Grant Thornton

An instinct for growth™

Cyber due diligence

Protecting M&A value

Introduction

Data vulnerabilities can seriously threaten the value of a business. As the cyber-risks facing organisations intensify, cybersecurity is becoming a critical part of the due diligence process for M&As.

Buyers beware

In August 2017, a US court handed down a ruling that confirmed Verizon's worst fears. A judge decided that its subsidiary Yahoo! would face litigation from more than a billion account holders.

The claimants say their personal information was compromised in successive cyber-attacks on Yahoo! – which went completely undetected at the time. Verizon became liable for these breaches when it purchased Yahoo! in June.

As Verizon's predicament shows, data has become a whole new risk area for M&A.

When you buy a company, you buy its data. And you take responsibility for its data security – past, present and future.

That can mean inheriting its cyber failings, which can have a significant impact on its value. Yahoo!'s misfortunes reduced the price paid by Verizon to the tune of $350 million.

The onus is now on an acquiring business to assure that the value of the data they're taking ownership of is maintained and protected. From private equity firms with portfolios of potentially vulnerable acquisitions, to high-growth start-ups looking for a buyer, the M&A community can no longer neglect cybersecurity due diligence.

So, how can cyber due diligence help M&A practitioners to safeguard the value of an acquired business?

"The onus is on acquiring businesses to assure the integrity of the data they're taking ownership of. The M&A community can no longer neglect cybersecurity due diligence."

The corporate cyber threat

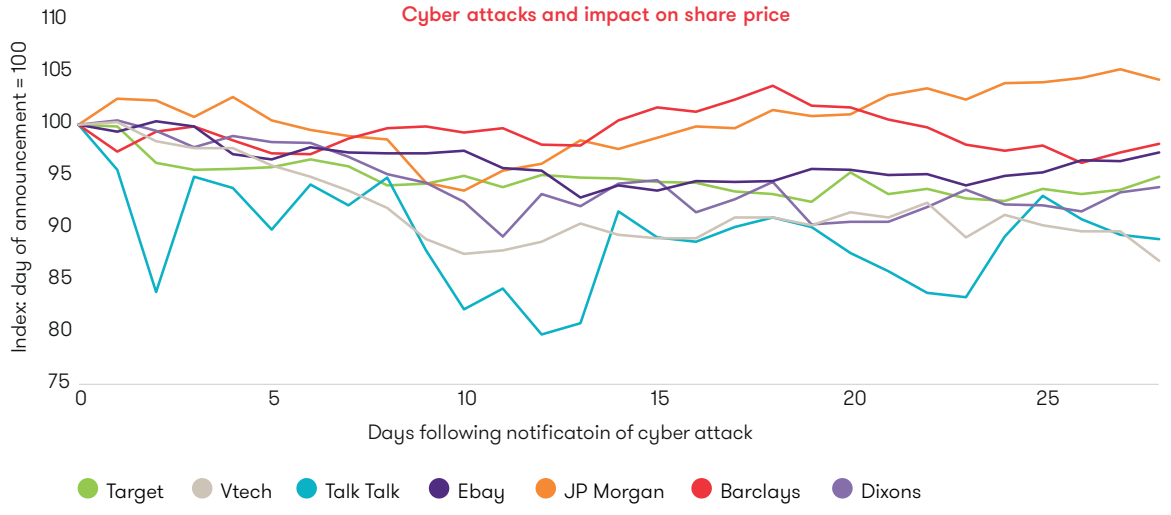
The scale and nature of the corporate cybercrime threat has grown increasingly alarming over the past few years. Alleged state-sponsored attacks, organised hacktivism, leaked entertainment content and global ransomware attacks are becoming all too commonplace.

And the danger is as acute as it is enormous. As corporate IT systems grow and evolve the 'attack surface' grows, presenting new vulnerabilities to be exploited. Cyber criminals have often weaponised exploits within days or weeks of discovering the vulnerability, yet breaches take some 191 days on average to detect, and a further 66 days to contain once discovered.

The financial impact of a cyber-attack can be huge. A breach costs the targeted organisation some £2.4 million on average, with each record stolen setting it back £126[1]. That's a sobering thought when hackers can access more than a billion accounts at Yahoo! without detection.

