DFIN

WHITE PAPER | VENUE MARKET SPOTLIGHT CYBERSECURITY

Venue® Market Spotlight Cybersecurity

DFINsolutions.com

Methodology

Mergermarket interviewed 25 global dealmakers from across the corporate and private equity communities for their views on issues related to cybersecurity. Respondents were split between the US (36 percent), Europe (32 percent), and APAC (32 percent).

Foreword

Our respondents have no doubt that cybersecurity has increased in importance when considering target companies over the past 12 months. And they don't have to look far to see examples of why this has become a crucial consideration — reports of new cyberattacks seem to grace news headlines almost weekly.

These headlines include the widely publicized breaches to Yahoo that were not discovered until 2016 — one in 2013 that is said to have impacted one billion consumers, and a second in 2014 that affected 500 million — that caused its sale price to Verizon to plummet during their acquisition negotiations last year. And a more recent cyberattack, on consumer credit reporting agency Equifax, is said to have potentially impacted 143 million consumers in the US.

While these attacks help to keep the issue of cybersecurity front-of-mind for corporates, the issue of upcoming changes to cyber regulations is equally pressing, such as the European Union's GDPR, which came into effect in May 2018.

Respondents are becoming more savvy to the threat of cybercrime and its potential impact on an M&A transaction. Some, however, fear that the rate at which businesses become more aware of cybersecurity does not match the pace of development by criminals looking to take advantage of weaknesses in a company's data and intellectual property safeguards.

Cybersecurity considerations are becoming the norm for bidders seeking out acquisition targets, respondents say, with cyber due diligence now playing an increasingly crucial part of the screening process.

Other key findings include:

Respondents were unanimous in their opinions that the importance of cybersecurity has increased in the past 12 months, some 44% say significantly so.

More than half (52%) of respondents say 26%-50% of the companies they have targeted for an M&A deal have experienced data security breaches at some point in the past 24 months.

Some 76% of respondents say that the consumer and e-commerce sector will be the most targeted by cybersecurity threats in the coming 12 months.

Survey

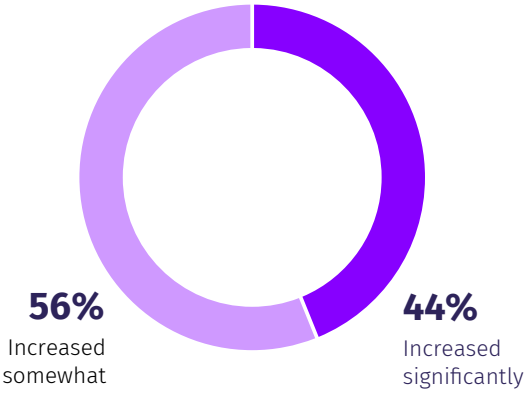
Q1

Over the last 12 months, how has the importance of cybersecurity issues at target firms in M&A deals changed for you, if at all?

As large-scale corporate and political hacks become an all-to-frequent occurrence, businesses are taking heed. Our respondents say, unanimously, that the importance of cybersecurity at the companies they target for deals has increased over the past 12 months. And many add that this is only going to continue: "Cyber issues now have the potential to bring down an entire business," says the managing director of a private equity firm in Australia. "It is a serious issue. In any deal, cybersecurity is an important aspect, and in some industries it is quite critical. The importance of cybersecurity is only going to increase further."

A senior director of corporate development at a private equity firm in the US says that while the concept of cybercrime has evolved over the years, the growth rate of cybercrime has been faster than the growth of cyber awareness and security.

"Our company depends on a digital structure where we contain our client information, business and investment plans," explains a managing partner at a private equity firm in the US. "If we acquire a target company which has a fragile cybersecurity structure, we might be at risk of acquiring a company whose digital assets might've already been compromised, and that puts us at risk, too."



