MARSH

UK 2015 Cyber Risk Survey Report

CONTENTS

INTRODUCTION

Marsh has undertaken an in-depth study into organisations' attitudes towards the cyber threat, the management control processes they have in place, and their understanding and use of cyber insurance as a means of risk transfer. The benchmarking data in this report was collected from risk professionals and CFOs from large and medium-sized corporations from across the UK. By conducting this study, we hope that the aggregated information will provide useful benchmarking data and reference points against which the reader can compare their own company's positions.

BOARDROOM DISCUSSION

Spotlight on cyber risk to UK companies:

18%

of organisations have a "complete understanding" of cyber risk, down on last year.

19.4%

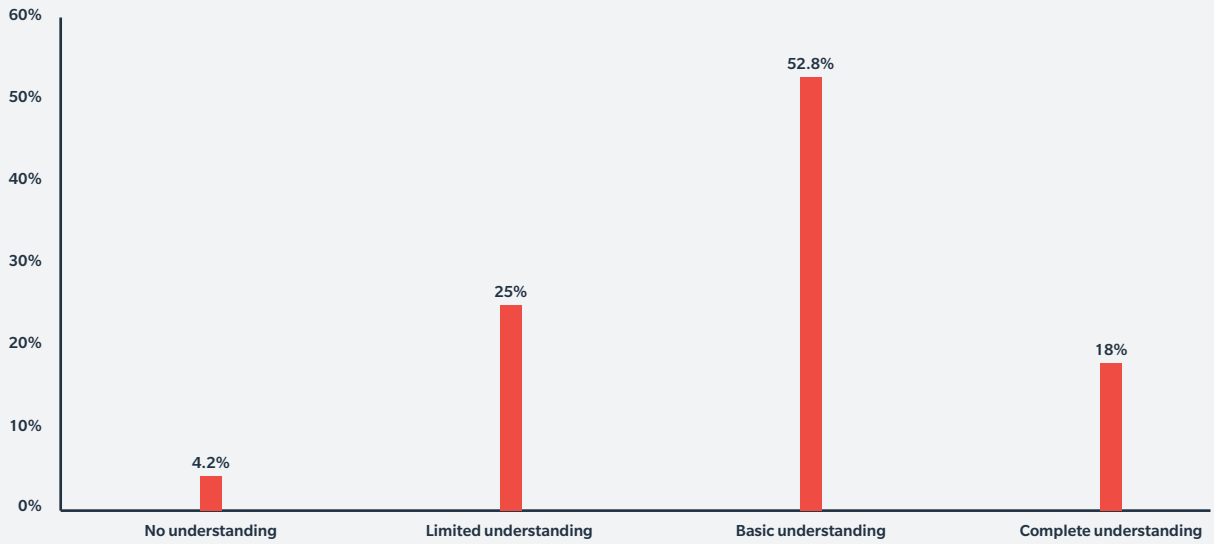
of UK businesses have board-level oversight of cyber risk.

69.4%

of companies do not assess their suppliers and/or customers for cyber risk.

WORK STILL TO BE DONE IN TERMS OF AWARENESS/ OWNERSHIP OF CYBER RISK

FIGURE 1
To what extent do you believe your organisation has a clear understanding of its exposure to cyber risk?



Firms across the UK continue to place cyber among their leading risks in terms of the likelihood and severity of impact[1]; however, the findings in FIGURE 1 suggest there is still a lot of work to do to improve understanding and management.

Interestingly, there has been a substantial drop in the percentage of respondents who feel they have a "complete understanding" compared to last year[2] (down from 34% to 18%).

This comes at a time when cyber risk is being elevated as a board agenda item, suggesting that executive-level interrogation has exposed a pre-existing overconfidence in the level of knowledge and understanding within certain organisations.

