MARSH

Continental European Cyber Risk Survey: 2016 Report

FOREWORD

Cyber risk is at the forefront of conversations across organisations, regularly hitting global headlines as a result of a rising number of threats. Virtually every business, no matter what the industry, is dependent on information/operational technology to run its critical business processes and to store important information, meaning no company or industry is immune to cyber risk.

I am pleased to share the findings of our *Continental European Cyber Risk Survey: 2016 Report.* When comparing the data with last year's results, we noted a modest degree of progress in some of the indicators, but had to conclude that much work still needs to be done in terms of cyber risk awareness. I would like to call a few key areas to your attention.

In 2015, an overwhelming majority (79%) of organisations had, at best, a basic understanding of their cyber risk profiles leaving only 21% of organisations with a complete understanding. In 2016, that number went up to 31%.

Last year, just 23% of organisations surveyed did not consider cyber risk to be material enough to even get on to their corporate risk register. That dropped to 9% in 2016. This year, 73% of organisations indicated that cyber is now on their register, with 32% featuring it in their top-five.

The fact that 60% of organisations have never conducted or estimated the financial impact of a cyber loss scenario, and that 59% have no plan in place to access funding in case of a loss, represent points of concern.

IT departments continue to take primary responsibility for cyber risk in the majority of organisations. We are expecting the board and risk management functions, alongside the most senior members of a management team, to assume greater responsibility for cyber risk. Cyber is a business risk – not a technical one. We recommend that boards conduct regular reviews to ensure that management has taken ownership of the cyber threat.

With its rapidly evolving nature and severity, cyber risk should be managed actively by all key stakeholders. Close public-private partnership will lead to a greater understanding of the impact of cyber risk as well as developing efficient methods to combat it.

I hope you will read the findings of our 2016 report with interest and that it will help you to identify areas which may need greater focus. In order to build-up greater resilience to cyber risk and to embed efficient cyber risk management culture in organisations, we all need to make necessary investments now. It is crucial to protect your business and your clients from the changing nature and magnitude of cyber risk.

Flavio Piccolomini
CEO Continental Europe and Africa

CONTENTS

INTRODUCTION

With the EU General Data Protection Regulation (GDPR) on the horizon – which will oblige companies operating in Europe to report data breaches to national authorities within 72 hours or otherwise risk heavy fines – appreciating the current perception of cyber risk is vital.

Marsh has united its knowledge and expertise on the subject to launch a study into organisations' attitudes towards the threat cyber risks pose, processes in place to manage them, and overall understanding and use of cyber insurance as a means of risk transfer.

This report gathers data from both risk and finance professionals in large and medium-sized corporations across Continental Europe.

Containing 15 questions relevant to the cyber issues of today, the survey is an excellent reference point thanks to pertinent data from around the continent. Readers can gain a more profound understanding of the level of awareness companies possess regarding cyber risks and whether business resilience is being compromised by a lack of cyber protection.

BOARDROOM DISCUSSION

- Cyber risk continues to rise up the boardroom agendas of European organisations.
- However, they still hold a limited understanding of the risk and their degree of exposure.
- Human error is perceived to be the most probable threat to organisations, while operational error is identified as the most impactful.

PROGRESS IN TERMS OF AWARENESS BUT RESPONSIBILITY NEEDS TO BE ASSUMED ACROSS THE ORGANISATION

Concerns about cyber-attacks have grown and this has led to a greater appreciation in organisations, right up to boardroom level. And while the figures are an improvement on 2015, they nonetheless demonstrate that a substantial amount of work needs to be done in order to align perceptions with the realities of cyber risks.

Just under one third (31%) of organisations have a complete understanding of cyber risk. This is a rise of almost 50% compared with 2015 (21%), principally indicating a greater yearning among organisations to comprehend their exposure to these risks (see Figure 1).

However, the figure is still relatively low considering that 61% of the organisations feel they have a limited understanding, illustrating that awareness and management of cyber-attacks needs improvement. It also leaves them badly placed when needing to prioritise their risk mitigation efforts and risk transfer strategies.

The increased awareness and understanding of cyber risk is reflected in a greater presence among companies' corporate risk registers. The appearance on the corporate risk register means that management, the board, and key stakeholders will be provided with significant information on the risk in question, ensuring that they understand the nature and extent of the risks the business faces.

