Freshfields Bruckhaus Deringer

Cyber security in M&A

Cyber security in M&A	5
Due diligence in the spotlight	7
Five steps to effective cyber security due diligence	10
Deals under threat	11
Behaviour is changing – but is it changing enough?	13
Panel – When Target became a target	14
Sectors under attack	15
Contact us	16

Cyber security in M&A

A survey of global deal-makers by Freshfields Bruckhaus Deringer reveals a growing awareness of the cyber threat. But it also shows respondents are yet to evaluate it in the same way as other risks that can undermine corporate value.

Cyber attacks are a growing risk to businesses across the world. A breach by hacktivists, state-sponsored agents, organised crime cartels or company insiders has the potential to disrupt operations, damage brands and erode corporate value.

The British government has been working with businesses to raise awareness of the threat and share information on attacks in real time. New EU laws on data protection threaten fines of between 2 and 5 per cent of global revenues if companies lose customer data while regulators, including the SEC, now compel businesses to disclose any data breaches that could affect investor decisions.

A growing complacency

With this concerted action and a series of high-profile strikes on businesses including eBay, Target and Yahoo!, the risks of cyber attack are evident. Yet as the global economy recovers and deal activity rises, research from Freshfields Bruckhaus Deringer reveals that increasing awareness of cyber risk has not resulted in meaningful changes to the M&A process.

Freshfields surveyed 214 global deal-makers from corporates, financial institutions, investors and legal services providers (63 per cent from North America, 34 per cent from Europe and 3 per cent from the rest of the world) on their awareness of cyber risk and how it affects their working practices. The results show that 78 per cent of respondents believe cyber security is not analysed in great depth or specifically quantified as part of the M&A due diligence process, despite 83 per cent saying they believe a deal could be abandoned if previous cyber security breaches were identified and 90 per cent saying such breaches could reduce the value of a deal.

Other findings include:

- 74 per cent of acquirers and 60 per cent of sellers involved in an M&A transaction are likely to be concerned about cyber security issues derailing their deal
- 58 per cent of respondents believe the risk of cyber attacks or incidents has changed the deal process in the last 12 months and 82 per cent believe they will change the process in the next 18 months
- 87 per cent say the use of technological security has grown over the last 12 months as awareness of cyber risks rises
- 52 per cent believe cyber risk training for teams involved in deal-making will become a part of the process during the next 18 months
- Defence and financial services are identified as the two sectors likely to be most affected by a cyber incident during an M&A deal

Due diligence in the *spotlight*

78 per cent of global respondents believe cyber security is not analysed in great depth or specifically quantified as part of the M&A due diligence process, despite 83 per cent saying they believe a deal could be abandoned if previous breaches were identified and 90 per cent saying such breaches could reduce the value of the deal.

Cyber security in the M&A process is about more than just keeping sensitive data safe. Acquirers must assess whether their target carries an acceptable level of cyber risk in the same way they would analyse its financial position. A thorough knowledge of a business's cyber security is equally important during the integration phase; as a former deputy assistant attorney general at the US Department of Justice who supervised cyber crime investigations has said: 'when you buy a company, you're buying its data – and you could be buying its data security problems'.

Deal-makers look back, not forward

A majority (87 per cent) of respondents to the Freshfields survey say cyber security due diligence is typically included within an overall review of a company's IT systems, but not treated as a risk category in its own right. And while 71 per cent say cyber security due diligence experts are starting to get involved in transactions worth more than $500m, 66 per cent say cyber risks are 'very difficult' to quantify given the time pressures involved. Almost three-quarters (73 per cent) say due diligence questionnaires tend to be more concerned with historic breaches than future threats, while just 39 per cent say they make cyber security policies (including a current insurance policy and a clear set of employee guidelines) a condition precedent that is addressed prior to completion.

Europe lags behind the US

More North American respondents (51 per cent) than European (39 per cent) have seen cyber security become a key part of due diligence in the last year. The US has also seen more suppliers and counterparties audited (38 per cent to 22 per cent), more internal cyber security specialists appointed (33 per cent to 17 per cent) and more external cyber security consultants engaged to review risks (28 per cent to 17 per cent). Slightly more than half (57 per cent) of global respondents expect cyber security due diligence to become more important in the next 18 months.

Commenting on results of the survey, Freshfields' IP/IT partner Chris Forsyth, says: 'It's surprising that deal-makers recognise the growing threat of cyber attacks to businesses but generally aren't addressing that risk during deals. You wouldn't dream of buying a chemicals plant without assessing environmental risk, so why would you buy a data-driven business without assessing the risks it faces around data management and cyber security?'.

'The effect of a cyber incident on value would work both ways – a business with a good track record and robust processes could be worth more than competitors, while a business with a bad track record could be worth less. It is odd that most respondents to the survey said they were concerned about cyber security risks but that most respondents aren't actually doing anything about them during an M&A process. One possible explanation is that it is a relatively new area that is not well understood and buyers are hesitant about how to tackle it.'

