AlixPartners

JUNE 2019

HOW CYBERSECURITY RISK IS DISRUPTING THE M&A LANDSCAPE…

And how investors are fighting back

Private equity and corporate investors continue to deploy capital at record rates, with investment volumes in 2018 surpassing pre-financial crisis levels for the first time.[1] But, as private equity acquires new companies, their exposure to cybersecurity risk is also reaching new heights.

Investors are struggling to appropriately assess these risks when making new investments, given:

- Increasingly complex privacy and data breach rules around the world
- Growth in the volume and complexity of cyber-attacks
- Unavailability of relevant information on security and privacy practices
- Lack of expertise needed to identify critical issues and quantify cyber risk

1. Preqin Quarterly Update: Private Equity & Venture Capital, Q1 2019

RISK HEAVY

Despite all of the attention that's been focused on this issue, cyberattacks are becoming more common, often with much greater impact. Undiscovered exposures and untreated vulnerabilities can lead to a data breach or can halt operations, damaging the value of an investment. And the indirect costs through lasting damage to the brand and to customer relationships can be even more devastating. The potential financial impact has also increased as new regulations have been implemented to protect consumers that have far-reaching, worldwide implications, with the potential to impose substantial fines.

As one example, Marriott International disclosed late last year that it had uncovered a data breach at its Starwood Hotels and Resorts subsidiary, which it had acquired in 2016. The personal data of as many as 500 million guests were exposed. Analysts estimate that Marriott could face up to $1 billion in fines and other costs associated with this breach, which includes a potential $450 million in fines solely from violations to the European General Data Protections Regulations.[2]

Another example is Equifax, the credit monitoring giant that fell victim to a 2017 cyber-attack that exposed some 147 million people's data. In addition to reputational damage, the high-profile breach has had a material financial impact on the company; so much so that Moody's lowered their credit outlook from stable to negative, the first time a cyber incident was cited as a reason for a downgrade. In the first quarter of 2019 Equifax took a $690 million charge, with infrastructure and remediation expenses expected to be $400 million per year for the next couple of years.[3]

These increased costs, which are a direct result of insufficient cybersecurity protections, are beginning to change the calculus when assessing a potential target company for investment.

INFORMATION LIGHT

With increased competition amongst investors, private equity firms are also frequently asked to make their investment decisions on compressed timelines, with limited due diligence. M&A deals are inherently complicated as it is, with cybersecurity risks adding an additional layer to that complexity. Investors need a consistent, yet comprehensive approach ready to implement in each of these situations to understand existing shortcomings and the investment required to reduce the risk of a cyber incident.

As the global economy slows and financial pressure on companies increases, the risks that cyber vulnerabilities go untreated and unreported also increases. Security often takes a backseat as executives devote their attention to the most important task: avoiding financial crisis. Security measures and precautions take a lower priority, and investments in these areas are frequently curtailed to cut costs.

As a result, as we've seen frequently in the news, vulnerabilities may go unpatched and new threats unaddressed, increasing the risk of a security incident and exposure of confidential company and personal data or an interruption of business operations. Breaches can go unnoticed for long periods of time - on average 197 days[4] – which if not detected could derail a deal or investment after closing.

2. https://www.bloomberg.com/news/articles/2018-12-14/marriott-cyber-breach-shows-industry-s-hospitality-to-hackers
3. https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html
4. https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

A CHANGING LANDSCAPE

Investors calibrate their financing terms based on anticipated growth and profit, tempered by perceived risks that could impact performance. Cybersecurity issues present a risk on multiple fronts, yet many have struggled to properly quantify the impact and historically have simply grouped it in with general IT transition costs. This generalization is beginning to prove costly and shortsighted.

As today's companies evolve and continue to incorporate technology as a fundamental component embedded in business operations, cyber risk grows increasingly pervasive.

As this continues to add uncertainty to M&A deals, leading investors have been quick to bolster their due diligence efforts to incorporate cybersecurity as a core component alongside financial, legal, ESG, and other traditional dimensions.