Almost a third of companies (32%) advised that cyber risk is amongst the top-five on the risk register, a big rise on the 19% who last year placed it in the same bracket. A further 41% of companies included it somewhere on their risk registers, and just 9% advised that cyber risk was not present at all – down from 23% in 2015 (see Figure 2).

These encouraging figures demonstrate that cyber risk is becoming an increasingly important part of companies' risk strategies, meaning greater mapping and quantification of the risk, and evaluation of their ability

32%

of companies advised that cyber risk is amongst the top-five on the risk register.

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

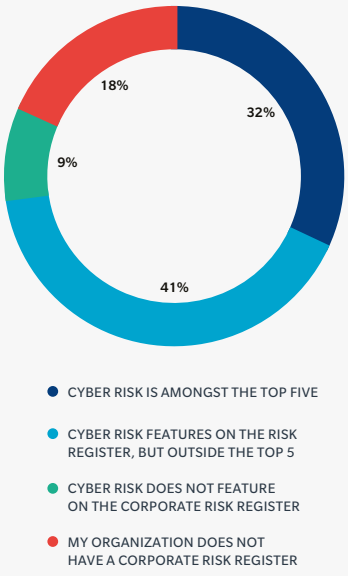
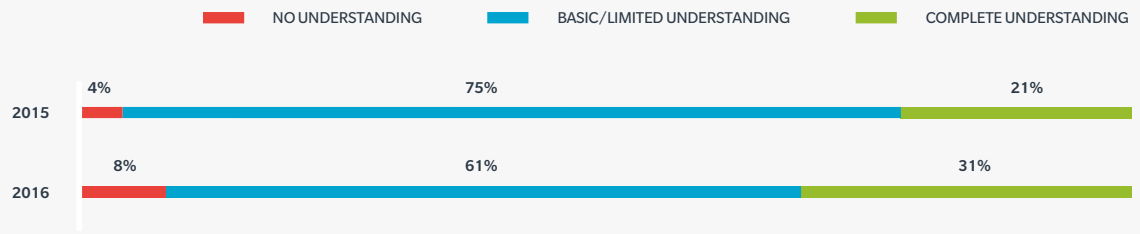


FIGURE 1 **To what extent do you believe your organisation has an understanding of its exposure to cyber risk?**
Source: Marsh Continental European Cyber Risk Survey



to manage it. Those risks high up on the corporate risk register will be identified and prioritised, ensuring those with the greatest probability or the greatest potential loss are handled first.

Companies are starting to mitigate the threat posed by cyber risk not just acting on technical measures but ensuring that the process of ascertaining the value, and therefore suitability, of available risk transfer options less problematic.

Inclusion in the corporate risk register is an important step but its simple presence is not enough. We see many companies develop risk registers and stop there in their efforts at risk management. The risk register is the first step in the risk management process – not the last.

Continental Europe witnessed little change in terms of where the responsibility lies in reviewing and managing cyber risks:

IT departments are primarily responsible in 68% of cases across the region.

The board retains primary responsibility in just 14% of cases, suggesting that even while the risks posed by cyber threats are now being taken far more seriously across organisations, their boards are still not taking ownership of the risk (see Figure 3).

The technical nature of cyber – moreover, data security – is an important consideration, but it needs to be judged more as a business risk, with the potential to result in operational disruption, physical damage, and perhaps most important of all, reputational and brand damage.

