MARSH

European 2015 Cyber Risk Survey Report

CONTENTS

INTRODUCTION

Using its knowledge and information about cyber risk in Europe, Marsh has undertaken an in-depth study into organisations' attitudes towards the threat, the 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 from large and medium-sized corporations from across the continent.

BOARDROOM DISCUSSION

Cyber risk to European companies:

79%

of organisations have, at best, a basic understanding of their exposures cyber risk.

43%

of respondents have not yet identified one or more cyber scenarios that could affect their organisations.

68%

of organisations have not estimated the financial impact of a cyber-attack.

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

Organisations across Europe are growing increasingly concerned about the likelihood and impact of cyber-attacks[1]; however, the findings in FIGURES 1A and 1B suggest there is still a lot of work to do to improve the understanding and management of cyber risk.

It is a concern that an overwhelming majority (79%) of organisations have, at best, a basic understanding of their cyber risk profiles, putting them in a relatively poor position to prioritise their risk mitigation efforts and risk transfer strategies.

It is a surprise that 25% of organisations surveyed do not consider cyber risk to be material enough to even get on the risk register, while 30% place the risk outside of the top 10 (SEE FIGURE 2).

We would suggest that these organisations undertake a re-evaluation of cyber risk, to understand how exactly it poses a threat to them and their operations.

These high figures are also a concern since it is reasonable to assume that, because cyber risk is low down on – or completely absent from – these companies' risk registers, it is not going to receive the level of investigation required to sufficiently map and quantify the risk to the business. Not only will this restrict efforts to mitigate the threat posed by cyber risk; it will make ascertaining the value, and therefore suitability, of available risk transfer options all the more problematic.

It may also be the case that the low level of understanding highlighted in FIGURE 1A/1B is as a consequence

FIGURE 1A To what extent do you believe your organisation has a clear understanding of its exposure to cyber risk?
Source: Marsh European 2015 Cyber Risk Survey

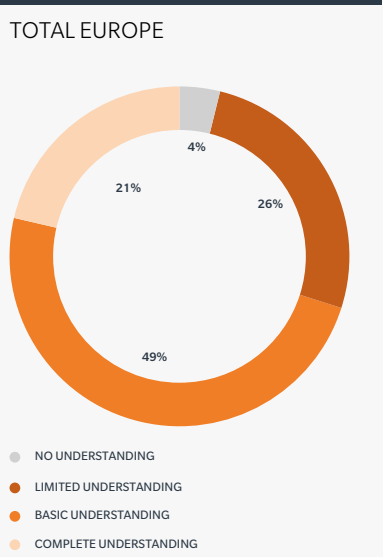
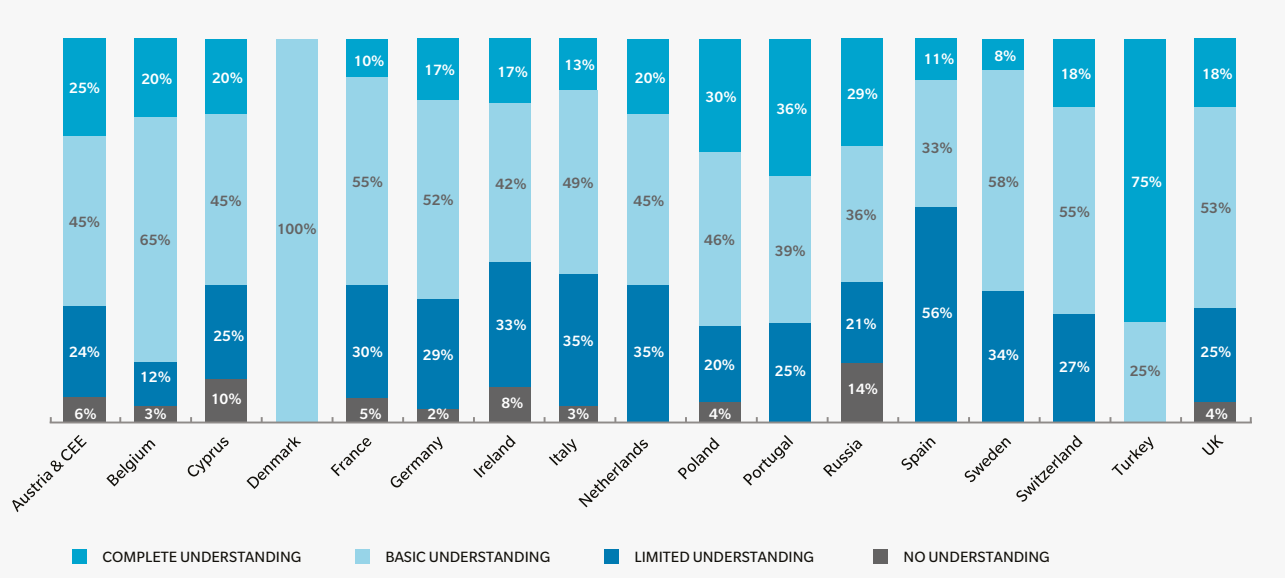


