Feb 2, 2022, 08:15am EST | 23 views

Why Cyber Due Diligence Is Imperative For VC, M&A And Private Equity Firms

Jim Goldman Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

Innovation

Jim Goldman, Co-founder and CEO, Trava Security, Inc.

GETTY

With the recent uptick in cybercrime in general and ransomware in particular, venture capital (VC), mergers and acquisitions (M&A) and private equity (PE) firms have had to broaden the scope of their due diligence efforts on potential investments to include cyber due diligence. But

given the lack of standards and frameworks against which to perform such cyber due diligence, investment firms are often at a loss as to where to turn for high-quality, affordable cyber due diligence research and reporting that can be delivered on their tight schedules.

Historically, due diligence was synonymous with the financial health and market potential of a target investment. Today, when it comes to investment, "buyer beware" is no longer limited to financial due diligence. Investment firms such as VC, M&A and PE must be able to quickly determine the cyber maturity posture and identify the cyber risks that could impact the parties involved in the transaction.

What is cyber due diligence?

Cyber due diligence involves identifying and addressing cyber risks across a company's information and data network. This process serves several purposes:

1. It identifies potential gaps in the firm's security systems, helps stakeholders understand where the business is most vulnerable and addresses areas of risk before they are exploited.

2. It also helps those organizations under consideration better manage third-party relationships by more effectively monitoring their vendors' cybersecurity posture.

3. Cyber due diligence helps determine if the business is adhering to the strict compliance and regulatory requirements when it comes to handling

and protecting its data. This should include assessing the safe transfer of data in the case of an M&A.

4. The insights gleaned from going through the cyber due diligence process with one deal can be used to establish benchmarks that can then be applied when assessing future investment opportunities.

What should be included in a cyber due diligence report?

VC, M&A and PE firms should engage a cyber risk management provider or virtual chief information security officer (vCISO) that specializes in conducting a comprehensive cyber due diligence process and providing a detailed report of the findings, along with recommendations for the company being considered. All to include:

1. Conducting an automated technical vulnerability assessment with targeted risk analysis that informs a cyber risk profile

2. Completing a critical controls survey to determine the cybersecurity capabilities of the target investment/acquisition company

3. Preparing a cyber due diligence report that includes an overall risk scoring profile and categorization, as well as a detailed analysis and technical findings

How do firms accomplish cyber due diligence on a tight timeframe?

The entire due diligence process, including cyber due diligence, can average 30 to 45 days for medium-sized deals ($1 million to $25 million), and often there is time sensitivity when it comes to the investment decision.

Many investment firms find it helpful to use an automated, data-driven approach to identify and baseline the cyber risk of target companies and investments. In these situations, automated assessment platforms that enable extensive scanning of internal and external technical environments with detailed surveys and phishing simulations serve to evaluate people and process weaknesses.

There are other advantages to investment firms running automated scans:

• External infrastructure vulnerability scans, targeted at your network's external IP addresses, provide useful information about vulnerabilities as well as a list of ports that are open to the internet.

• Internal network vulnerability scans, performed from a location that has access to the internal network you are scanning, show vulnerabilities at a greater depth as they can "see" more of the network compared to an external scan only.

Up to this point, we have explored the importance of cyber due diligence for investment firms pre-acquisition. But in the particular case of private equity — because they are actually owners of the businesses — it is equally

important to run vulnerability assessment scans on a regular basis post-acquisition.

Running these scans allows business owners to find weaknesses in the systems that could help avoid potential incidents and identify pressing security issues.

In conclusion, for today's VC, M&A and PE firms, evaluating a company of interest's cyber hygiene is as important as assessing its financial health and market potential. Cyber due diligence research and reporting provide necessary insights that are imperative for making the right investment decisions pre-acquisition as well as ongoing insights into the cyber posture of a company post-acquisition.

Follow me on Twitter or LinkedIn. Check out my website.

Jim Goldman

Jim Goldman, Co-founder and CEO, Trava Security, Inc. Read Jim Goldman's full executive profile here.