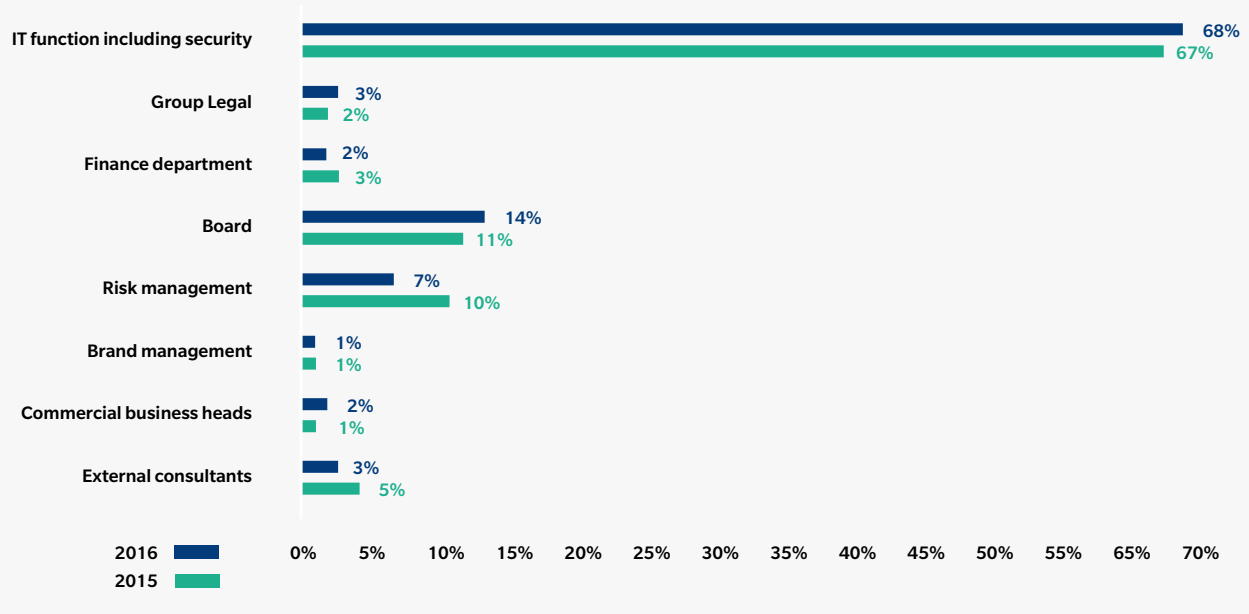
With a clearer perception of the risks posed by cyber and its growing presence on corporate risk registers, the overall situation has witnessed an improvement since 2015.

There is, however, more work to be done. Less than a third of organisations have placed it amongst the top-five in their corporate risk registers, and only a minority have a complete understanding of cyber risk itself.

The fact that few organisations have made their boards responsible for the review and management of cyber risks is concerning.

Figure 2 indicates that the risk is being taken seriously; however, Figure 3 shows that it is still largely regarded as a technical risk - as opposed to a business one. IT departments remain largely responsible for cyber, and while they will know how to implement cyber security, they are not in a position to identify business-critical elements nor map the potential operational and financial impacts a cyber event could have.

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 Continental European Cyber Risk Survey



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

Companies' ability to measure the potential impact of cyber risks, and consequentially the overall level of preparedness in case of an attack, has not improved since 2015.

Cyber risks are far different from those typically faced by organisations, given their ability to change and transform continuously. Increasing digitalisation and interconnectedness are exposing organisations more frequently to more sophisticated kinds of cyber threats. Each and every organisation faces multifaceted cyber risks, both internal and external, from data breaches right down to theft of funds, and as such it is highly recommended that a plan is in place, preferably by the board. Organisations should assume that they will be breached: It is not a case of if, but when.

With primary responsibility sitting with IT, this largely excludes the organisations' other functions, which could potentially compromise risk management. Survey results indicate that little over half of organisations have identified cyber loss scenarios that could affect them, with a considerable 48% having never pinpointed any such scenario – an increase over last year's 45% (see Figure 4).

While being proactive in the face of such a complex risk is advisable, a substantial number of organisations have not made any estimate of the financial impact of a cyber event. In a world in which the estimated annual cost of cybercrime to the global economy is at USD445 billion[1], it is particularly worrying that, while little over half have identified loss scenarios, just 40% have estimated the potential financial impact. This corresponds with the mere 40% that have a plan in place to access appropriate funding in case of a financial loss, leaving the remainder exposed in the event of a cyber-attack (see Figures 5 and 6).

14%

of organisations have made their boards responsible for the review and management of cyber risks.

Only 40%

have estimated the potential financial impact of a cyber loss scenario.