FIGURE 1B To what extent do you believe your organisation has a clear understanding of its exposure to cyber risk?
Source: Marsh European 2015 Cyber Risk Survey



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

of its low weighting on some organisations' risk registers. This is because there is likely to be a poor level of understanding of cyber risk in those organisations that haven't given it the level of investigation required to move it forward.

IT departments continue to take primary responsibility for cyber risk in nearly two thirds (65%) of organisations (SEE FIGURE 3). This is inadvisable, however, in the sense that cyber is a business risk – not a technical one.

Instead, the board and risk management function should take a greater responsibility for cyber risk, since they are better positioned within their organisations to understand which parts are business-critical and map the many potential operational and financial impacts an event could have.

This could be another reason for the lack of attention paid to cyber risk on European companies' risk registers (SEE FIGURE 2) – namely that the oversight of cyber is located in a part of the business that doesn't have the capability and/or authority to carry out the financial evaluations and more detailed scenario analysis required to adequately assess the risk posed to the organisation. This is something we shall look at in closer detail in Section 2 of this report.

Of those functions with a financial or fiduciary responsibility – the board, finance department, and risk management have the greatest interest and responsibility for the financial impact on an organisation of a cyber event. Despite this, the responsibility for cyber risk lies with these functions in just 26% of respondents' organisations.

FIGURE 2 **Where does cyber risk feature in the corporate risk register?** Source: Marsh European 2015 Cyber Risk Survey