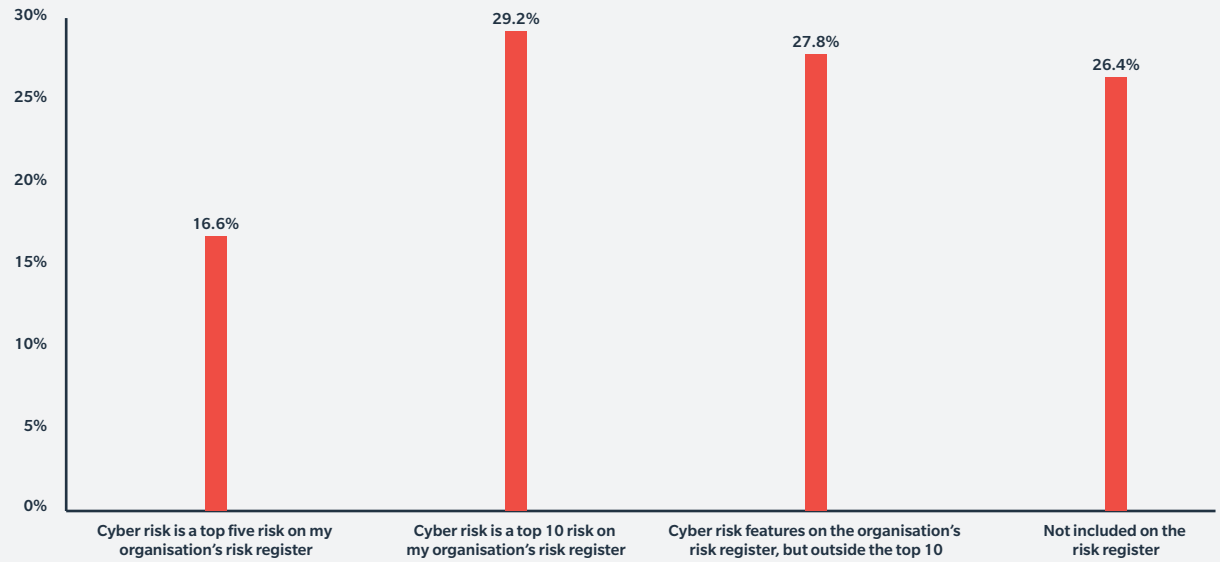
If this is the case, then it is clear those tasked with creating and delivering critical management information relating to cyber risk need more help and guidance to get them to a position where the level of management information is adequate.

Cyber risk is ranked as a tier one threat according to the UK National Security Strategy, and it is therefore surprising that more than a quarter (26.4%) of UK companies surveyed do not consider it to be material enough to even get on the risk register. Just 16.6% of companies place cyber as a top five risk on the risk register, while the remainder place it outside of the top 10.

[1] *Global Risks 2015 (10th Ed.)*, World Economic Forum, Geneva, 2015.

[2] Comparisons are with the *2014 UK and Ireland Cyber Risks Survey*, London, Marsh.

FIGURE 2
Where does cyber risk feature on the corporate risk register?



In light of the results in FIGURE 2 relating to the understanding of cyber risk, however, these findings are easier to explain. Employees in those companies that do not place cyber risk on their risk registers are unlikely to have a decent level of understanding of cyber, since it will not have received the necessary level of investigation to move it forward.

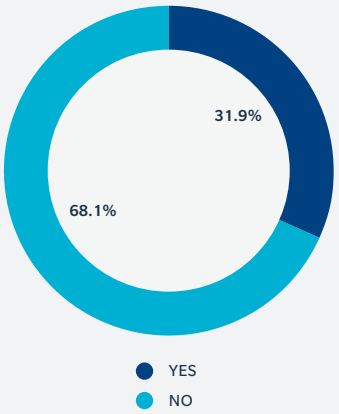
Nearly three quarters (73%) of respondents from the manufacturing industry say that cyber risk does not appear in the top 10 risks on their corporate risk registers — the highest proportion of industry segments we surveyed. This is perhaps understandable due to a low level of high-profile cyber incidents within the industry; however, as a key target for industrial espionage, and with instances of industrial control technology being compromised recently reported[3], one could argue that the threat is being underestimated.

Those tasked with creating and delivering critical management information relating to cyber risk need more help and guidance to get them to a position where the level of management information is adequate.

[3] As disclosed by the German Federal Office of Information Security, which reported "massive damage" to a blast furnace at a steel mill in Die Lage der IT-Sicherheit in Deutschland 2014, available at *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.*

FIGURE 3

Have you identified one or more cyber scenarios that could most affect your organisation?

