MARSH JLT SPECIALTY

INSIGHTS | OCTOBER 2020

Why Cyber Risk Should Be Quantified in M&A Transactions

More and more dealmakers consider cyber risk during their due diligence processes. Yet there is often a lack of insight into the potential financial impact of acquiring an asset that may have previously suffered a cyber-attack/incident, or could suffer one.

Dealmakers should consider modelling this potential financial impact and incorporate the insights into their M&A strategy. This will ensure they are fully informed of the range of costs they could incur, and also allow them to develop strategies both pre- and post-deal to reduce the potential financial impact and preserve deal value.

Cyber Risk's Impact on Deals

Cyber threats have continued to increase in sophistication, frequency, and impact. Over the last few years the global cost of cybercrime has steadily increased, and is ***projected to reach US$5.2 trillion over the next five years***, according to Accenture.

Cyber risk presents a particular challenge for dealmakers, as cyber vulnerabilities can be inherited through transactions. The acquisition and/or integration of portfolio assets may bring exposure to cyber risk and technical debt through vulnerable legacy technology, inadequate cyber security controls, or compromised supply chains. In fact, when levying fines on companies for data breaches, the UK's Information Commissioners Office has sometimes cited a failure to conduct adequate due diligence prior to purchase as an aggravating factor in its judgement.

Traditional due diligence may not pick up on or adequately quantify these risks, which increases the likelihood of cyber-attacks or cyber-related incidents causing significant losses that could destroy deal value post-acquisition. In some cases, hidden cyber vulnerabilities have led to losses for dealmakers that were greater than the value of the asset they had acquired.

What Should Dealmakers Do?

As part of the due diligence process, dealmakers should seek to quantify the potential financial impact of a cyber-attack or incident taking place at one of their portfolio assets, and reflect the outcome in their deal strategy.

Quantifying the financial impact of a cyber-attack or incident is not straightforward, but, when done well, it can provide a reasonable estimate of the categories and scale of the direct costs that may be incurred by dealmakers if the worst was to happen. Attention must be given to tangible costs such as investigative costs, fines and penalties, as well as intangible costs such as reputational damage.

This quantification can be combined with more traditional due diligence to gain a fuller and financially driven picture of how cyber risks could impact a potential acquisition.

MARSH

FIGURE 1

The cost of recovery after a cyber breach can potentially outweigh the expected ROI or deal value of an asset.

SOURCE: MARSH.

REINSTATEMENT COSTS

Cost of repairing systems affected by a breach or corruption.

CALL CENTRE COSTS

To set up a call centre to provide information to those affected.

CARD REISSUANCE LIABILITY COSTS

To stamp, notify, and mail out new identification cards.

PRIVACY NOTIFICATION COSTS

To distribute information to individuals affected.

CARD NETWORKS ASSESSMENT COSTS

To monitor fraudulent transactions on payment card networks.

CREDIT MONITORING COSTS

Cost of independent credit review to reduce the chance of identity theft.

FINES COSTS

Regulatory fines and penalties.

LEGAL COSTS

To defend against class action or other suits and costs spent on public relations.

PAYMENT CARD FRAUD LOSSES

To indemnify affected cardholders, losses resulting from fraudulent transactions.

FORENSIC COSTS

To determine cause of breach.