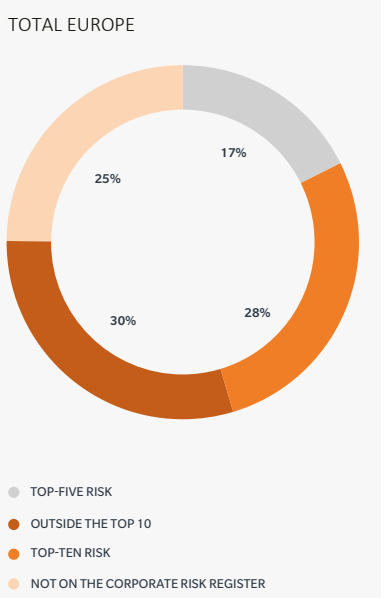
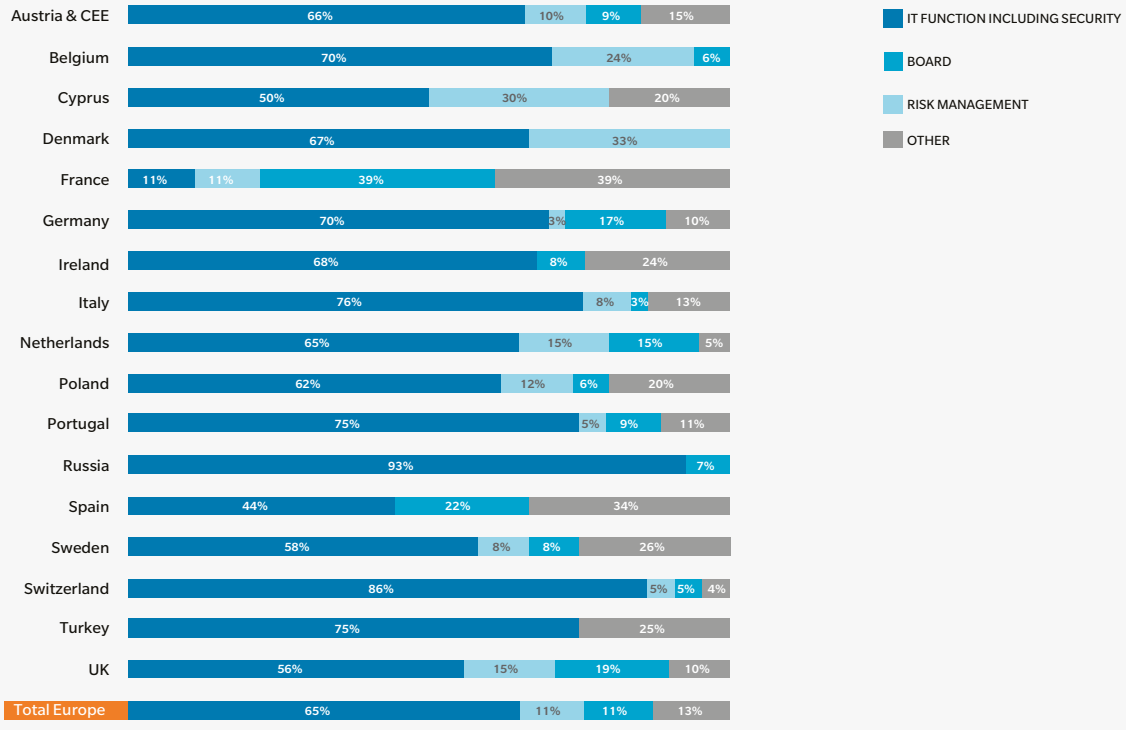


FIGURE 3 **Please indicate which of the following potential stakeholders takes primary responsibility for the review and management of cyber risks in your organisation.** Source: Marsh European 2015 Cyber Risk Survey



A LACK OF PROPER OVERSIGHT CONTINUES TO PREVENT COMPANIES FROM ADEQUATELY ASSESSING CYBER RISK

FIGURE 4 **Have you identified one or more cyber scenarios that could most affect your organisation?**
Source: Marsh European 2015 Cyber Risk Survey

	YES	NO	N/A
AUSTRIA & CEE	58%	42%	
BELGIUM	74%	26%	
CYPRUS	60%	40%	
DENMARK	67%	33%	
FRANCE	50%	50%	
GERMANY	39%	61%	
IRELAND	33%	67%	
ITALY	41%	59%	
NETHERLANDS	65%	35%	
POLAND	64%	36%	
PORTUGAL	64%	36%	
RUSSIA	7%	50%	43%
SPAIN	33%	67%	
SWEDEN	50%	50%	
SWITZERLAND	68%	32%	
TURKEY	100%	0%	
UK	32%	68%	
TOTAL EUROPE	**57%**	**43%**	

The lack of board-level oversight of cyber risk in European organisations is undoubtedly one of the reasons that such a high number have failed to identify one or more cyber scenarios and/or conduct or estimate the financial impact of a cyber-attack (43% and 68%, respectively). This makes it difficult for these organisations to mitigate the risk of a cyber-attack since, without knowing what will harm the organisation most, they can't effectively direct their resources to the places where they would have the greatest impact.

In addition to this, a lack of preparedness puts them in a poor position to approach the insurance market in search of comprehensive risk transfer opportunities and to determine their value-for-money.

The majority of organisations across Europe have not arranged sources of funding that may be required in the event of a cyber-attack; however, the 33% (SEE FIGURE 5) that have is an encouraging number. Seeing as just 12% of companies are buying insurance for cyber risks, it must be the case that the remainder are bypassing the insurance market and finding alternative methods of funding (lines of credit, assets, for example).