A worrying lack of understanding

Edward Braham, Freshfields' global head of corporate, adds: 'The message to deal-makers – whether buyer or seller – is to evaluate cyber risk in the same way they would any other risk that could affect the value of a target. Cyber risk presents a significant threat to the operations, reputation and the bottom line of virtually every company, regardless of industry. While market practice is still developing in this area, buyers can use an M&A process to understand better the cyber risk a target faces.'

On the difference between North American and European responses, Jane Jenkins, co-head of Freshfields' international cyber security and defence teams, says: 'Differences in cultural attitudes and the perception of cyber risk may be reflective of the varying levels of exposure to follow-on litigation and class actions in the US compared with Europe. While the environment is starting to change, there is still much more emphasis on transparency in the US than in Europe, with the SEC threatening enforcement action against companies for failure to notify cyber breaches.'

Five steps to effective cyber security due diligence

Data-management risk

An effective due diligence process would analyse what data the company holds and where it gets that data from. It would be important to quantify how valuable the data was to the business and then to focus on how the company protects and exploits it.

Technical risk

If valuable data is used in an internet environment, a forensic IT services provider could assess how it is encrypted and what firewalls and other systems are deployed to keep it safe. As any business is only as secure as its third-party suppliers, these systems would also need to be analysed.

Corporate risk

A company's contracts with its third-party suppliers would need to be audited to ascertain how they purport to protect any valuable data assets. Are they sufficiently robust to protect that data and by extension the value of the business and its brand?

Employee risk

Effective cyber security is about more than just expensive and complex technical systems. Human behaviour is a bigger risk to data security than even the most sophisticated hacker. It is vital to assess what processes a business has in place to protect its data and how these are reflected in its employment contracts.

Track record

Another factor to consider is whether a business has suffered a data breach in the past and if so, where that breach originated from. An assessment could then be made of how the company dealt with the breach and what procedures were put in place to guard against a repeat.

Deals under **threat**

74 per cent of respondents say acquirers are either very or slightly concerned and 60 per cent say sellers are either very or slightly concerned about cyber security issues derailing their transaction.

The survey reveals a higher level of concern in North America than Europe that a deal could be derailed by a cyber security issue (88 per cent to 76 per cent). Of greatest concern to acquirers globally when negotiating terms is whether a target has suffered a previous cyber theft of data or IP (which 91 per cent of respondents rank as a very important or important factor), and whether a target becomes the victim of a cyber attack during deal discussions (90 per cent very important or important). Evidence of a business not handling a past breach effectively or being disrupted by a historic DDOS attack was deemed important or very important by 87 and 82 per cent, respectively.

A threat to the bottom line

Almost two-thirds (64 per cent) said a cyber incident mid-deal, or the identification of past data breaches during due diligence, could have an impact on the transaction. The most likely consequences are warranty claims (59 per cent of global respondents said this was either likely or very likely), a change of deal terms (55 per cent), or a reduction of deal value (45 per cent).

The century of data

That respondents say more acquirers than sellers are likely to be concerned about cyber security issues derailing a transaction could be explained by what they have to lose. Ginni Rometty, CEO of IBM, said earlier this year that if the 20th century was all about oil then the 21st century would be all about data. Some of the world's most valuable businesses are data-driven and more data has been generated in the last two years than in the rest of history combined. When acquirers are scoping out targets whose price is predicated on data, they need to know their investment is safe. But sellers must also make appropriate disclosures if their cyber security plans are inadequate or they have been the victims of an attack.

Chris Forsyth says: 'Acquirers are concerned because of the risk they're buying something that's overvalued. We're in a mini dotcom boom where huge sums are being paid for internet data and customer-relations type businesses and acquirers are wondering how fragile that value is.'

'Investors and corporates are starting to wake up to cyber risk. More companies are being penalised by shareholders for being a victim of an attack and executives are having to step down as a result. It is no surprise that sales of cyber insurance are surging and that companies are increasing their spend on internet security. Buyers can be expected to ask more penetrating questions than previously and sellers will want to think about cyber risk in much more detail than before.'

Behaviour is changing – but is it changing enough?

87 per cent have seen increased use of technological security in the last 12 months. 58 per cent say the risk of cyber attacks or incidents has changed the deal process in the last 12 months and 82 per cent say they expect further change in the next 18 months.

While the high proportion of respondents noting an increase in technological security shows the threat is being taken more seriously, better and more expensive technology doesn't necessarily make businesses more secure.

A key theme of the UK government's efforts to make Britain 'one of the most secure places in the world to do business in cyberspace' is to take cyber security out of IT and into the boardroom – and embed the idea that dealing with the threat is as much about people and processes as it is about technology. Edward Snowden's revelations have shown that employees are a greater risk to data security than even the most sophisticated hacker, but sensitive information can just as easily be lost unintentionally through poor cyber security processes. Any technological precaution can be undermined by a single rogue, careless or ill-informed employee.