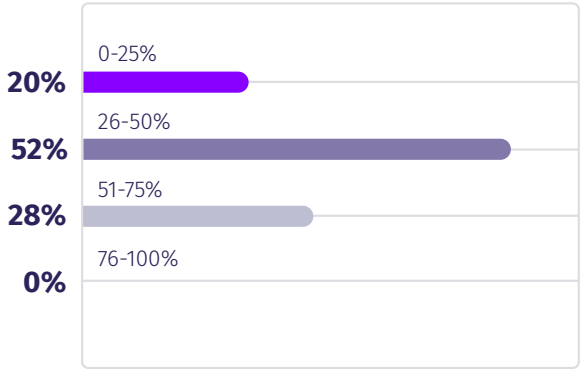
Q2

At roughly what percentage of M&A targets have you uncovered data security issues in the past 24 months?

According to the annual Symantec Internet Security Threat Report, there were more than 1,209 cybersecurity breaches in 2016, exposing an estimated 1.1 billion identities. Ransomware attacks grew in the number of detections, rising to 463,841 in 2016 from 340,665 in 2015. With figures such as these, it is no surprise that 80% of respondents say that they have uncovered data security breaches in between 26 percent and 75 percent of M&A targets.

A managing director at a private equity firm in China says his firm has faced data security issues in at least 50 percent of its targets. "The data security issues varied quite a lot according to the market the target was based in, and also to an extent the sector the target was operating in. In regions like APAC, Africa and the Middle East, the data security issues were much higher and critical than in Europe or North America."

"Over the past two years we've noticed an increase in demand for cybersecurity solutions," explains a managing director at a PE firm in the US. "Cyberattacks like ransomware and Wikileaks have made it really clear that cybercrime exists in every industry. Though there are M&A targets that haven't achieved the utmost level of expertise in cybersecurity, we see that they're definitely willing to work towards it."

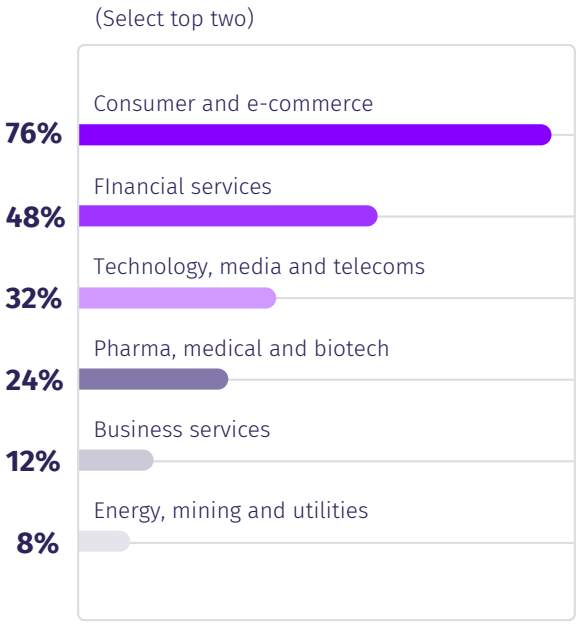


Q3

In which sectors are cybersecurity issues currently most important in M&A transactions?

Consumer and e-commerce convincingly topped the ranking of sectors in which cybersecurity is most important, with 76% saying the threat of cyberattack was strongest in this industry. “Cyberattacks aimed towards the consumer and e-commerce sector have more to them than just the monetary factor; there’s a breach of confidentiality,” explains a director of corporate development at a US corporation. “People get affected, their private lives get compromised, and nobody likes that.”

Financial services and technology, media and telecommunications were the second and third-ranked sectors most at risk from cyberattack, with 48 percent and 32 percent citing them respectively.