Cyber risk covers more than just protecting data from being stolen.

Technology's unrelenting pace often leaves companies scrambling just to keep up with competitors. The perceived need for speed usually leaves rigorous processes for securing technology development, integration, and third-party risk as an afterthought.

In today's digital economy, companies not traditionally thought of as technology-focused, such as shipping companies and manufacturers, have seen their businesses crippled by ransomware. Even digitally-native companies may not be prepared to react when a crucial service goes down or they find themselves the victim of a denial of service attack, which could prevent them from capturing revenue.

TOWARDS A SYSTEMATIC APPROACH

Private equity investors have taken many different approaches to accounting for cybersecurity risks revealed during M&A transactions.

While these approaches differ between firms, and often even between industry or regional teams within firms, they typically consider, if sometimes only informally, such factors as the size of the investment, their reliance on technology, the frequency with which the industry is targeted by attackers, the locations where business is conducted and data is stored, and the complexity of post-merger integration when such strategies are at play.

With so much at stake, these concerns have become acknowledged as a universal threat to the investment community, industry groups are stepping forward to help facilitate discussion around this topic, giving greater visibility and highlighting the importance to the business community and financial system. For example, last year, the World Economic Forum established their Centre for Cybersecurity, which focuses on initiatives to address the needs of investors and the global financial community.[5]

Also, at the request of a number of its members, the European American Chamber of Commerce has hosted a panel specifically focused on cybersecurity complexities on cross-border M&A transactions.[6]

5. https://www.weforum.org/agenda/2019/03/4-ways-to-cyberproof-your-business-during-m-a/
6. https://www.eaccny.com/events/?event_id=589

Over time, as a community, investors should be able to find common answers to some of the difficult cybersecurity questions that they face, such as:

What types of investments warrant a deeper cyber review?	What are the risks of integrating two portfolio companies?	How do you monitor cyber risks across a portfolio of investments and when should action be taken?
How do you incentivize portfolio companies to mitigate critical cyber risk and align their interests with those of investors?	What level of expense is realistically expected to bolster existing cyber protections?	Does our model adequately capture underlying risk from cyber exposure?

LOOKING FORWARD

M&A has always been a complicated endeavor, with investors looking for a competitive edge in pursuit of the best returns on their capital. Evaluating and compensating for uncertainty is a core function of financing many of these deals, and private equity is no stranger to taking on such risk. But with the current pace of technological change, the type and scope of risk taking has begun to take a new form.

Many firms are feeling left behind, as they only now are beginning to take this into account. Ideally, as executives begin recognizing cybersecurity as a core component of their due diligence framework and allocate resources accordingly, investors can get back to doing what they do best: making large bets on the future earning potential of a great business.

AlixPartners

CONTACT THE AUTHORS:

Gretchen Ruck
Director, Cybersecurity Practice Leader
+1 646 428 9185
gruck@alixpartners.com

Kevin Madura
Vice President, Cybersecurity Practice
+1 202 756 9068
kmadura@alixpartners.com

ABOUT US

For nearly forty years, AlixPartners has helped businesses around the world respond quickly and decisively to their most critical challenges – circumstances as diverse as urgent performance improvement, accelerated transformation, complex restructuring and risk mitigation.

These are the moments when everything is on the line – a sudden shift in the market, an unexpected performance decline, a time-sensitive deal, a fork-in-the-road decision. But it's not what we do that makes a difference, it's how we do it.

Tackling situations when time is of the essence is part of our DNA – so we adopt an action-oriented approach at all times. We work in small, highly qualified teams with specific industry and functional expertise, and we operate at pace, moving quickly from analysis to implementation. We stand shoulder to shoulder with our clients until the job is done, and only measure our success in terms of the results we deliver.

Our approach enables us to help our clients confront and overcome truly future-defining challenges. We partner with you to make the right decisions and take the right actions. And we are right by your side. When it really matters.