Given the scale of the damage cyber-attacks can do, it can take weeks or months for a listed company's market cap to recover (see graph).

The costs of a breach are about to become even more acute. The EU's General Data Protection Regulation (GDPR) comes into force in May 2018, ushering in potentially enormous fines: up to €20 million, or 4% of global turnover (whichever's higher).



Source: Capital IQ, analysis by Grant Thornton UK LLP.

"Data is the lifeblood of today's organisations. And in many cases, it is also their intellectual property."

[1] 2017 Cost of Data Breach Study, Ponemon Institute, 2017

The case for cyber due diligence

Data is the lifeblood of today's organisations. For many firms – like Yahoo! – data is also their intellectual property (IP). Their customer, subscriber or membership base is their commercial offering; it's where the business value lies.

A cyber-breach is therefore a major operational risk. It can affect a company's value in a number of ways:

- it can result in IP theft
- it can cause significant business interruption if systems go down under attack from hackers
- revenues will be lost: customers will vote with their feet, and those that remain will do less business with you, as their trust in your brand will be damaged
- there are direct costs of dealing with the incident: remedial action, customer notifications, PR, investigations, system improvements, potential legal claims
- there are longer-term costs, as raising finance and securing specialist cyber-insurance become more expensive

Despite these risks, M&A practitioners have been routinely overlooking cybersecurity when valuing and buying companies.

A report from law firm Freshfields Bruckhaus Deringer found that as of 2014, almost four in five dealmakers weren't testing cybersecurity as part of their due diligence process[2].

To some extent, this reflects their capabilities. Few M&A professionals' technical skills will extend to cybersecurity. They're adept at poring over the financial and legal aspects of due diligence, and even the IT landscape of a target firm. But cybersecurity is a highly specialist domain.

In the digital era, however, cyber due diligence needs to be part of every transaction.

It's a reality that the M&A community seems to be waking up to. According to a 2016 study by consultancy West Monroe, 80% of practitioners consider cyber due diligence to be 'highly important'[3].

80% of practitioners now consider cyber due diligence to be highly important.

[2] Cybersecurity in M&A, Freshfields Bruckhaus Deringer, 2014
[3] Testing the Defenses: Cybersecurity Due Diligence in M&A, West Monroe, 2016

Best practice

Cyber due diligence is the M&A professional's first line of defence against hackers decimating the value of a target business.

The cyber due diligence process consists of a comprehensive audit of the governance, procedures and controls that an organisation uses to keep its information assets safe.

An effective cyber due diligence exercise should therefore involve the following four measures:

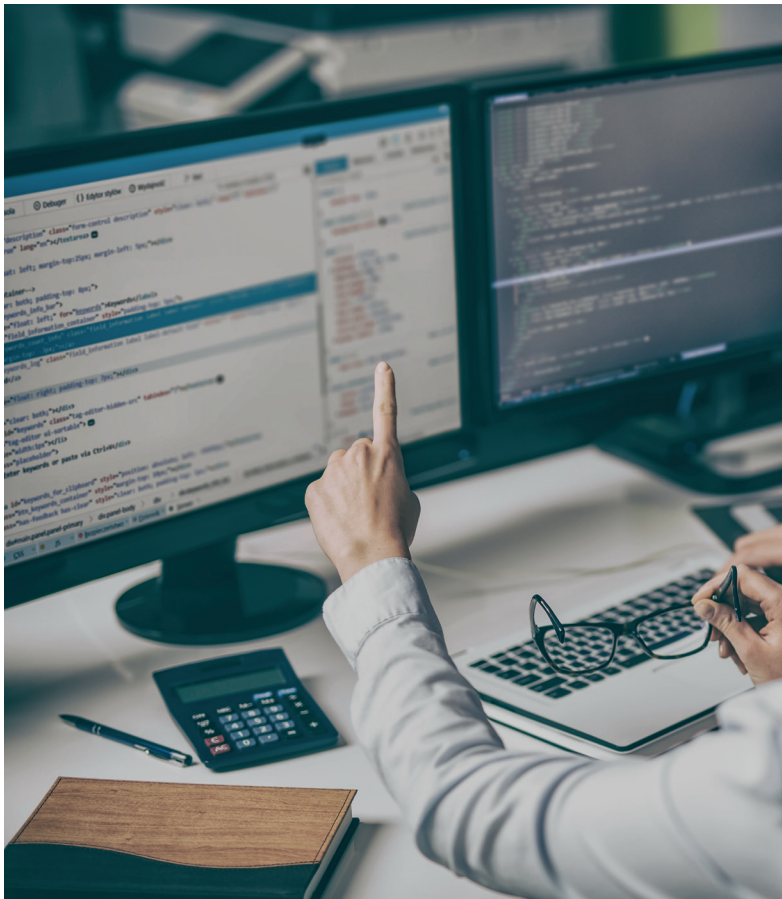
1. a review of the target firm's:
   - data protection measures – to identify any vulnerabilities that need addressing before the transaction goes through
   - breach management, disaster recovery and business continuity plans
   - compliance with industry-specific data regulation – for example, FCA risk management standards in financial services; PCI DSS standards for credit card handing in retail; OfCom regulations for telco providers; etc.
2. penetration testing of the target firm's cyber-defences, and potentially those of its suppliers
3. a dark web search for signs of a breach – for instance, elements of the target firm's IP, or customer or client personal data being offered for sale
4. a valuation of the target firm's information assets