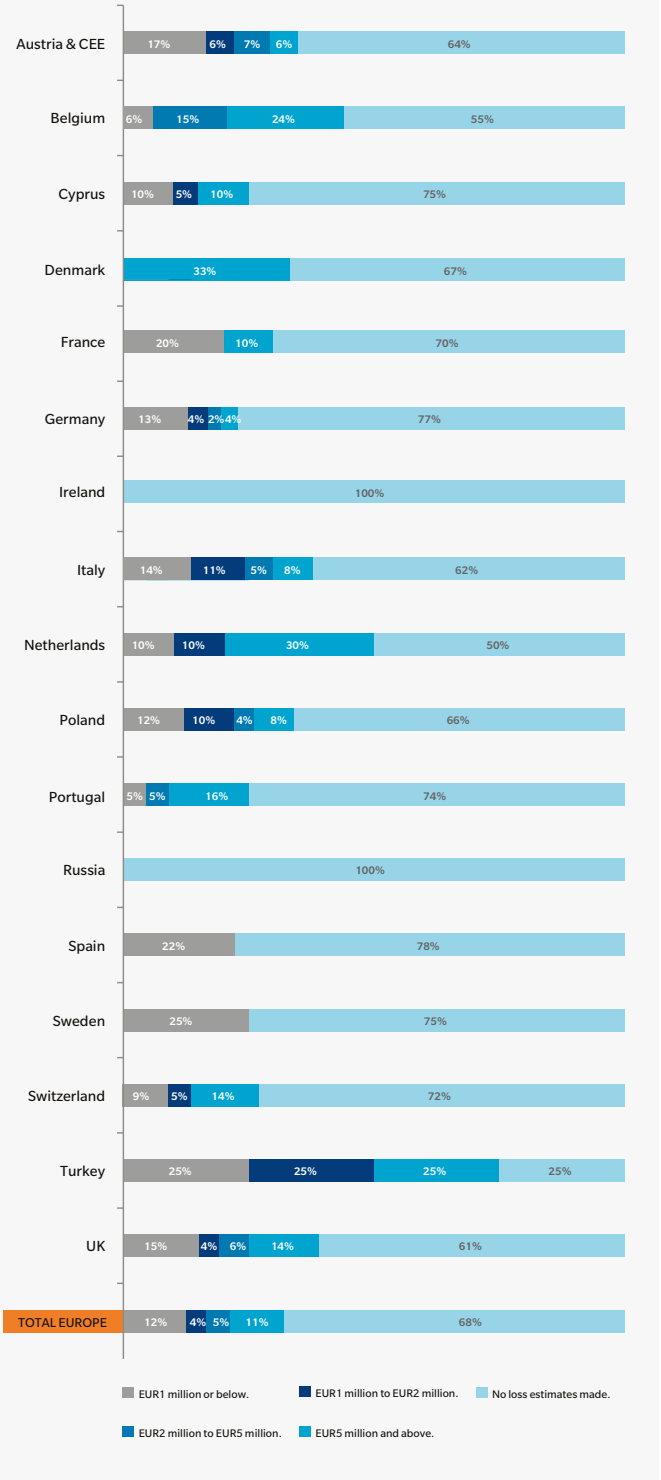
Considering the low levels of companies that have identified scenarios (57%) and conducted financial impact analysis (32%), we would speculate as to how appropriate these alternative methods of funding really are and how quickly they will respond in the event of an attack.

FIGURE 5 **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 to be accessible at the point when it is needed?***
Source: Marsh European 2015 Cyber Risk Survey

	YES	NO
AUSTRIA & CEE	25%	61%
BELGIUM	35%	41%
CYPRUS	30%	70%
DENMARK	33%	0%
FRANCE	15%	60%
GERMANY	15%	85%
IRELAND	0%	100%
ITALY	41%	59%
NETHERLANDS	45%	55%
POLAND	16%	70%
PORTUGAL	25%	64%
RUSSIA	0%	50%
SPAIN	11%	56%
SWEDEN	42%	25%
SWITZERLAND	9%	50%
TURKEY	100%	0%
UK	49%	51%
TOTAL	**33%**	**67%**

*RESULTS DISPLAYED ILLUSTRATE THE PERCENTAGE OF RESPONDENTS, NOT THE PERCENTAGE OF RESPONSES.