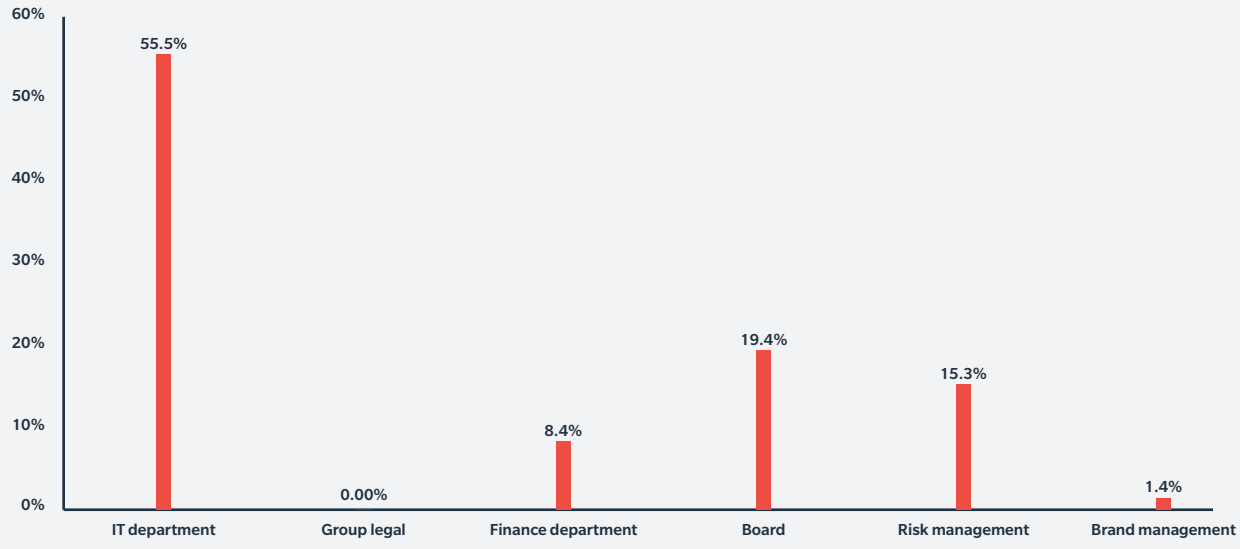


The fact that fewer than one third (31.9%) of respondents have identified one or more cyber scenarios that could most affect their organisations (see FIGURE 3) correlates with the findings from FIGURE 1. It suggests that the lack of a complete understanding and absence/low positioning of cyber on the risk register is, for many companies, filtering through to a lack of definition around specific scenarios that might impact their businesses.

Board-level ownership of cyber risk exists in 19.4% of UK organisations. While this figure is broadly in line with last year's findings (20%), it remains very low (see FIGURE 4). Meanwhile, IT departments continue to take primary responsibility for cyber risk in the majority (55.5%) of organisations. Cyber risk is increasingly recognised as a business risk rather than simply a technical control, and, within this context, it is disappointing to note that there is no material upwards movement in risk management and board functions seizing responsibility from IT (the percentage has risen incrementally to 15.3% from 14% in 2014). IT departments might know how to implement cybersecurity; however, the inability of IT to drive value for the organisation or the potential for significant damage to be caused as a result of a security breach, most certainly is a business risk — the consequences of which will be felt at the highest levels of the organisation should it occur. Boards therefore need to take ownership of cyber risk before a cyber event forces it on to the board agenda, and communicate the identified security priorities to IT departments so that they can align their activity and resources against the business's risk management agenda.

FIGURE 4

Please indicate which of the following potential stakeholders takes primary responsibility for the review and management of cyber risks in your organisation.



LACK OF DATA CONTINUES TO PREVENT COMPANIES FROM ADEQUATELY ASSESSING CYBER RISK

The percentage of firms that have experienced a cyber-attack in the past 12 months has risen to 40.3% (see FIGURE 5), albeit marginally (from 31% in 2014).

However, compared with other statistics (HM Government's *2015 Information Security Breaches Survey* states that 90% of large organisations and 74% of small organisations have suffered a security breach)[4], this figure is still low, indicating that many of the respondents to this year's survey are either particularly fortunate or (more likely) unaware of breach events within their firms.

Interestingly, 100% of respondents in two industries — communications, media, and technology and energy — reported that they had been subject to a cyber-attack in the past 12 months. This most likely reveals a more enlightened position of those organisations rather than any high level of vulnerability.

In terms of organisations that have conducted or estimated the financial impact of a cyber-attack, this year's survey results are somewhat contradictory to earlier findings. As such, it would be reasonable to question the rigorousness of the financial analysis around those numbers and how many are in fact high-level estimates rather than worst loss values calculated from detailed information and knowledge of cyber risk and individual exposures.

The majority (61.1%) of organisations have not yet made any attempt to estimate/calculate loss estimates (see FIGURE 6), however, suggesting that they are operating in the dark when it comes to the financial impact upon their businesses.

FIGURE 5

Has your organisation been subject to a cyber-attack in the past 12 months?

