Beazley Logo

Article

Buyer’s remorse: acquiring cyber risk

Tim Allen

Despite ongoing market disruption and uncertainty, dealmakers remain eager to seize new opportunities. However, the mergers & acquisition (M&A) landscape has evolved significantly since the last boom, bringing new challenges and considerations to the forefront. One critical factor that must not be overlooked is cyber security. When acquiring a company, the buyer not only inherits its assets but also its cyber risks, and it can become a target of cyber criminals.

According to our annual Risk & Resilience research1, **29%** of global business leaders identified cyber risk as their most pressing technological concern. Yet, despite this awareness, cyber risk and security in M&A transactions is often an afterthought post the financial negotiations. Fewer than **10%** of M&A deals reportedly involve thorough cyber security scrutiny.2 This oversight can have profound financial, operational and reputational implications.

A cautionary tale

The 2017 Yahoo-Verizon acquisition serves as a stark reminder of the costly consequences of overlooked cybersecurity. Verizon’s planned US$4.5bn purchase was disrupted when data breaches from 2013 and 2014 surfaced, reducing Yahoo’s valuation by US$350m and leading to US$115m in fines and shareholder payouts.3

While it remains the most high-profile example, Yahoo it is not unique and in the intervening years the cyber threat has only grown more complex. M&A activity often attracts cyber risk, and third-party vulnerabilities are a persistent risk. It is also essential to assess third party vendor relationships and system integration points, and check if they meet the acquiring firm’s security standards.

Uncovering hidden risks

Acquirers may also inherit identified and unquantified risks, leading to unexpected costs. Poorly planned IT integration and legacy IT systems

can introduce vulnerabilities.

Standardising security tools and protocols is essential to protect the combined organisation. Assessing the existing vendor relationships of the acquired companies is also key. What contracts do they have with third parties, and are they compliant with the acquiring firm's security standards?

In the post-acquisition rush, cyber criminals often look to exploit transitional vendor weaknesses. High profile attacks on vendors like CDK4 and Change Healthcare have shown how cyber criminals can disrupt entire ecosystems.

Expanding attack surfaces

The proliferation of edge devices and the Internet of Things (IoT) is expanding the attack surface. In today's hybrid work environment, personal devices often link to corporate systems, creating new 'back door' vulnerabilities. Cyber criminals can exploit weak passwords and unsecured apps to gain access to corporate systems.
But not all cyber risks are as sinister as a bad actor lurking in the acquiree systems. Often more rudimentary challenges can often lead to operational headaches and prevent the acquired firm from meeting expectations. For example, domain expirations and a lack of administrative credentials can cause significant disruptions, making gaining control over these critical digital assets from day one essential to ensure business continuity.

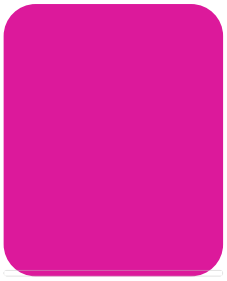
The human element

The risks don't end once the deal is done. While boardroom celebrations may be underway, disgruntled employees from the acquired firm can pose insider threats. Managing and monitoring access rights during the transition period is a vital step in safeguarding the organisation's system security.

Involve cyber specialists from the start

Cyber security should be a core component of the M&A due diligence process, and not an afterthought. Involving cyber security professionals from the outset allows potential risks to be identified and addressed early, rather than waiting until post-acquisition integration. This proactive approach can help to uncover areas where additional resources or third party expertise may be needed, strengthening the overall combined firm's IT framework.

Embedding cyber security into the due diligence and integration phases of an M&A, companies can better protect their investments, reduce the risk of post-deal surprises, and avoid the kind of buyer's remorse that can lead to liability claims from shareholders against company executives.



Tim Allen

Head of Global M&A

[1] Methodology | beazley

[2] Ignoring Cybersecurity Can Sour M&A Deals

[3] How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom | CNN Business

[4] How the ransomware attack at Change Healthcare went down: A timeline | TechCrunch

Home

©Beazley Group | LLOYD's Underwriters