FIGURE 4 **Have you identified any cyber loss scenarios that could affect your organisation?**
Source: Marsh Continental European Cyber Risk Survey

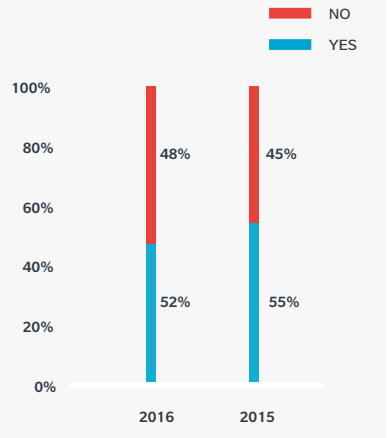
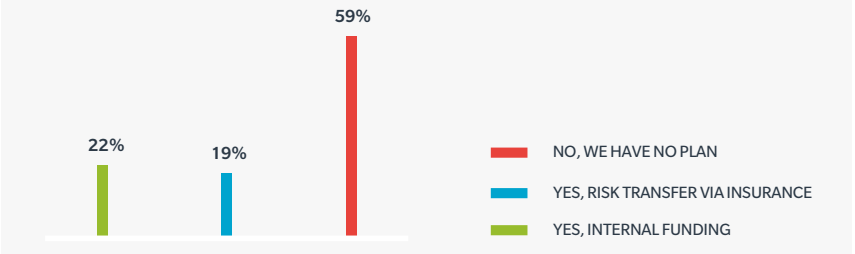


FIGURE 5 **In case of cyber loss, does your organisation have a plan in place to access appropriate funding?**
Source: Marsh Continental European Cyber Risk Survey



[1] *Net Losses: Estimating the Global Cost of Cybercrime, McAfee, USA 2014.*

With hackers potentially attacking your network, criminals attempting to extort you, and rogue, disgruntled employees taking malicious action, cyber-attacks often bear financial repercussions and reputational damage. However, just 40% of companies possess an incident response plan for cyber events, down from 61% in 2015 who had at least partially planned for such an occasion. The lack of assessment in terms of identification, quantification, and analysis means that these organisations' risk profiles are not being adequately updated in order to manage cyber risks, either in terms of prevention or preparation (see Figure 7).

Having such a dedicated incident response/crisis management plan in place has been proven to have a very positive effect on the operational, financial, and reputational impact of a cyber-attack.

However, year-on-year results demonstrate that, as of yet, organisations are not adequately prepared. The cyber threats that many companies previously considered to be unthinkable are now regularly in the news and, as such, the need to promote a proactive rather than a reactive approach so that they are prepared to deal with an incident strategically and minimise the overall damage.

FIGURE 6 If your organisation has conducted or estimated the financial impact of a cyber loss scenario, what is the worst potential financial loss?
Source: Marsh Continental European Cyber Risk Survey

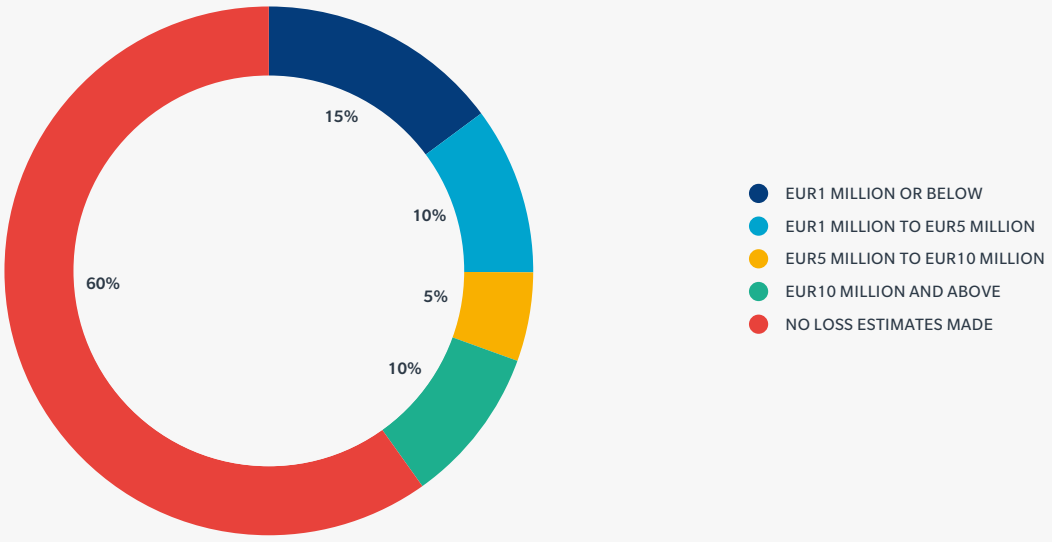
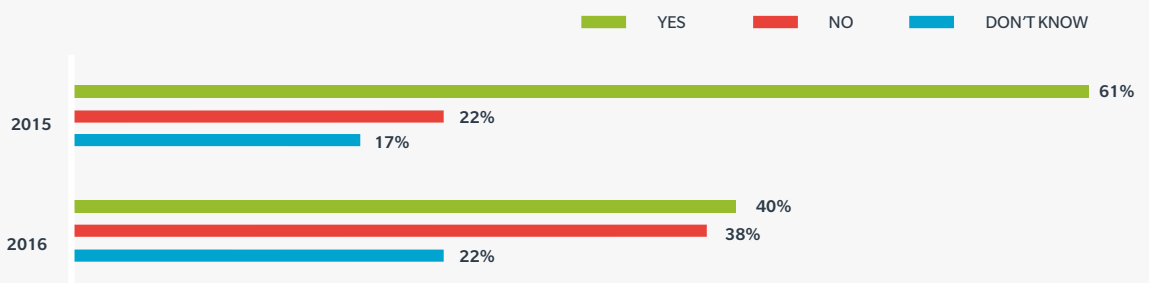