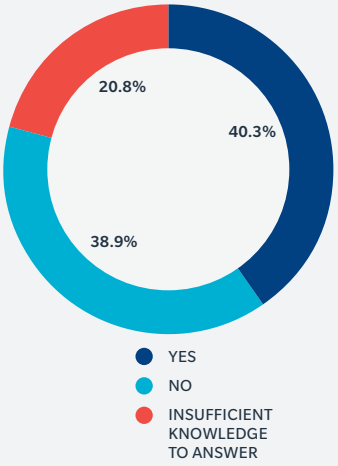
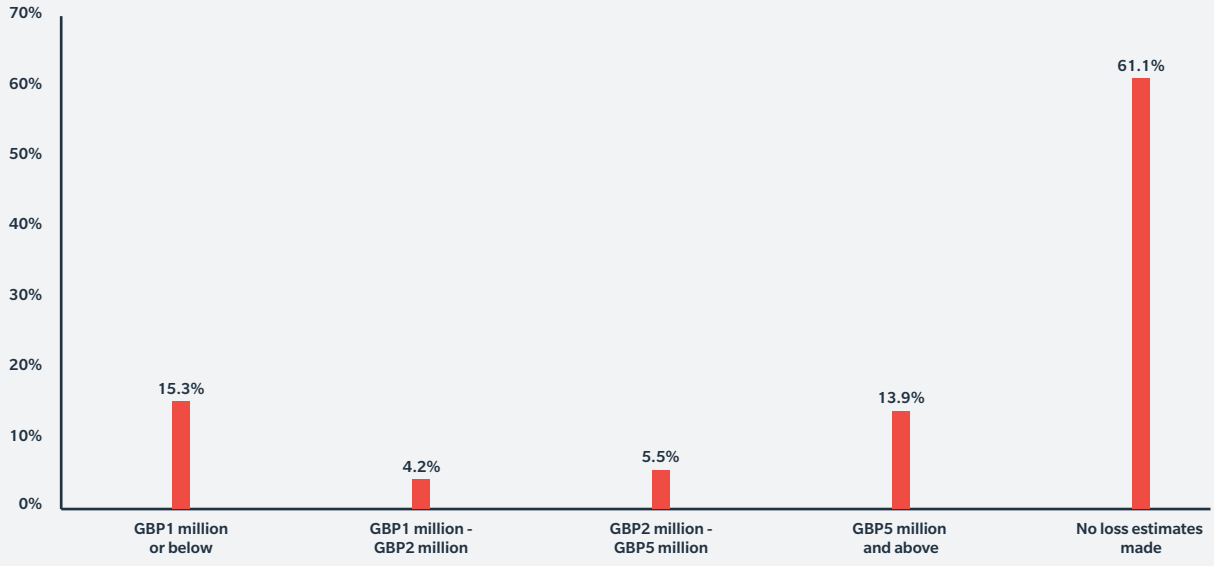


FIGURE 6

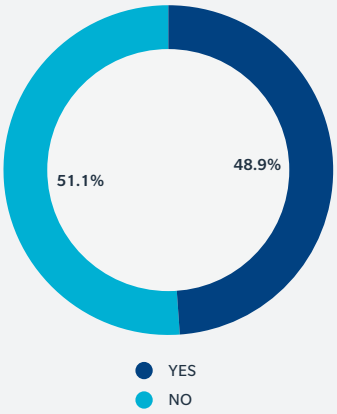
Has your organisation conducted or estimated the financial impact of a cyber-attack? What is the worst loss value?



[4] *2015 Information Security Breaches Survey,* UK Department for Business Innovation & Skills, London, 2015.

FIGURE 7

If yes, does your finance function have a plan in place to access sources of appropriate funding to deliver both the required amount of funds and be accessible at the point when it is needed?



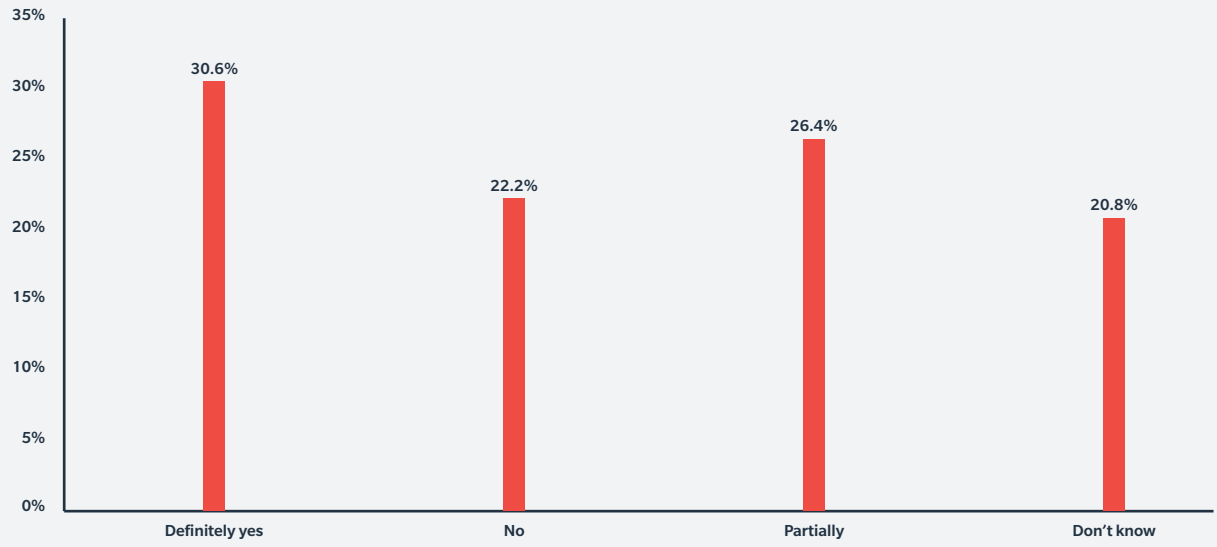
This puts them in a poor position to transfer the risk or even to appreciate whether a cyber event might threaten the viability of the company. Event modelling, combined with financial stress testing, is required to evaluate both the total financial loss attaching to an event and the shorter-term availability of cash to maintain trading.