FIGURE 6 **Has your organisation conducted financial impact analysis or estimated the financial impact of a cyber-attack? What is the worst loss value?**
Source: Marsh European 2015 Cyber Risk Survey



The majority (61%) of organisations surveyed have some sort of crisis response plan for material cyber events. It seems surprising that such a large percentage of companies would have this high level of sophistication with regard to incident response when there is so little focus on the risk in the other areas mentioned already, including scenario testing and financial impact analysis.

Bearing this in mind, it may be the case that some of the 36% of respondents who report 'partially' having an incident response plan in place are in fact referring to a more general crisis response plan that covers multiple events, including everything from product recall to financial scandal.

FIGURE 7A Does your organisation possess an incident response plan for material cyber events?
Source: Marsh European 2015 Cyber Risk Survey

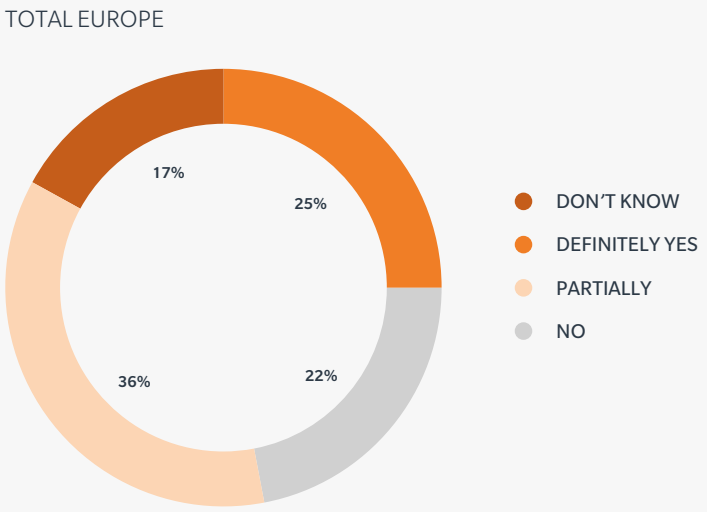


FIGURE 7B Does your organisation possess an incident response plan for material cyber events?
Source: Marsh European 2015 Cyber Risk Survey

	DEFINITELY YES	NO	PARTIALLY	DON'T KNOW
AUSTRIA & CEE	23%	19%	40%	18%
BELGIUM	35%	9%	32%	24%
CYPRUS	20%	25%	40%	15%
DENMARK	67%	33%	0%	0%
FRANCE	15%	30%	40%	15%
GERMANY	7%	44%	26%	23%
IRELAND	8%	67%	25%	0%
ITALY	27%	8%	49%	16%
NETHERLANDS	30%	20%	35%	15%
POLAND	28%	16%	42%	14%
PORTUGAL	32%	14%	39%	15%
RUSSIA	29%	0%	29%	42%
SPAIN	0%	67%	33%	0%
SWEDEN	25%	25%	42%	8%
SWITZERLAND	32%	14%	50%	4%
TURKEY	75%	0%	25%	0%
UK	31%	22%	26%	21%

LACK OF CONTROL OVER SUPPLIERS/AFFILIATES A MAJOR CONCERN

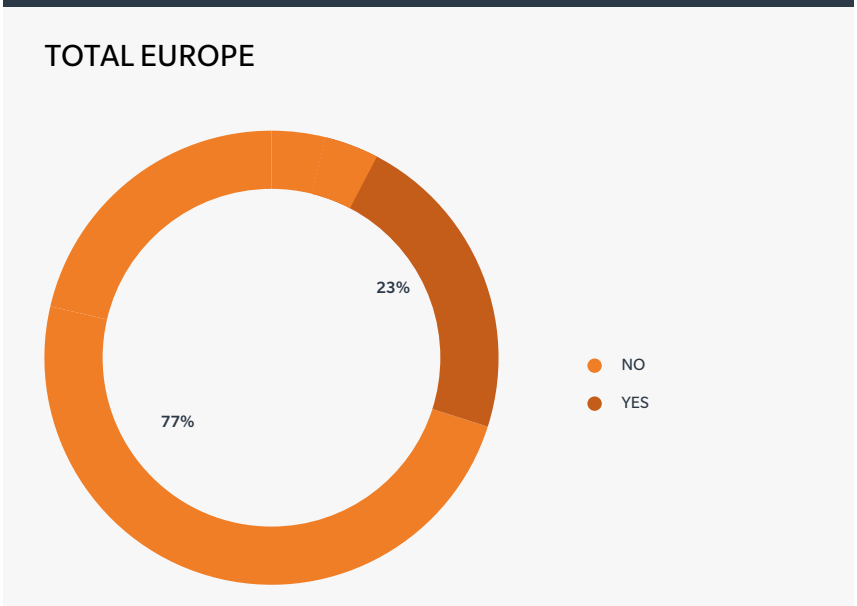
It is both a surprise and a huge concern that more than three quarters (77%) of respondents to this year's survey do not assess suppliers and/or customers they trade with for cyber risk.