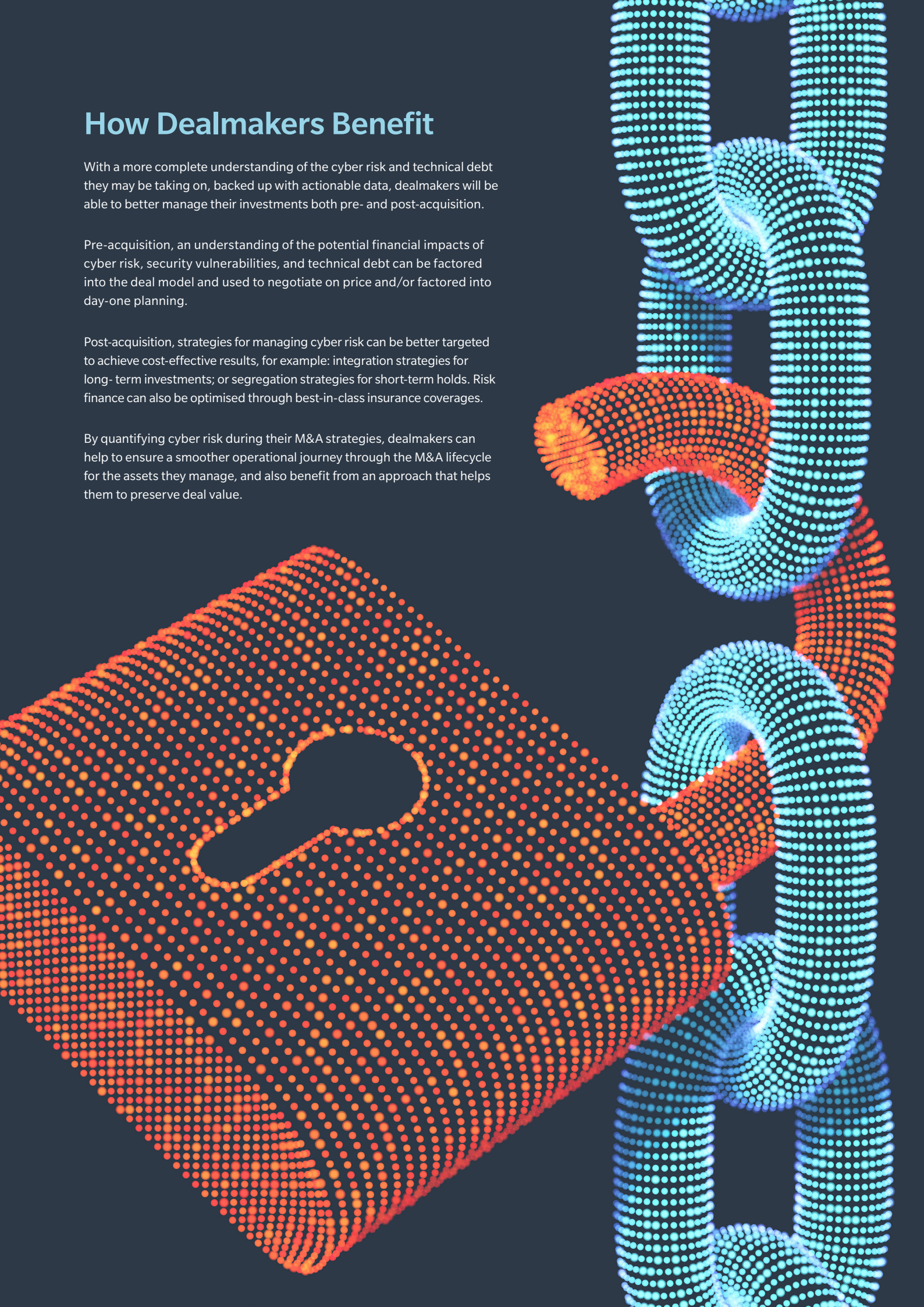
How Dealmakers Benefit

With a more complete understanding of the cyber risk and technical debt they may be taking on, backed up with actionable data, dealmakers will be able to better manage their investments both pre- and post-acquisition.

Pre-acquisition, an understanding of the potential financial impacts of cyber risk, security vulnerabilities, and technical debt can be factored into the deal model and used to negotiate on price and/or factored into day-one planning.

Post-acquisition, strategies for managing cyber risk can be better targeted to achieve cost-effective results, for example: integration strategies for long- term investments; or segregation strategies for short-term holds. Risk finance can also be optimised through best-in-class insurance coverages.

By quantifying cyber risk during their M&A strategies, dealmakers can help to ensure a smoother operational journey through the M&A lifecycle for the assets they manage, and also benefit from an approach that helps them to preserve deal value.



For more information on how we can help manage cyber risk for your M&A transactions and portfolio assets please contact:

CAL MCGUIRE
Vice President, Consulting Solutions
Marsh Advisory
+44 (0)79 3933 9015
cal.mcguire@marsh.com

JAMES WHITE
Head of UK Transaction Advisory
Private Equity and M&A Practice
+44 (0)207 357 5229
james.white@marsh.com

Insurance Brokers
Chartered