The majority of organisations have not planned for sources of funding (see FIGURE 7); however, the 48.9% that have is an encouraging number. Since just 11.1% of companies are buying insurance (see FIGURE 11), it must be the case that companies are bypassing the insurance market and finding alternative methods to fund the risk (from available cash lines or lines of credit or assets that can be disposed of rapidly, for example).

Possessing and rehearsing an incident response plan is recognised as having a very positive effect on the operational, financial, and reputational impact of a cyber-attack upon an organisation. The effect for breaches of personal data was quantified in the Ponemon Institute's *2015 Cost of Data Breach Study*, which reveals that those companies with an incident response team in place typically make a GBP9.50 saving on the per capita cost of a data breach, compared with the mean per capita cost[5].

FIGURE 8

Does your organisation possess an incident response plan for material cyber events?



[5] *2015 Cost of Data Breach Study*, Ponemon Institute, London, May 2015.

LACK OF CONTROL OVER SUPPLIERS/THIRD PARTIES A MAJOR CONCERN

It is both a surprise and a huge concern that more than two thirds (69.4%) of respondents to this year's survey do not assess the suppliers and/or customers they trade with for cyber risk (see FIGURE 9).

Suppliers and external organisations with whom system links are shared present one of the key vulnerabilities to UK companies. Businesses have done a lot to improve cybersecurity in the past 12 months; however, their exposure to third parties, whether service providers, product suppliers, customers, or, in the case of banks, borrowers, presents significant risks to companies' networks. In addition to this, more than half of respondents (51.4%) are not asked to demonstrate a competent standard of IT security practices to their own bank and/or customers in order to do business with them.

While organisations can control their own networks, they have much less control over those of the suppliers/third parties that they might be linked to. Without the appropriate checks, this leaves them exposed and lacking control over standards of IT security in systems where hackers might find a "back door" into their organisation. There therefore needs to be an improvement in supply-chain resilience to cyber-attack if organisations are going to reduce the threat arising from this key vulnerability. This is especially true for large organisations with a profile that attracts highly motivated and sophisticated hackers who might identify smaller business partners that are typically less well protected. For example, a recent report published by Marsh and the UK Government highlighted that nearly a quarter (22%) of small businesses admit they "don't know where to start" with cybersecurity[6].

FIGURE 9

Do you assess suppliers and/or customers you trade with for cyber risk?

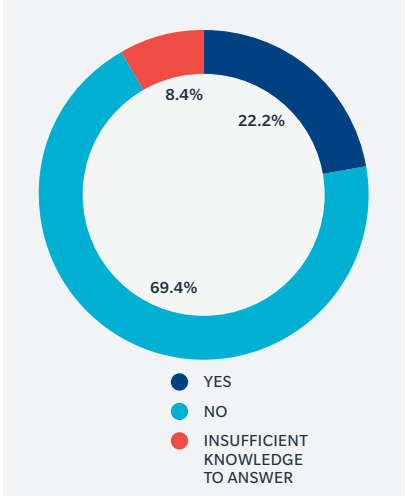
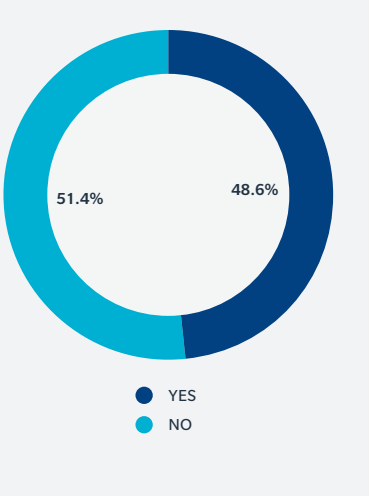


FIGURE 10

Has your bank or your customers required you to demonstrate a certain standard of IT security practice in order to do business?



One of the most well-publicised cyber breaches in recent years occurred at a large US retail company after hackers stole network credentials from a third-party heating, ventilating, and air conditioning (HVAC) contractor that had an IT link with the victim's corporate systems. Incidents like these are likely to rise in frequency until organisations place greater focus on setting out the basic technical controls that all suppliers/contractors should have in place.

More than half of respondents are not asked to demonstrate a competent standard of IT security practices to their own banks and/or customers.

[6] *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*, UK Cabinet Office, London, May 2015.

TAKE UP OF CYBER INSURANCE REMAINS LOW

It is encouraging to find that more than half (52.8%) of respondents' organisations are engaged with the insurance market in one way or another (see FIGURE 11).

Our experience and earlier findings in this survey suggest that the remainder are not yet ready to approach the market as they have an incomplete understanding of the risk, as opposed to them making a conscious decision not to purchase insurance following a value-based judgment.

