PROTECTING INVESTMENTS THROUGH M&A CYBERSECURITY DUE DILIGENCE

Failure to appropriately assess cyber risk can lead to deals derailing and the assumption of unwanted vulnerabilities

Dave Harvey, senior director

Ayala Maurer-Prager, consultant

As we tentatively return to relative normality post-Covid-19, M&A activity is surging to pre-pandemic levels. With attackers exploiting critical vulnerabilities at speed, however, the identification and quantification of cyber risk provided by the due diligence process is assuming ever-increasing importance.

The consequences of cyber incidents remain largely unchanged by COVID-19: costly incident response, reputational damage, IP theft, regulatory fines and litigation are unwavering threats. M&A due diligence processes, however, are having to adapt to a threat landscape that continues to be socio-politically shaped. The pandemic has catalysed a sharp rise, for example, in ransomware attacks on the Life Sciences and Healthcare industries[1]. Whilst consumer demand makes investment in these fields an attractive prospect, the M&A due diligence process must place increasing amounts of emphasis on evaluating sector-specific risk.

By its very nature, the M&A process contributes to permutations in risk at various points. Publicity around M&A deals, while desirable and necessary in many situations, also notifies malicious actors of current business valuations and their potential market growth. Insider threat also becomes a factor to consider as the M&A lifecycle progresses: if employees feel under threat of redundancy, for example, malicious activity from the inside can spike. M&A cyber due diligence must therefore continue to expand its scope to assess a business's security and resilience capability from a human and technological perspective.

Organisations must be fully aware of their digital attack surface and level of cyber-risk exposure: and the due diligence process, performed correctly and independently, is primed to generate this strategic intelligence. Prioritising the remediation activities identified by assessments of this kind will significantly improve business resilience capabilities.

Discussions around due diligence in an M&A context often focus on traditional risks to the acquisition or investment target. A question that is less often considered though is: what does inheriting the digital vulnerabilities associated with a target business mean for the security of the acquiring party? It is here that integration risk becomes a key area of focus. It is not beyond the realm of possibility, for example, that a threat actor could exploit the system or infrastructure vulnerabilities of the target business to attack the acquiring company as integration progresses. Considered through this lens, cyber due diligence might also provide important insight into how the acquiring party's own risk profile might change as a result of the deal.

It is also critical to understand that you are only as resilient as the weakest of your third-party suppliers. It is not enough to have contracts in place defining how these third parties process and protect your data. Today, businesses must provide a level of assurance around compliance and be confident that their organisation has full visibility of what data can be accessed, who can access it, and how it is stored and handled.

How will this continue to evolve?

We are likely to see digital synergies becoming key considerations in M&A transactions as investors look for increasingly frictionless portfolio integrations. As a result, the question of an acquisition target's cyber readiness becomes a pivotal one.

The role of innovation in cybersecurity due diligence is also worth monitoring. From a practitioner's perspective, using artificial intelligence and data analytics to scan hundreds of documents, such as supplier contracts, can make an assessment faster, more standardised, and more accurate. From a threat perspective, however, we are seeing malicious cyber actors rapidly exploiting vulnerabilities within these automated processes. Due diligence methodologies must therefore work to maintain the fine balance between effectiveness, efficiency, and their own security.

To generate the accurate assessment crucial to successful M&A transactions, cyber due diligence must be comprehensive. Cyber-related vulnerabilities are not just the result of technological gaps, but of erroneous human interactions with machine processes, poor business practices, misplaced investment priorities, and employee satisfaction. In a world where a cyber incident has an aura of inevitability, cyber due diligence must be developed and carried out with a dynamism and agility that matches the threats and risks it seeks to mitigate.

1 HTTPS://US-CERT.CISA.GOV/NCAS/ALERTS/AA20-302A

FTI CONSULTING | CYBERSECURITY

FTI Consulting, Cybersecurity, 200 Aldersgate St, London, EC1A 4HD
E-mail: Dave.Harvey@fticonsulting.com / Ayala.Maurer-Prager@fticonsulting.com
Tel:+44 (0)20 763 25147 **Web:** fticybersecurity.com/thelawyer