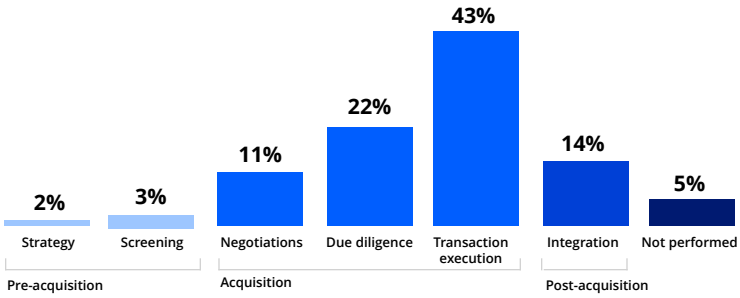
PERFORMING CRITICAL CYBER DILIGENCE FOR MERGERS AND ACQUISITIONS USING MIXMODE

According to a recent M&A trends survey conducted by Deloitte, 51 percent of 1,000 Executives responsible for Mergers and Acquisitions (M&A) at U.S. companies and private-equity investor firms listed cybersecurity threats as their top concern in executing deals virtually. (Compliance Week)

Especially now - as virtual work environments and digital-first processes are driving business in a post-pandemic era, cyber risk assessments must play a major role in M&A deals. 80 percent of global dealmakers said they uncovered data security issues in at least one-fourth is their M&A targets. From poor due diligence, to failures in post-merger processes, data security issues have created catastrophic exposures for numerous companies.

Figure: When organizations perform a comprehensive cybersecurity assessment



CYBER ATTACK ACQUISITION RISKS

After the disclosure of two massive data breaches, Yahoo and Verizon agreed to new terms for the sale with Verizon paying $350 million less than originally planned. The two agreed to accept the hacking from the terms of "business material adverse effects" that could have affected the deal from closing with Verizon refraining from making any further attempts to reduce the deal price because of these hacks. Many wondered at the time if Verizon would simply cancel the Yahoo deal.

Another recent example known to MixMode involved a private equity company that acquired an e-commerce platform, and during the post-acquisition period, learned of a breach affecting the company's public-facing application server. An attacker had gained unauthorized access to the underlying operating system, installed malicious code, and was skimming the credit card information of customers performing legitimate transactions.

Unfortunately, the private equity company had not integrated cybersecurity into its due diligence process at the time of this acquisition but discovered immediately a cybersecurity solution was needed to be able to bring extensive external data and expert analysis to investigate the nature of the breach and assist the e-commerce platform with remediation.

Over 700 customer credit cards were flagged with fraudulent charges and this event caused significant damage to the brand reputation of the e-commerce platform. **In hindsight, if proper diligence had been completed prior to the acquisition, the private equity company would have known about the breach before closing the acquisition.**

In the end, the private equity company's quick action likely saved the business but not before the e-commerce platform suffered damage to its reputation and was forced to spend six figures remediating all of the damage the attacker had already done.

Figure source: IBM Institue for Business Value benchmark study, 2019, n = 720.

MIXMODE FOR MERGERS AND ACQUISITIONS

Network and data vulnerabilities can seriously threaten the value of a business. With intelligent adversaries and attacks on the rise, cybersecurity has become a crucial step in the due diligence process for M&As.

When a company is acquired, the buyer typically then owns all the data, technology and assumes the liabilities related to data security - past, present and future. For the seller, a lucrative deal for shareholders and employees could fall through on due diligence or a lawsuit by the buyer if insufficient cybersecurity is discovered.

MixMode's unsupervised AI threat and anomaly capabilities enable both private equity firms with portfolios of potentially vulnerable acquisitions and high-growth start-ups looking for a buyer with the ability to proactively hunt for malicious events in any network environment along with continuous self-supervised AI-powered monitoring before, during, and after a successful merger.

Given the damage of what an attack can do to ignoring cybersecurity assessments in M&A due diligence can result in serious risks to all parties. Cyber due diligence is integral to maintaining the value and integrity of the seller and their shareholders. To learn more about MixMode's next-generation AI-powered cybersecurity platform contact us to schedule a consultation and demo.

USING MIXMODE GIVES ANY ORGANIZATION WITH AN M&A OPPORTUNITY:

Deployment in Less Than an Hour
When assessing an acquisition candidate the acquirer has limited time and access to the target company's environment. MixMode provides a lightweight software-based sensor that can be deployed in less than an hour. Furthermore, this passive sensor sits out of band and will not impact the target company's network performance.

Comprehensive Coverage *(Cloud + Network + Logs)*
Assessing target organizations with hybrid environments is no problem with MixMode. With the ability to ingest public cloud data (AWS, Azure & GPC), on-premise network data and logs, MixMode gives you the complete picture for any potential acquisition.

Immediate Network Visibility, Accurate Network Baseline, and Actionable AI Insights
MixMode Unsupervised Third-Wave Artificial Intelligence is the only AI that can build a self-evolving baseline of network behavior based on current network conditions. This allows for immediate visibility and actionable AI-based insights where other tools can take months and in some cases years to provide such data.

Faster detection and Investigation, Better Correlation and Less Noise
In an M&A situation, the acquiring company can't wait 6-12 months for actionable AI insights. MixMode's Unsupervised AI with an industry-leading 7-day deployment and baseline period provides the insights you need in a matter of days rather than months with 95% less noise than other tools increasing productivity and efficiency tenfold.

Multi-Stream Network Anomaly Detection and Correlation
MixMode's generative model baseline intelligently monitors all network data in the cloud, on-premise, or in hybrid environments. Leverage MixMode's third-wave, unsupervised AI to identify in-context anomalous patterns, trends and threats across streams from incoming, outgoing and local traffic.