This latter explanation would tie in with the earlier finding that 68.1% of organisations have not identified one or more cyber scenarios that could most affect their organisations (see FIGURE 3). Organisations such as these — because they have not carried out the financial assessment required — are in a poor position to approach the insurance market and place a value on transferring the risk. The survey data therefore suggests that more work needs to be done by organisations and their professional advisers — including their insurance brokers — to help improve their understanding of cyber risk and their cyber exposures and demonstrate what value insurance can bring.

The insurance market continues to address the issues that represent organisations' greatest concerns (see FIGURE 12): A standard cyber insurance policy can deliver cover against breach of customer information (31.9%) and business interruption (22.2%), while computer crime/fraud (12.5%) can be insured against via a comprehensive crime insurance policy. The insurance market is also making inroads to deliver meaningful cover for reputational loss (8.4%).

Of particular interest is that none of the respondents from the industrial sectors identified physical property damage as a priority risk, despite a lot of recent attention being given to the threat that exists to critical infrastructure and the potential for tampering with industrial control technology.

FIGURE 11

Please indicate your organisation's current status with regard to cyber insurance.

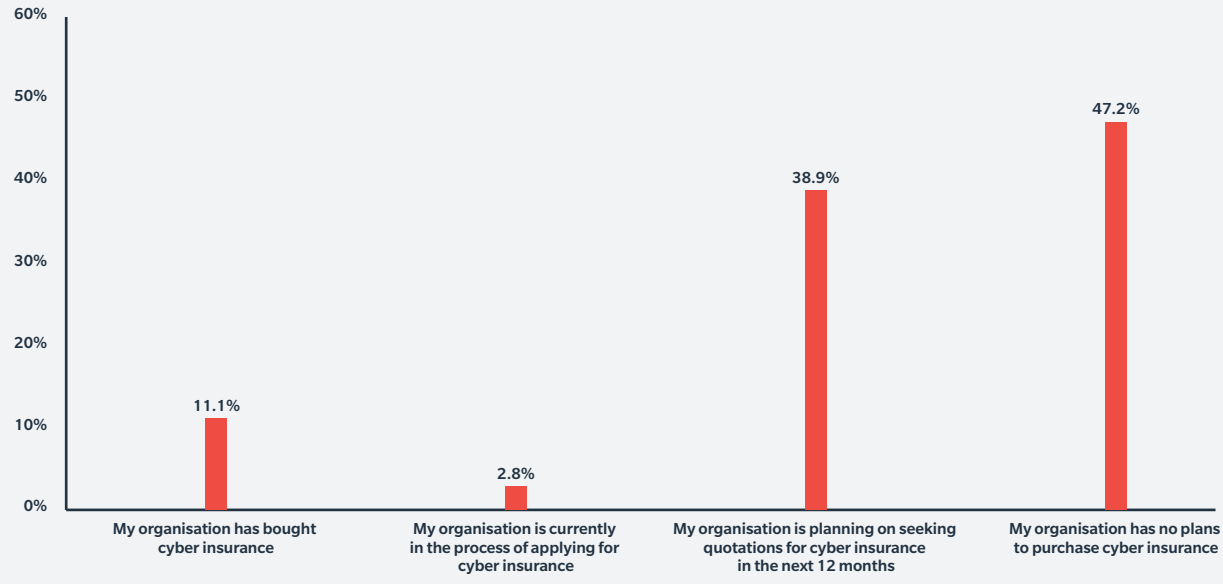


FIGURE 12

Which cyber loss scenario presents the greatest threat to your organisation?