Focus on technology

The most common changes noticed during the deal process in the last year include the increasing use of technological security on phones, laptops and in virtual deal-rooms (89 per cent in Europe, 95 per cent in North America) and training for deal teams on cyber risk (33 per cent Europe; 31 per cent North America). An analysis of what's expected over the next 18 months reveals that while a high proportion (82 per cent) of global respondents believe the M&A process will change, most see this being technological (85 per cent).

Room for improvement

Typical security procedures always seen during a transaction to protect information include the use of online data rooms (65 per cent Europe; 57 per cent US) and project passwords (63 per cent in both territories). But use of the most advanced security procedure, biometric identification, is always or occasionally seen by just 30 and 28 per cent of European and North American respondents, respectively.

Supply chain risk

The respondents say law firms are the most likely deal advisers to use some form of specific security procedure to protect documents made available online during a transaction (86 per cent of respondents), followed by financial advisers (83 per cent) and accountants (74 per cent). Bottom of the list are financial PR firms, of which 42 per cent of respondents believe have no deal-specific security procedures in place.

Chris Forsyth says: 'More of our clients are asking us for our cyber security credentials when we pitch for M&A work. Good cyber governance has to flow through the supply chain. And technical solutions represent less than half of what would be seen as an effective response to cyber risk.'

When Target became a target

The potential of a cyber attack to wreak havoc on a business was evident last year when US retailer, Target, revealed a huge data breach in which 40m of its customer accounts were hacked and the personal details of a further 70m shoppers stolen. Target's shares fell 2.2 per cent after it disclosed details of the attack and a further 1.2 per cent when it admitted that the breach had hit sales.

Between January 2013 and January 2014, Target's customer traffic fell 23 per cent, according to figures from Kantar Retail. The breach highlighted the issue of third-party vulnerability, beginning as it did when hackers stole the network login details of a heating and air conditioning contractor. This information was used to insert malware into point-of-sale systems and harvest customer data.

Sectors under *attack*

Defence and financial services are identified as the two sectors likely to be most affected by a cyber incident during a deal.

Recent analysis of filings to the Securities and Exchange Commission (the SEC) paints a sobering picture of the cyber threat. The number of annual reports that mention cyber security more than doubled from 519 in the 12 months to May 2012 to 1,174 just two years later. While it's true that the SEC has been putting pressure on companies to report data breaches, the scale of the problem appears to be growing.

The number of commercial banking reports mentioning cyber security issues more than doubled between 2012 and 2014 (from 36 to 81), while in the 18 months from mid-2012 to 2014, distributed denial of service (DDOS) attacks were launched against the consumer websites of financial institutions including Charles Schwab, American Express and SunTrust.

Can finance keep up with the hackers?

Analysts estimate that more than half of the world's securities exchanges have fought off cyber attacks since the start of 2013, while an IBM review of its client base shows 21 per cent of attacks are launched against finance and insurance businesses, the second worst-affected sector after manufacturing. A recent report from the New York Department of Financial Services concluded that financial institutions will continue to be challenged by the speed of technological change and the growing sophistication of the cyber threat. As a result, the department plans to add cyber security to its examination procedure, monitoring everything from incident response and access controls to network security and disaster recovery procedures.

More than one in four (28 per cent) of respondents to the Freshfields survey identified financial services as the sector where M&A activity was most likely to be affected by a cyber incident occurring mid-transaction or because of previous cyber security breaches being identified during due diligence. Defence was identified by 25 per cent, followed by technology/software (18 per cent), telecoms (9 per cent), pharmaceuticals (6 per cent) and energy (5 per cent). Interestingly, professional services companies were ranked the least likely to be affected (1 per cent).

Chris Forsyth says: 'A financial institution is likely to suffer more from a cyber attack because of the reputational damage that could result. Banks are where people believe their money and data are safe. If that faith is shaken then banks are more exposed than other businesses.'

Contact us

To discuss your cyber risks, please contact:

Klaus Beucher
Partner, Cologne
T +49 221 20 50 71 13
E klaus.beucher@freshfields.com

Bertram Burtscher
Partner, Vienna
T +43 1 515 15 319
E bertram.burtscher@freshfields.com

Chris Forsyth
Partner, London
T +44 20 7832 7100
E christopher.forsyth@freshfields.com

Matt Friedrich
Partner, London
T +1 202 777 4528
E matt.friedrich@freshfields.com

Jane Jenkins
Partner, London
T +44 20 7832 7280
E jane.jenkins@freshfields.com

Rutger Kleemans
Partner, Amsterdam
T +31 20 485 7642
E rutger.kleemans@freshfields.com

Simon Weller
Partner, Hong Kong
T +85 22 9132 647
E simon.weller@freshfields.com

freshfields.com