Suppliers and external organisations are one of the key vulnerabilities to companies' networks. This is due to the fact that, while organisations can control their own networks, they have much less control over those of the suppliers and affiliates that they might be linked to. The findings in FIGURE 8 would appear to leave them exposed and lacking control over standards of IT security in systems where hackers might find a 'back-door' into their organisation.

Perhaps an even greater surprise is that more than two thirds of respondents (67%) are not asked to demonstrate their IT security practices to their own bank and/or customers in order to do business. For large banks in particular, we would have expected this to be standard practice.

In 2013, a well-publicised cyber breach occurred at a large US retail company after hackers stole network credentials from a third-party heating, ventilating, and air conditioning (HVAC) contractor which had an IT link with the victim's corporate systems. Incidents like these will only rise in frequency until organisations place greater focus on setting out the basic technical controls that all suppliers/contractors should have in place.

FIGURE 8 **Do you assess suppliers and/or customers you trade with for cyber risk?**
Source: Marsh European 2015 Cyber Risk Survey



SPOTLIGHT

Only
25%

of organisations possess an incident response plan for material cyber events.

THE TAKE-UP OF CYBER INSURANCE REMAINS LOW, BUT THE INSURANCE INDUSTRY'S FOCUS IS ON THE RIGHT AREAS

Nearly half (45%) of respondents' organisations are engaged with the insurance market in one way or another. With the remainder, we wonder whether this may be as a consequence of them not being in possession of the correct information to enable them to approach the insurance market and make a value-based judgment on what is available, as opposed to available insurance products not meeting their needs.

The former explanation would appear to correlate with earlier findings in the survey (SEE FIGURES 9 and 10). If this is the case, it suggests that more works needs to be done by organisations and their professional advisers – including their insurance brokers – to help improve their understanding of their cyber risk profile and demonstrate what value insurance can bring. Just one third of respondents believe that available cyber coverage options meet the needs of their organisations in one way or another; however, the majority (57%) admit to having insufficient knowledge to answer, which may be due to a lack of understanding of their firms' own risk profiles.

Perhaps the insurance industry has more to do to highlight what insurance can deliver in terms of protection, since FIGURE 11 appears to show that it is currently focussed on the right areas, namely breach of customer information (24%), business interruption (22%), and crime/fraud (12%), which represent the greatest concerns of respondents.

While there is an evident knowledge gap about firms' own risk profiles and the suitability of available cyber insurance coverage options, at least there is some recognition among respondents as to what the greatest cyber threats are. The insurance market can take some comfort in the fact it appears to be aligned with companies' biggest concerns.

FIGURE 9 **Which statement best reflects your attitude to cyber insurance based on your current knowledge?**
Source: Marsh European 2015 Cyber Risk Survey