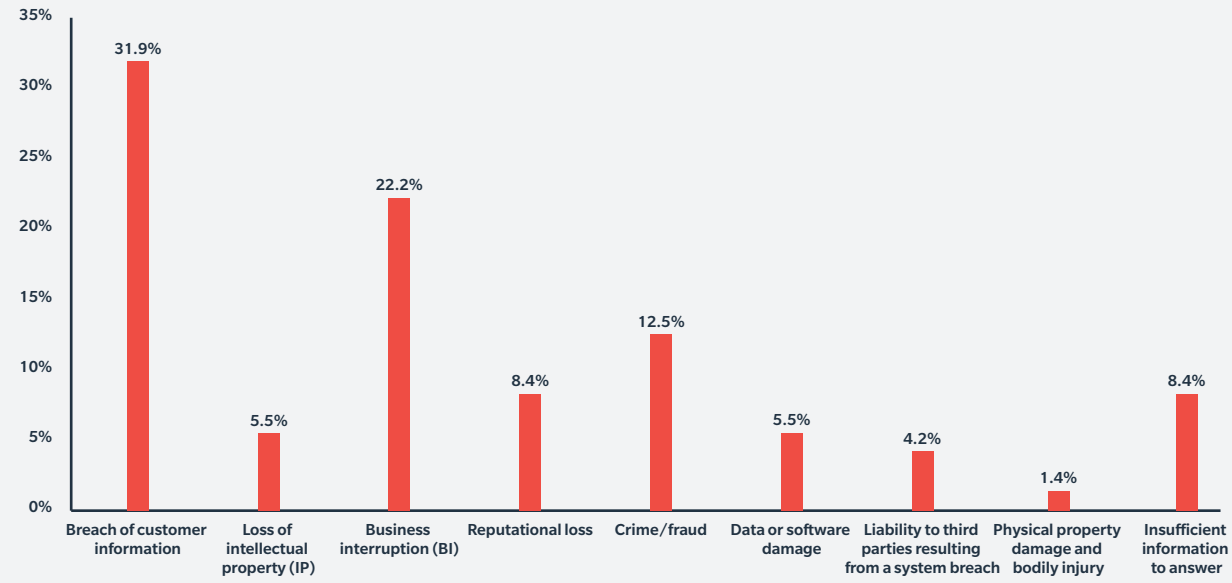


FIGURE 13

Where do you view the greatest threat to your organisation originating from?

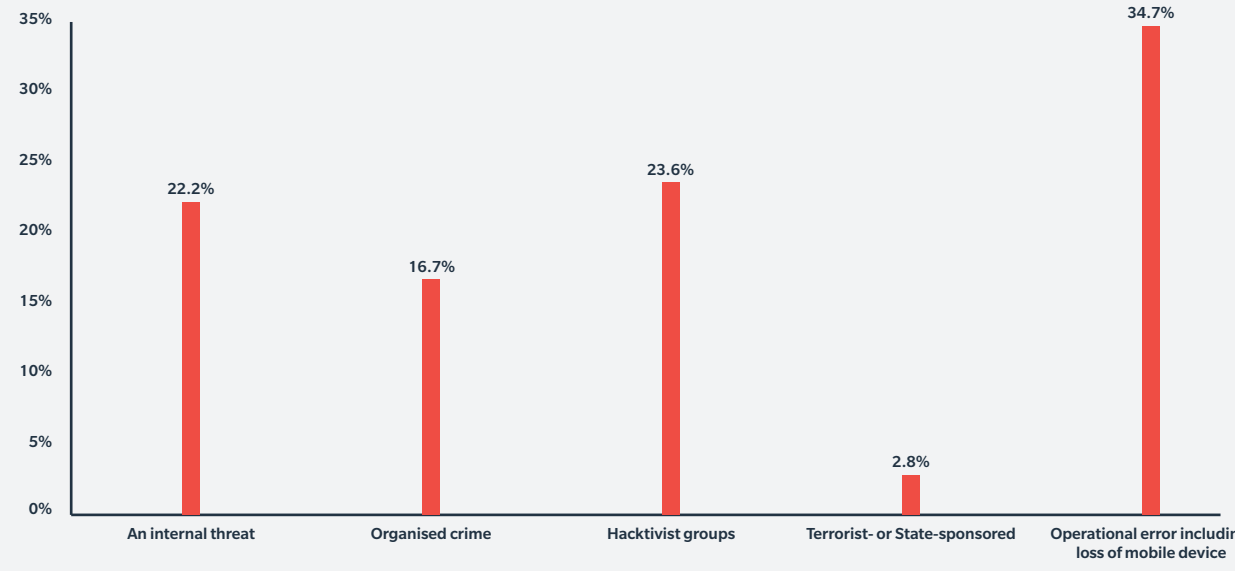
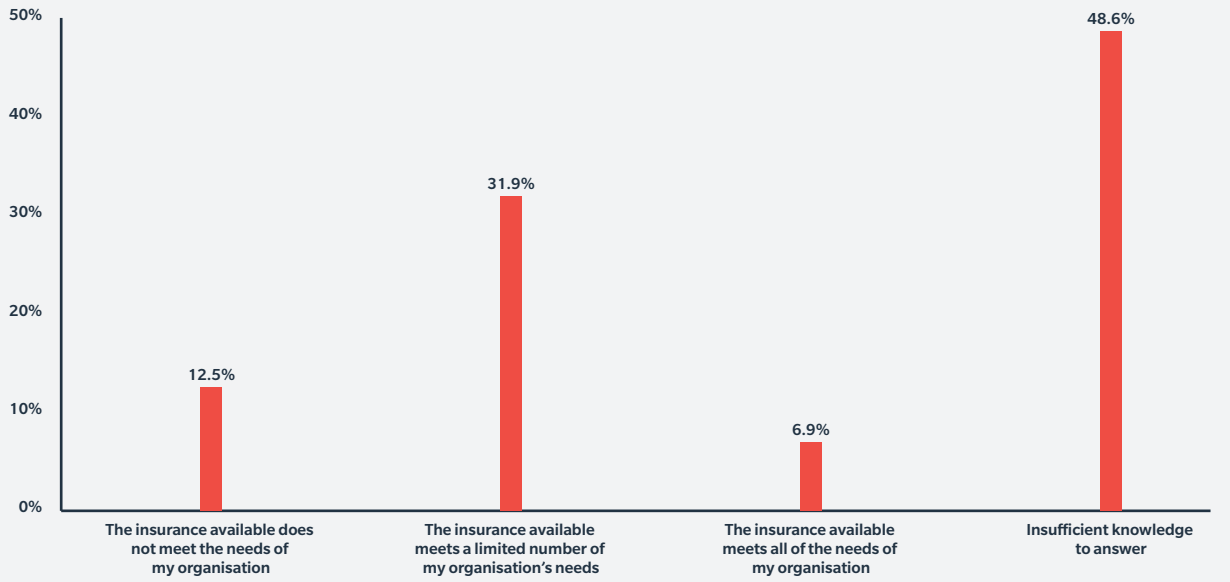