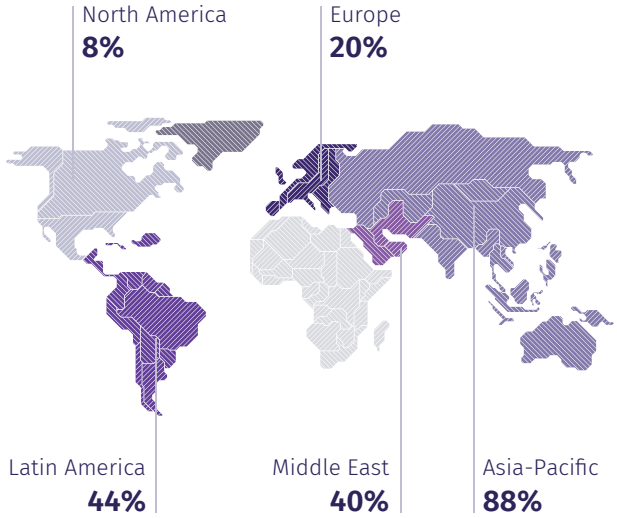
Q4

In which regions are cybersecurity issues currently most challenging in M&A transactions?

Developing economies in the Asia-Pacific region are the most likely to encounter challenges with cybersecurity, say an overwhelming 88 percent of respondents. “There’s definitely an increase in cyber threats in the Asia-Pacific region, and the attacks that have been executed in recent times have done a lot of damage” says a managing director at a PE firm in Hong Kong. “The last thing an investor would want is to invest in a platform which has threats that cannot be comprehended or controlled.”

A managing partner at a PE firm in the US explains further: “In the Asia-Pacific region, the digital world is growing very fast, and that invites a lot of cybercrime or hackers, but they don’t have a strong cybersecurity structure. However, even in countries like America, where companies are investing a lot of money in cybersecurity, they are also witnessing the growth of cybercrime at an unbelievable speed.”

(Select top two)



Q5

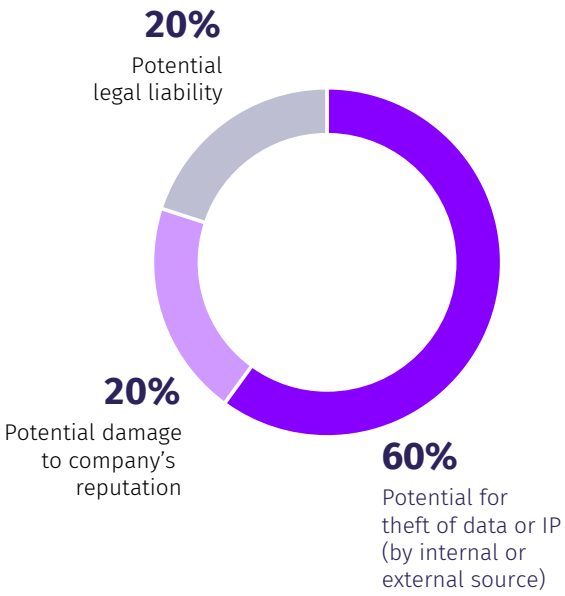
When evaluating cybersecurity threats at an M&A target, what is usually your greatest concern?

The potential theft of intellectual property or data is overwhelmingly the greatest concern for acquirers when assessing a target for cybersecurity threats. Some 60 percent of respondents cited this as their top concern, with 20 percent each naming the potential for legal liability and potential reputation damage.

"The intellectual property of a company is its foundation," says a head of corporate finance at a corporation in India. "It literally defines the movements, the actions, the growth and the direction of the company. In the wrong hands, it could be responsible for the downfall of the company."

Another respondent, the CFO of a corporation in Japan, says that the concern of lost data or IP and potential legal liability go hand-in-hand: "Intellectual property consists of all the confidential information that is under the disclosure policies, and we become legally liable once the IP is stolen. Therefore, both would be our greatest concern."

(Select one)



Q6

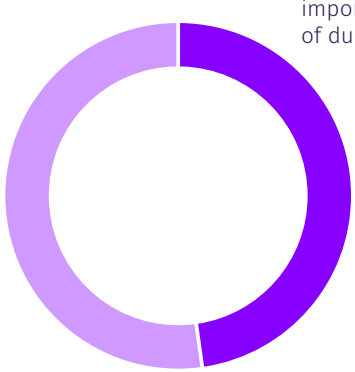
Compared to other types of due diligence, how important has cybersecurity diligence become in a typical M&A deal?