FIGURE 7 Does your organisation possess an incident response plan for cyber events?
Source: Marsh Continental European Cyber Risk Survey



CYBER INSURANCE TAKE-UP ON THE RISE AS FEARS OF BUSINESS INTERRUPTION DOMINATE

The procurement of cyber insurance is on the rise, with nearly half of organisations (47%) who responded to our survey either already covered by a policy or intending to purchase one over the next 12 months. The remaining 53% is likely to be formed largely of those companies that are lacking the necessary information in order to make a value-based judgment on transferring the risk (see Figure 11).

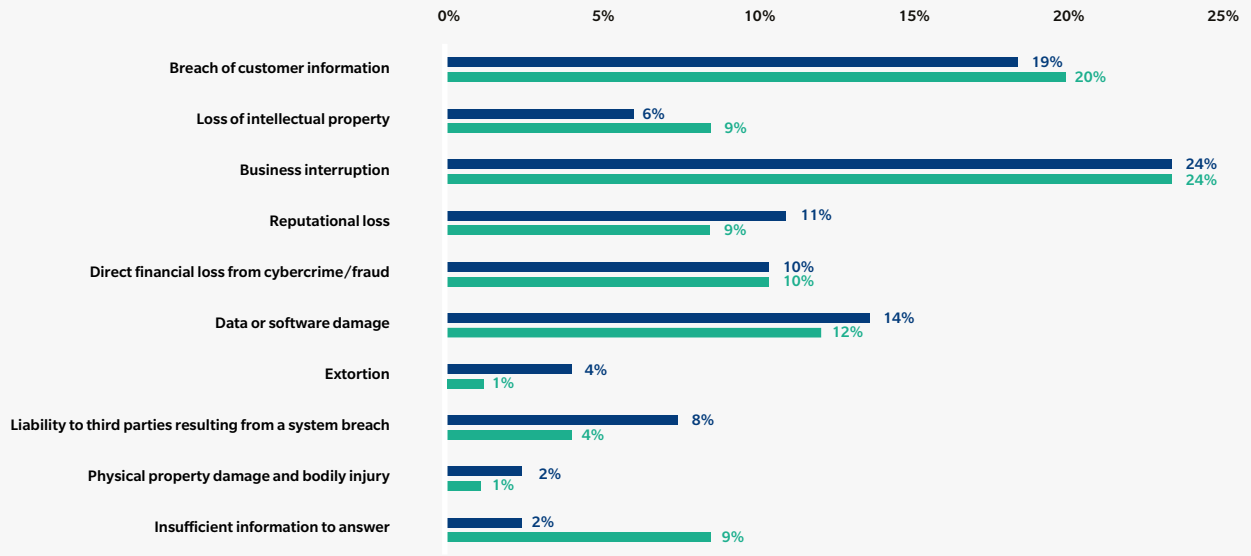
Interest in cyber insurance has been high in the US now for some time due to regulatory requirements to report cyber breaches. Take-up in Europe, on the other hand, has been more modest; however, it is catching up. In 2015, 20% of surveyed organisations confirmed that they had either bought cyber insurance or were in the process of applying for it. In 2016, we see the number go up to 24%, with another 23% planning on seeking quotations for cyber insurance in the next 12 months. We have observed an 80% increase in Marsh clients purchasing standalone cyber insurance in Continental Europe, mostly by financial services; communications, media, and technology; retail; and, more recently, manufacturing clients.