Cyber due diligence therefore offers some important benefits. Properly executed by expert assessors, it will help acquiring businesses to identify any cybersecurity risks and vulnerabilities in a target entity. And it should bring to light any previous breaches that the target firm may have suffered without realising.

As such, it will evaluate the likely costs of a past or potential breach. And it will reduce the risk of future breaches and liabilities, helping to avoid fines, litigation, brand damage, loss of customers, and so on.

Ultimately, it will enable the correct valuation of the target's information assets – leading to a more accurate assessment of the value of the business as a whole. And most of all, it will help you to preserve that value in the future.

"Cyber due diligence helps to accurately evaluate a target firm's information assets – and therefore the business as a whole. And it will help you to preserve that value in the future."



Key considerations

Close scrutiny of any organisation is bound to affect its culture, values and morale – and therefore its performance.

As with any due diligence exercise, cyber due diligence can have unintended consequences if not handled in the right way:

- auditing a firm's cybersecurity arrangements can be enough to make people more cyber-aware. This may give the impression of a business that's more secure than it really is.
- being assessed will also have an impact on morale among the cybersecurity team. It may make them nervous, or fearful that they're being measured because they're not up to the job. That could prompt people to give the answers they think the assessors want, again creating a 'rose-tinted glasses' effect.
- low morale may also hit the team's performance, leaving the company more exposed in the run-up to the transaction. Or worse, it might stoke resentment and provoke malicious behaviour.
- the cyber due diligence process could even lead to rumours of the forthcoming merger, acquisition or investment – with the potential to reduce value, or derail the deal altogether.

Buyers need to keep an eye out for such upheaval while carrying out cyber due diligence. For example, by monitoring what's being said about the target company on social media while the process is happening.

Having an objective third party carry out your cyber due diligence is a way to ease some of the negative effects.

Conducting a cyber due diligence exercise undoubtedly adds to the cost, complexity and workload involved in preparing for a transaction.

But given the risks of a breach, and the damage it can do to the value of a business, cyber due diligence is critical to maintaining the value and integrity of a newly acquired entity.

"Cyber due diligence can have unintended consequences. Using a third party helps to keep these to a minimum."

Contact us

To discuss your cyber due diligence needs, please contact:

Vijay Rathour
Head of Digital
Forensics Group,
Forensic and Investigations Services
T +44 (0)20 7184 4684
E vijay.rathour@uk.gt.com

Manu Sharma
Head of Cyber Security,
Financial Services,
Business Risk Services
T +44 (0)20 7865 2406
E manu.sharma@uk.gt.com

Kev Brear
Head of Resilience Services,
Financial Services,
Business Risk Services
T +44 (0)20 7865 2425
E kev.brear@uk.gt.com

Mike Thornton
Head of Valuations,
Corporate Finance
T +44 (0)20 7728 2644
E michael.j.thornton@uk.gt.com

Grant Thornton

An instinct for growth™

grantthornton.co.uk

GRT106984