Cyber-Integrity

Buyer Beware: Cyber Diligence in M&A

By Cynthia Cole, Cyrus R. Vance Jr., and Alan Zoccolillo

Trillions of dollars are spent on M&A each year, yet reports suggest that less than 10% of deals integrate cybersecurity into the due diligence process.¹

Despite the FBI and private watch dog groups raising multiple warning flags about ransomware groups hitting more and more companies in the middle of significant transactions like M&A, and despite increased focus from the FTC and the SEC on data security failures as legitimate reasons for shareholder and government enforcement actions, companies continue to struggle with how to capture and mitigate cyber risk in an M&A transaction. Even with increased top down pressure from Boards of Directors and the potential for breach of fiduciary duties related to lax data security measures, companies are fumbling the ball on what questions to ask and how to measure the security risk in a target.

Whose risk is it?

Where does the responsibility lie for an acquiring company to understand and evaluate cyber risks in an acquisition? How can these risks be identified and mitigated in the middle of a fast-paced deal? A data breach can have serious financial consequences to both the buyer and the seller. A significant security breach can lead to a nearly instantaneous devaluation of assets and can severely damage the acquiring company's business viability, raising serious questions as to purchase price and follow-on integration issues. Unresolved risk can also push investors to question the impact of future attacks. And for good reason: An increasing number of deals have stalled or not gone through at all since the widely publicized 2017 Yahoo disclosure of a data breach which led to a decrease in the deal price for Yahoo in its acquisition by Verizon Wireless Inc. Initially Yahoo did not disclose any significant cyber events but later disclosed an earlier data breach affecting more than 500 million users. The following day Yahoo's stock dropped 3%, and it lost $1.3 billion in market capitalization.

Verizon determined that the incident was a material adverse event under the stock purchase agreement and the parties agreed to reduce the purchase price by $350 million, or 7.25%. In response to this and

---

¹ Aon Cyber Solutions, 2020 Cyber Security Risk Report
similar incidents, and as cyber events increase in scope and complexity, investors are requiring more detailed quantification of cyber risk exposure, including risks of financial loss and reputational harm.

Upgrade your diligence

Preemptive and proactive cyber integrity risk assessment must be incorporated into the M&A process. This means that dedicated cyber and security experts must be involved at an early enough stage of the transaction to gauge a company's cyber security and resiliency. Risk reports should inform both initial deal-making and stay relevant through the lifecycle of the deal.

There is no simple playbook for an acquiring company to address cyber risk but the diligence process is key to getting it right.

As part of efforts to uncover cybersecurity risks or incidents at a target, some key areas for an acquiring company to direct its focus include:

- **IT and data assets**: What IT assets, systems, software, platforms, websites and applications exist and are critical to the target? How is company data stored, and is it encrypted?

- **Governance practices**: Who has responsibility for privacy compliance and data security within the company and for overseeing security preparedness? Is there a specifically appointed data protection officer?

- **Security risk management**: What is the target’s data security infrastructure? When and how has it been upgraded? What third parties are involved in maintaining?

- **Historic incident or loss experience**: Has the target received complaints from customers, employees, contractors or other third parties regarding data privacy and security practices? Have any such complaints resulted in litigation or other proceedings?
Sharing information with third parties: How does the target vet third party security infrastructure, policies and records? Does the target ensure audit rights in contracts with third parties? Has the company assessed its obligations to notify customers and regulators in case of a breach?

Ultimately, while these examples provide a starting point for appropriate cybersecurity diligence, it is critical that the acquiring company tailor its diligence on data privacy and security matters to the target company by also understanding its data collection and use practices. Foremost, the forthrightness of the target in these matters is of increasing importance. A blank stare or a vague response to any of the data security questions is itself an answer and should be given attention.

Conclusion

Cybersecurity and resilience has become increasingly important for successful business practices. Executive teams are judged on lax security measures and appropriate breach response. Ransomware is increasing at an alarming rate. Ignorance or the inability to obtain a straight answer from a seller company no longer appeases shareholders and regulators when significant fines and enforcement actions could be at stake. Cyber integrity and proper data security due diligence is no longer a "nice to have," it is a necessary and critical part of M&A.

Jake Rubenstein contributed to this article.