Earlier in the report we found that 61% of organisations have a limited understanding of their exposure to cyber risks and this is further reflected by the fact that 57% of respondents believe they have insufficient knowledge as to whether current cyber insurance offerings meet the needs of their company. In fact, just 8% signalled that cyber insurance definitely does not meet those needs (down from 10% in 2015; see Figure 9).

24%

of organisations view business interruption as the number one threat ahead of breach of customer information (19%).

FIGURE 8 **Which cyber loss scenarios present the greatest threats to your organisation?**
Source: Marsh Continental European Cyber Risk Survey



Organisations must work to improve their understanding of their cyber risk profiles and to quantify the risk. This will, in turn, enable them to place a value on the risk transfer options currently available to them in the marketplace.

Organisations recognised a wide range of threats, with business interruption (24%) ahead of breach of customer information (19%) as the number one threat deriving from cyber loss scenarios. Recent high-profile cyber-attacks, after which companies have seen their operations disrupted, have raised public awareness of their capability to impact daily business. Both of these threats can be covered against in a basic cyber policy, a promising sign that the insurance market is focusing on the right areas (see Figure 8).

Concern about reputational loss has increased, with 11% of organisations citing it as the greatest threat to their organisation (up from 9% in 2015). This was prompted by prominent cyber events where companies have been hugely impacted in terms of brand and reputational value. Data or software damage (14%, up from 12%) and direct financial loss from cybercrime/fraud (stable at 10%) completed the top-five.

As in 2015, operational error is considered to pose the greatest potential impact to organisations, particularly including concerns persisting relating to a cyber-attack bringing down entire servers, with 33% of organisations listing it as the most likely to occur, and 27% rating it as the threat which could bear the greatest impact on their company (see Figure 10).

And indeed employee, or human, error – including loss of mobile and other devices – comes top in terms of probability, and third in terms of impact. This category, new for the 2016 survey, reflects the very distinct possibility of devices afforded to employees getting lost

FIGURE 9 **To the best of your knowledge, cyber insurance available...**
Source: Marsh Continental European Cyber Risk Survey

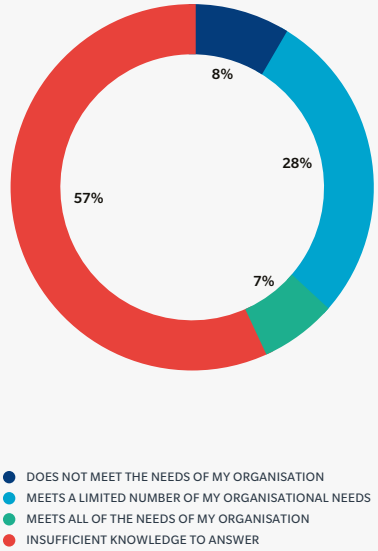
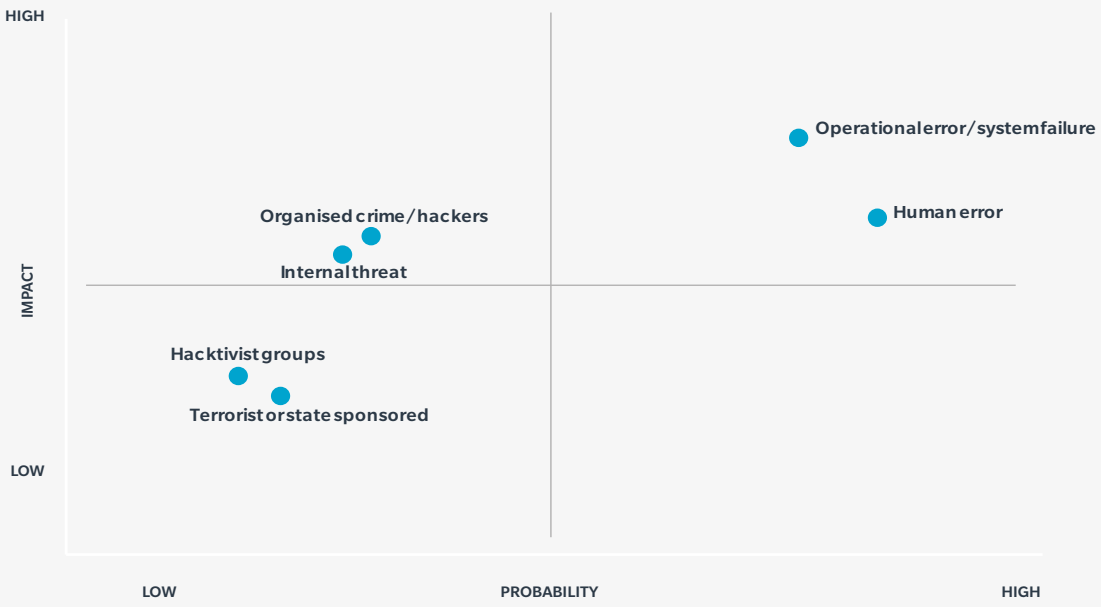


