For M&A professionals, quantifying cyber risk is key

Chris Harner, FRM
Lisa Henderson

Milliman

The *Wall Street Journal* reported that cybersecurity due diligence is a growing factor in mergers and acquisitions (M&A) deals.[1] Over the past 15 years, cyber risk has evolved from a nuisance some businesses hoped to ignore to an imposing and often unpredictable risk with the potential to cause tremendous harm. The September 2017 breach of the consumer credit reporting agency Equifax is a case in point, affecting more than 143 million consumers. As cyberattacks occur with increasing severity and frequency, cyber risk has moved to the top of many organizations' non-financial risk concerns.

The evolution of cyber M&A due diligence

In the financial services and insurance industries, many of the practical details surrounding M&A transactions are based on reasonably sound approaches with sufficient supporting data. Advisers leading buy-side due diligence teams understand what they have to value and whether it's positive or negative: revenue, client base, distribution channels, physical assets, and so forth. Within reasonable parameters, they can estimate the value of a target entity.

What is more challenging to quantify is the impact a cyber event may have on the value of the target. In the past, companies have used systemic labeling metrics such as red/yellow/green or one-through-five indicators to rate cyber risk. As cyber events have increased in scope and complexity, investors are requiring that the quantification of a target's cyber exposure be part of their due diligence. Yet with cyber risk, the unknowns are many and the impacts can be severe. Due diligence efforts may uncover, for example, holes in a target's cyber risk management as it relates to third-party vendors or a target's failure to conform with legal cybersecurity regulatory compliance.[2] Those results, however, must then be translated into predictable costs and benefits to use as the basis for determining a reasonable acquisition price.

Cyber vulnerabilities bear two separate but equally important risks: the obvious risk to the business of financial losses and reputational harm. Look at the impact, for example, of the Yahoo! breach on its acquisition by Verizon in 2017. Details of that breach became public during acquisition discussions and quickly led to a $350 million drop in Yahoo!'s purchase price, down to $4.48 billion, and other drastic changes in the terms and structure of the finalized deal.[3] As with any company affected by breaches, Yahoo! inevitably took a reputational hit, too. Quantifying that kind of fallout from both potential and actual breaches into a single figure is not easy.

As another example, if a company were looking to buy retailer Target prior to its breach, it would have wanted to attach some kind of value to that potential liability and then account for it in the purchase price negotiations. This includes assessing potential liability not only of the target company, but also the exposure from third-party vendor relationships which led to the breach. How do you avoid buying something with a $500 million liability instead of a $50 million liability? The stakes are high for the potential investor as can be seen in the examples of Yahoo! and Target.

1 Nash, K.S. & Minaya, E. (March 5, 2018). Due diligence on cybersecurity becomes bigger factor in M&A. Wall Street Journal. Retrieved March 27. 2018, from https://www.wsj.com/articles/companies-sharpen-cyber-due-diligence-as-m-a-activity-revs-up-1520226061.

2 Trope, Roland and Tom Smedinghoff (ABA 2017). The Importance of Cybersecurity Due Diligence. Retrieved April 13, 2018, from https://www.americanbar.org/groups/business_law/publications/blt/2017/09/04_trope.html.

3 Lunden, I. (February 21, 2017). After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B. TechCrunch. Retrieved March 27, 2018, from https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/.

Strategic approaches to valuation

This quantifying of a target company's cyber risk is a problem that might be best thought of in the same way actuaries in insurance companies think about reserving. An actuary working for an investor will compare the target's booked reserves to a best estimate of the unpaid claims liability of the target. However, the actuary owes it to the investor to also describe the variability—the uncertainty—of those reserve estimates.

Take two contrasting examples. If the target company writes property insurance, the expected payout of all future claim payments will be relatively short, so the uncertainty factor will, correspondingly, be relatively small. However, if the target company writes long-tailed workers' compensation insurance, where the expected payout can be 30, 40, or 50 years or longer, a very reasonable uncertainty factor can be considerably large and, thus, significant in the purchase price negotiations .

In a similar way, the uncertainty of the cost of a cyber event can also be significant. And it can change on a dime. Imagine that an investor acquires a business. The acquiring company's stock gets a nice bump. But then, one month later, after the deal has closed, the acquired entity discovers it was a victim of a cyber breach which occurred months before the deal closed. It wasn't caught, it wasn't calculated into the deal—or maybe it was to some degree, but insufficiently—and now suddenly the acquiring company is facing unplanned for exposure. Assessing and quantifying the potential for cyberattacks calls for placing a valuation on the various reputational and financial risks that could befall an acquiring company due to a cyber event: from a drop in market value, to client loss, legal action, or a change in C-suite or other senior management. While some of these risks are manageable and can be overcome, a large breach might lead to a change in the business model or financial peril if the exposure is not assessed properly.

Assessing and quantifying cyber risk

When it comes to M&A transactions, investors are often already making use of security-type firms that can offer forensic views into the plumbing and wiring of a target company's cyber exposure. These third-party firms often provide checklists of actions that would need to be taken to mitigate a target's cyber risk. There is an absolute place in the market for these firms, and it's likely that most investors now bring them on board as a matter of routine.

However, the critical piece that remains missing is how to quantify those risks in order to provide a better valuation of the target and overall risk profile of the transaction. A deeper understanding of cyber risk would enhance the negotiations between the buyer and the seller. Quantifying cyber exposure should begin with a methodology to capture and evaluate a company's security posture, vulnerabilities, threat vectors, compromised assets, and impacts of a cyber event or events. The model then allows for scenario development to determine the frequency and severity of an event. Running thousands of iterations allows for creating a continuous distribution of loss outcomes and quantifying the potential range of cyber risk costs, including expected loss, tail loss, and the volatility around these losses. Lastly, the model should allow for management actions such as what happens with increases or decreases in specific areas of IT spend or insurance coverage.

Such a tool would allow investment bankers, risk managers, and cyber experts to better understand some of the more challenging questions in M&A transactions. If the expected loss occurred, for example, how would the target's current insurance coverage respond? Are there gaps that need to be considered? What do they look like? What if, rather than the expected loss, a more extreme event (tail loss or worst-case scenario) materialized? The insight gained would be invaluable to the acquiring company regarding the target's risk profile, potential management actions, strategic planning, and resource allocation.

A significant benefit of a cyber risk assessment during M&A due diligence is that it presents the broadest view of how to value the cyber risk of a target company, while at the same time taking into account that company's current insurance protections. Whether the acquiring company intends to make allowances for any potential gaps with additional insurance, carve-outs, escrow, reserves, or other options, solutions exist to help put a number on the risk in the first place. Overlaying the results with a company's insurance coverage can help identify gaps in coverage and determine how much uncertainty is or is not already understood.

Informed assessment of the cost of cyber risk greatly assists the investor in determining the potential net increase in its own risk profile, allowing the company to more accurately determine whether a target may exceed the acquiring company's formal risk appetite parameters. The more capable a buyer is in measuring all risk, the greater advantage it has during M&A negotiations.

The investor will often take the extensive financial information it is given about the target and then outsource that information to third-party firms hired specifically to help value targets appropriately. There's a clear approach and a clear process, there's data, and there are traditional methods used to get at appropriate valuations.

Cyber exposure by contrast is uncharted territory. It is new, growing, and represents a daunting array of potentially very expensive risks within a context of mostly unknown factors. These days, if a company cannot determine a plausible estimation of cyber risk, the valuation of the target is incomplete, and the investor is lacking a full picture of the risks inherent in the potential deal.

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Chris Harner,FRM
chris.harner@milliman.com

Lisa Henderson
lisa.henderson@milliman.com