There is no doubt among respondents that cyber due diligence is an important aspect of the wider due diligence process. During Verizon's acquisition of Yahoo, the internet giant disclosed two massive data breaches that affected more than one billion user accounts. Consequently, Verizon cut $350 million off its offer, even though the companies had initially agreed on a sale price months before Yahoo disclosed the breaches. What's more, publicized data breaches can lead to a drop in stock price and devaluation of the company.

60 percent of respondents say that theft of data or IP is the greatest cybersecurity threat

"We've seen what cybercrimes lead to and are capable of doing. The damage is too high; we can't afford to move ahead with a target company that has a vulnerable cybersecurity system. Hence, it has to be one of the top priorities in M&A deals," says a director of corporate finance at a corporation in Germany.

The CFO of a Chinese corporation puts it plainly: "Cybersecurity diligence can make or break a deal. An acquirer wouldn't want to put its entire company under risk of being invaded and then dealing with major damages."



48%
Among the most important aspects of due diligence

52%
Roughly the same level of importance as other aspects of due diligence

Q7

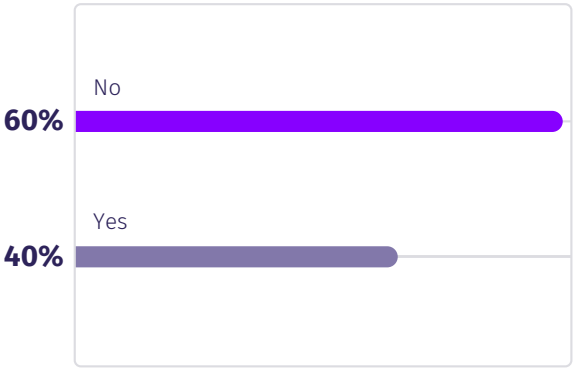
Over the last 24 months, have you walked away from any deal due to cybersecurity issues at a target firm?

Even when a breach or insufficient cybersecurity measures are discovered at a target company that may not be the end of the deal. Like Verizon, who pushed ahead with their acquisition of Yahoo despite the large attacks the company had endured, more than half (60 percent) of respondents have not walked away from a deal because of cybersecurity issues.

A director of corporate development at a corporation in the US explains that his company is usually able to work around a potential cybersecurity risk. “If we spot cybersecurity issues at a target firm, we bring them the solution too, and then we restructure the deal accordingly. So far, it’s always worked for us. We have walked away from deals, but not for cybersecurity issues.”

Other companies draw a harder line on the subject: “We were in talks with a product-based company looking at expansion, and it was going to be a direct investment,” explains a managing director at a PE firm in France. “We analyze our targets inside-out and that exposed their casual approach towards the cyber threats that were out there. This company had a small budget and didn’t want to invest further in cybersecurity. Therefore, the deal was terminated.”

According to respondents, investors can also influence the decision of whether or not to go ahead with the acquisition of a company that has encountered a breach or one that has low cybersecurity safeguards.



Mergermarket is an unparalleled, independent mergers and acquisitions (M&A) proprietary intelligence tool. Unlike any other service of its kind, Mergermarket provides a complete overview of the M&A market by offering both a forward-looking intelligence database and a historical deals database, achieving real revenues for Mergermarket clients.

Acuris Studios, the events and publications arm of Acuris Global, offers a range of publishing, research and events services that enable clients to enhance their own profile, and to develop new business opportunities with their target audience.

To find out more, please visit **www.acuris.com**

About Donnelley Financial Solutions (DFIN)

DFIN is a leading global risk and compliance company.

We're here to help you make smarter decisions with insightful technology, industry expertise and data insights at every stage of your business and investment lifecycles.

As markets fluctuate, regulations evolve and technology advances, we're there. And through it all, we deliver confidence with the right solutions in moments that matter.

Learn about DFIN's end-to-end risk and compliance solutions.

Visit **DFIN**solutions.com | Call us **+1 800 823 5304**