target acquisition being compromised and spreading malware, or already established unauthorized access leveraged against the acquirer through infrastructure interconnections.

   d. Cognizance of accepted risk in both organizations' networks and applications culminating in a sometimes unacceptable aggregated risk picture.

   e. Target acquisition has a better security program than the acquirer, resulting in a myriad of decisions on which components to keep.

   f. Identification, baseline activity and access to the most important assets in the target acquisition.

2. Stand-alone acquisitions create a different set of challenges:

   a. An ongoing breach means that the acquired company is to some extent controlled by an unknown attacker. Moreover any sensitive data or intellectual property might already be gone, affecting the value of the acquisition target. The buyer must also deal with a public relations fallout, which can be very costly and damage the company's reputation.

   b. If the acquired company suffered a breach in the past that only comes to light to the buyer later, valuable data may have been lost, and the intruder could still be in the network. Did the acquired company remediate fully?

   c. The acquired company may be host to a persistent attacker that maintains a presence in the environment, watching and waiting. There are many ways for such an intruder to move into the acquiring company, even without direct interconnections.

   d. A generally insecure, commodity malware-riddled environment cannot be trusted even if there is no evidence of a focused attack. Remediation could mean an unexpected, expensive IT investment.

   e. An inadequate security program at the acquired company will generally lead to systemic cyber security issues. Weak oversight and guidance over a period of time can lead to increased costs and effort to bring the company up to speed.

   f. The possibility of insider threat rises if people at the acquired company are concerned about their positions. Is monitoring in place to detect malicious activity?

WHEN TO START CYBER SECURITY DUE DILIGENCE

Cyber security should be planned for like any other form of due diligence — as early as possible. Because the quality of cyber security due diligence depends on some fairly specific requirements, some language may need to be inserted into agreement documents such as a Letter of Intent (LOI). This will enable key components of cyber security due diligence, such as network monitoring. Some key staff should be allowed to be part of the due diligence process; relying solely on documentation is not enough.

M&A due diligence teams sometimes contain IT subject matter experts who are occasionally asked to provide an opinion on cyber security posture. However, cyber security is a specialized field, and if security expertise is not available on staff, due diligence providers should start planning to engage external experts.

WHAT CYBER SECURITY DUE DILIGENCE SHOULD BE

Cyber security is a fundamental piece of the due diligence puzzle, but what should it look like? The following factors should be incorporated into effective cyber security due diligence planning.

M&As can vary widely in terms of ramp-up time. Some allow for a very short due diligence effort, while longer deals can afford months to assess risk. Business decisions control this pace, not the due diligence team. Therefore it is important to have relatively quick and lightweight cyber due diligence options as well as longer, more in-depth approaches.

The cyber security posture of a seller can have a significant impact on the risks and costs to the buyer

Due Diligence at Pace

Even if the window for due diligence is short (1-2 weeks), much can be accomplished to provide a high-level view of the risks of the seller environment. A week provides time for cyber security experts to conduct documentation review and interviews with seller staff, which they then analyze in a focused risk framework. The product of this activity should be a quantified risk assessment across important cyber security domains (data safeguarding, infrastructure security, and others) in a brief, easy-to-understand report on risk and general recommendations for the buyer.

Even a brief cyber security due diligence period should also have a technical component to provide an objective view as to the health of the seller's security posture. One of the most important aspects of a technical assessment is creating a historical scorecard going back in time: Have the seller's computers been compromised in the past? If so, what was the character of those breaches (advanced and persistent, commodity, insider, financial fraud, etc.)? The Freshfields survey discovered that 90% of respondents believed that a past breach could reduce the value of a deal.[5]

A current snapshot is also important. Detecting malicious activity (or the lack of such activity) from the seller provides insight into the overall security posture and types of possible intruders already in place. This needs to be recognized and analyzed in a relatively short time frame.

After this analysis the now-informed buyer can act to significantly reduce the risk of major missteps.

In-Depth Due Diligence

If more time is available, more detailed and granular cyber security due diligence is possible. In addition to a risk assessment conducted by cyber security analysts, software agents can be deployed in the seller's network to report on the state of the endpoints.

Network monitoring can examine traffic to and from the network for a period of time to collect very detailed information on the state of the organization's cyber security and what compromises are happening, or have already happened. This allows the buyer to know the seller's environment inside and out from a real-world risk perspective, and provides both the high-level view needed to inform decisions and granular detail to estimate remediation costs.

The Results

As with all due diligence efforts, the intent of cyber security due diligence activities is to inform the risk decisions of the buyer and to prevent unplanned liabilities. Do the terms of the deal need to change? Is the acquisition still worth pursuing if the cost to mitigate the risks is too high?

Also, like most other types of due diligence, cyber security due diligence can add value post-acquisition by helping scope some common post-acquisition activities.

[5] "Cyber Security in M&A." www.freshfields.com. Freshfields Bruckhaus Deringer.

OPTIONS GAINED BY BUYERS BECAUSE OF CYBER SECURITY DUE DILIGENCE

Information about cyber risks provides beneficial options for the buyer (Fig. 1). With due diligence, options can be seen starting in the lower left quadrant, with the best possible outcome: minimal risk, which is understood and accepted. Due diligence discovery of risk opens options for the buyer, such as price or terms negotiation, security uplift for the acquisition, or transference of risk through insurance.

Organizations should seek to avoid the upper right quadrant, with the lack of due diligence leading to an array of unforeseen and potentially costly outcomes. At that point, the only option is damage control.

Only with due diligence can risk be incorporated in planning, with various planned costs and benefits. Without due diligence, there are only unexpected costs and reputational impacts.

POST-ACQUISITION ACTIVITIES

Information gathered during due diligence can be used to guide post-acquisition activities.

Integration

A fairly common follow-on activity, particularly with mergers, is integration of the two companies' IT infrastructures. In the long run, this should reduce costs and ease management. However, in the short-term it can create its own set of problems, and become a long-term effort.

One of the first questions to answer is: What can be trusted? Is it safe for the buyer to connect to certain acquired systems? Can two-way trust relationships be established? All of these depend on assessing the security of both the overall environment and specific systems. Cyber security due diligence is a good start and can allow for level of effort and cost estimates to be made and included in IT planning.

Continuous Monitoring

In some post-acquisition or merger cases there will be a need or risk-based decision to put a continuous monitoring program in place. This can apply to organizations needing oversight consistent with Securities and Exchange Commission (SEC) guidance and other relevant regulatory requirements. Security baselines may need to be adjusted by both parties to align requirements and expectations post-acquisition. Some cases may require the development of a tailored continuous monitoring program that closely fits organizational requirements.

THE FUTURE IS ALREADY HERE

The impact of adverse cyber security events has been felt by businesses for some time. Current news gives some sense of the scale of the challenges that have emerged as even local businesses can be exploited by global criminals. Cyber security risk is not science fiction, even though it has essentially been treated as science fiction by being left out of M&A processes. Acquiring companies and due diligence practitioners must now catch up to the reality of the costs and risks that cyber security issues create, and the benefits that cyber security due diligence can bring.

FIGURE 1. HOW BUYERS IN M&A TRANSACTIONS BENEFIT FROM DUE DILIGENCE.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

To learn more about FireEye, visit:
www.fireeye.com/services/mergers-and-acquisitions-risk-assessment.html

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com