FIGURE 14
Which statement best reflects your attitude to cyber insurance based on your current knowledge?



The findings in FIGURE 14 suggest that companies recognise that cyber insurance is not a holistic solution in dealing with cyber exposure and that, in fact, it covers only certain specific events and outcomes. Cyber exposure might attach itself to a number of different insurance policies that need to maintain an effective response when the loss or liability outcomes are created by cyber events. Nearly half (48.6%) of respondents admit to having "insufficient knowledge" in order to assess the insurances available, which may suggest a lack of insight into what can be insured by a cyber insurance policy. However, in view of the earlier findings, this figure might also indicate that a lack of understanding of their firm's own risk profile places many respondents in a position where they are unable to make an informed judgment as to whether the cover is appropriate.

Cyber insurance is not a holistic solution in dealing with cyber exposure and covers only certain specific events and outcomes.

CONCLUSION

Clearly, there is still a lot of work that needs to be done by UK organisations in order to improve their understanding and management of cyber risk. Achieving a high level of understanding is essential as it serves as the foundation stone upon which all other cyber risk transfer and mitigation decisions need to be made.

The solution to this lies in the boardroom, and it is still a great concern that the board takes primary responsibility for cyber risk in less than one fifth (19.4%) of organisations surveyed. Only with board-level buy-in can companies take the big strides needed to advance their knowledge and perform the financial modelling required. Proper assessment and quantification of the risk will lead to better targeted mitigation, practical improvements in risk management, and the ability to judge the value of the risk transfer options available on the market.

One particularly interesting — and somewhat remarkable — finding to emerge from this year's survey is that more than two thirds (69.4%) of respondents' organisations do not assess the suppliers they trade with for cyber risk. Supply chains are proven to be a critical vulnerability in corporate IT networks, yet there appears to be too little work being done to ensure that the entities with which companies share system links are following basic good security practices.

This has to improve as, for all the proactive steps taken and money invested to harden corporate networks against cyber-attacks, a security breach at a contractor or service provider, for example, could potentially allow hackers to circumnavigate all of that. The insurance industry can play and is already playing a role in that assurance process; however, more work needs to be done in order to move the security focus away from the edge of the corporate network and to the heart of strategic decision making.

Proper assessment and quantification of the risk will lead to better targeted mitigation, practical improvements in risk management, and the ability to judge the value of the risk transfer options available on the market.

About Marsh

Marsh is a global leader in insurance broking and risk management. We help clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 27,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global team of professional services companies offering clients advice and solutions in the areas of risk, strategy, and people. With 57,000 employees worldwide and annual revenue exceeding $13 billion, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a global leader in providing risk and reinsurance intermediary services; Mercer, a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a global leader in management consulting. Follow Marsh on Twitter @MarshGlobal.

About this *UK 2015 Cyber Risk Survey Report*

This report was prepared by Marsh's Cyber Risk Practice, which is dedicated to providing insurance and risk management solutions for the cyber exposures of clients around the world.

In the UK, the practice:

- Manages premium volume in excess of GBP4 million.
- Has 10 cyber risk experts dedicated to serving clients across the UK.

At Marsh we have a proven track record of helping our UK clients of all kinds operate in an increasingly technologically dependent environment, particularly at a time when many businesses' critical processes are often automated and delivered to the point of use by a mixture of internal and external resources. Our UK team works closely with our clients to meet the complex risk management challenges that the diversity of dependent systems and use of critical third-party IT suppliers for delivery create. Clients with operations outside the UK can benefit from access to our global team which works out of more than 20 offices worldwide to provide clients with the support they require when directing preventative mitigation resources and taking informed risk transfer decisions. By combining the expertise within Marsh Risk Consulting and Marsh FINPRO's cyber placement team we are able to deliver a seamless service for clients in this important area of risk.

According to specific requirements, we can deliver:

- Cyber risk financing optimisation.
- Coverage gap analysis.
- Cyber placement benchmarking.
- Enhanced cyber insurance policy wordings.

Notes

MARSH

For more information, please contact:

STEPHEN WARES

EMEA Leader, Cyber Risk Practice
Marsh Ltd
+44 (0)20 7357 5420
stephen.wares@marsh.com