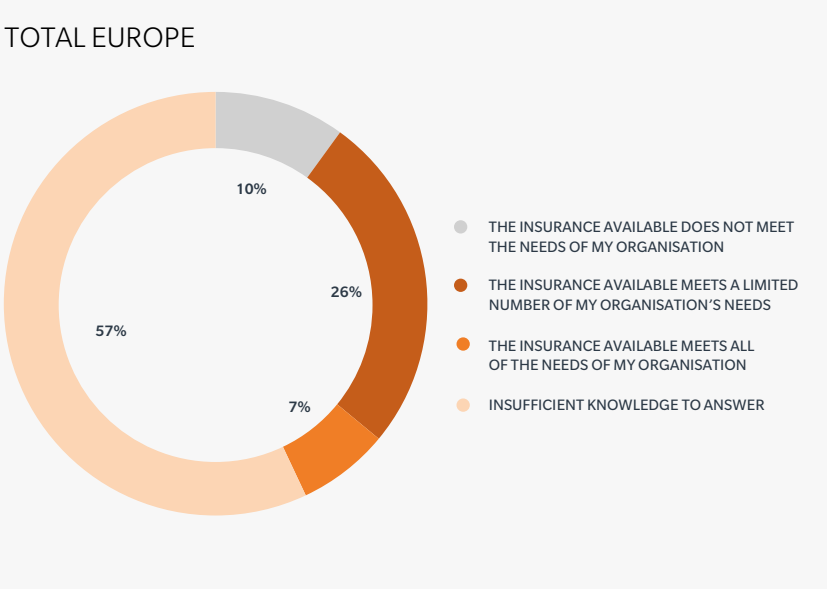


FIGURE 10 **Please indicate your organisation's current status with regard to cyber insurance.**
Source: Marsh European 2015 Cyber Risk Survey

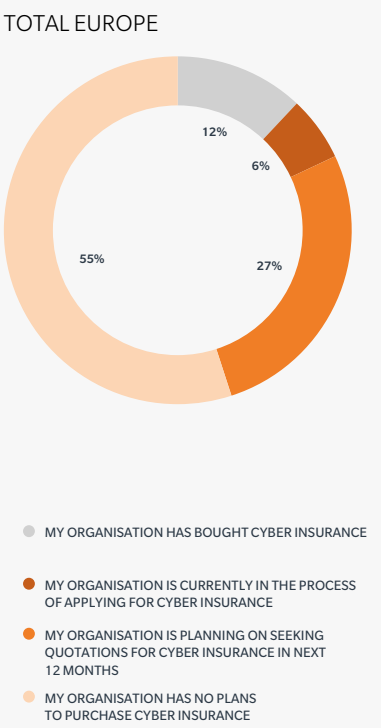
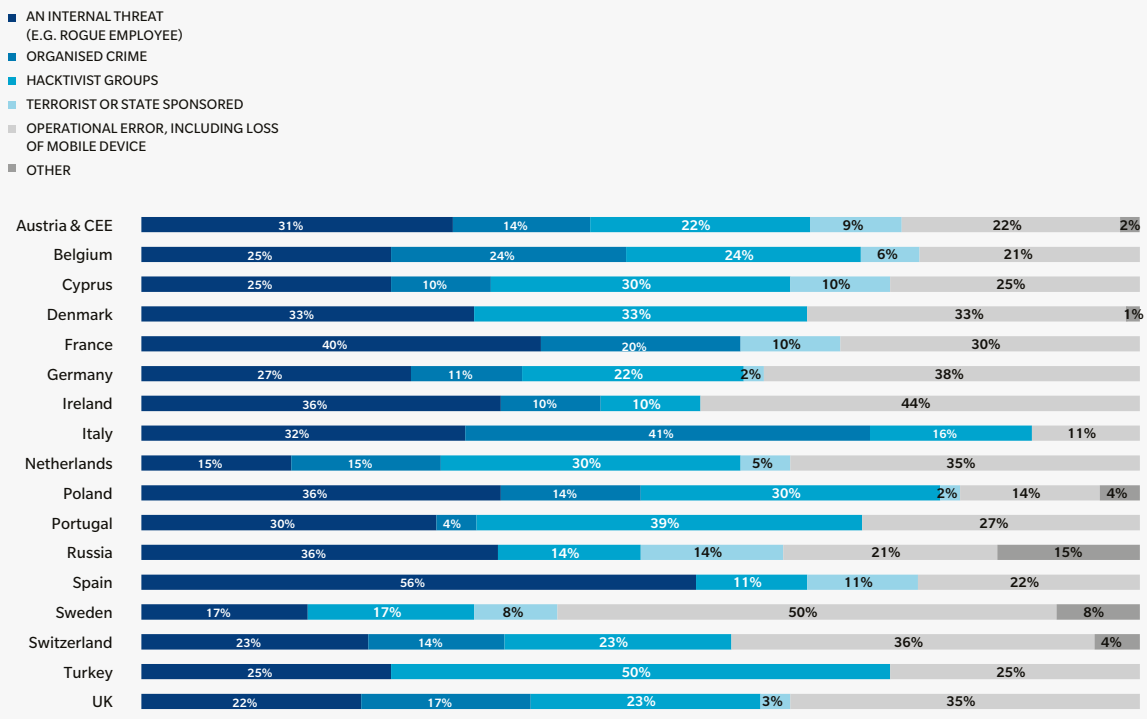


FIGURE 11 Which cyber loss scenario presents the greatest threat to your organisation?
Source: Marsh European 2015 Cyber Risk Survey

	AUSTRIA & CEE	BELGIUM	CYPRUS	DENMARK	FRANCE	GERMANY	IRELAND	ITALY	NETHERLANDS	POLAND	PORTUGAL	RUSSIA	SPAIN	SWEDEN	SWITZERLAND	TURKEY	UK	TOTAL EUROPE
BREACH OF CUSTOMER INFORMATION.	26%	12%	40%	0%	30%	11%	26%	16%	30%	34%	18%	30%	11%	25%	23%	0%	32%	24%
LOSS OF INTELLECTUAL PROPERTY.	7%	11%	5%	33%	5%	13%	0%	3%	10%	8%	7%	0%	34%	0%	13%	25%	6%	8%
BUSINESS INTERRUPTION.	17%	23%	15%	67%	0%	41%	26%	30%	20%	10%	29%	7%	33%	17%	27%	0%	22%	22%
REPUTATIONAL LOSS.	8%	24%	0%	0%	5%	4%	8%	14%	10%	12%	5%	7%	0%	8%	23%	0%	8%	9%
DIRECT FINANCIAL LOSS FROM CYBERCRIME/FRAUD.	13%	15%	0%	0%	30%	4%	16%	16%	0%	22%	5%	21%	0%	17%	9%	75%	13%	12%
DATA OR SOFTWARE DAMAGE.	10%	6%	15%	0%	15%	8%	8%	16%	15%	4%	20%	0%	11%	8%	0%	0%	6%	10%
EXTORTION.	3%	0%	10%	0%	5%	1%	0%	3%	0%	4%	0%	0%	0%	0%	0%	0%	0%	1%
LIABILITY TO THIRD PARTIES RESULTING FROM A SYSTEM BREACH.	3%	0%	10%	0%	0%	2%	0%	0%	10%	2%	9%	7%	0%	17%	5%	0%	4%	4%
PHYSICAL PROPERTY DAMAGE AND BODILY INJURY.	1%	0%	0%	0%	0%	1%	0%	0%	5%	0%	0%	7%	0%	0%	0%	0%	1%	1%
INSUFFICIENT INFORMATION TO ANSWER.	12%	9%	5%	0%	10%	15%	16%	3%	0%	4%	7%	21%	11%	8%	0%	0%	8%	9%

FIGURE 12 Where do you view the greatest threat to your organisation originating from?
Source: Marsh European 2015 Cyber Risk Survey



CONCLUSION

Despite European organisations placing a greater focus on cyber risks in the past 12 months, clearly there is still a considerable amount of investigation required by many in order to improve their understanding and management of cyber risk.

Part of the solution to this lies in moving responsibility for cyber away from IT departments and into the boardroom. Only with board-level buy-in can companies identify business-critical areas and undertake scenario testing and financial impact analysis to build up their cyber risk profile, enabling them to mitigate and/or transfer the risk accordingly.

On a positive note, when these organisations have carried out the assessment and quantification of the risk, they will be able to choose from a suite of relevant insurance products focussed on their main areas of concern, namely breach of customer information, business interruption, and crime/fraud.

One particular finding of this report that deserves special attention is the high level of organisations (77%) that do not assess suppliers they trade with for cyber risk. For all the proactive steps taken and money invested to prevent cyber-attacks occurring within their own organisations, a security breach at a contractor or supplier, for example, could potentially undo all of that.

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.

MARSH