FIGURE 10 **Threats to organisations: potential impact versus perceived probability.**
Source: Marsh Continental European Cyber Risk Survey



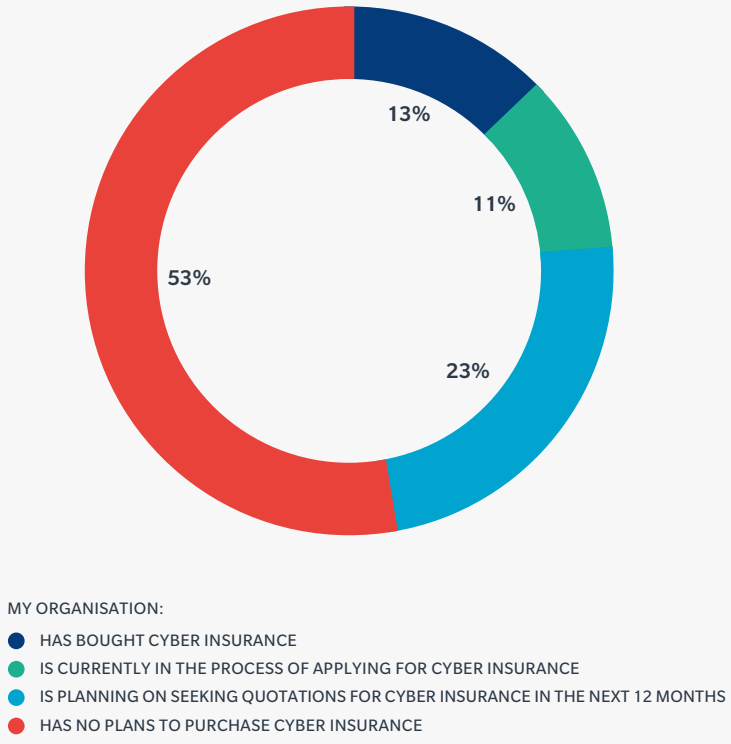
or an employee clicking a seemingly innocuous but ultimately very harmful ransomware or phishing link via their work email account.

Organised crime rose in terms of potential impact (up to 22% from 15% in 2015) but fell in probability (from 15% to 10%), reflecting perhaps an increased level of IT security awareness amongst organisations. The threat posed by hacktivist and terrorist/state sponsored groups was seen as negligible.

Internal threats such as employee sabotage also fell both in terms of impact and probability.

Respondents demonstrated a knowledge gap, particularly when taking into account their own risk profiles and suitability of available cyber insurance coverage options. However, the clear-cut recognition as to what the greatest cyber threats are and indeed their sources shows alignment between what the insurance market offers and companies' concerns.

FIGURE 11 **Please indicate your organisation's current status with regard to cyber insurance.**
Source: Marsh Continental European Cyber Risk Survey



PREMIUM VOLUMES

Globally, we estimate the size of cyber insurance premium to be around USD3.5 billion with USD3 billion coming from the US, and around USD300 million coming from Europe. With cumulative average annual growth in the range of 25% to 35%, the global cyber market is expected to reach USD7.5 billion by 2020. Once the EU General Data Protection Regulation is formally implemented, we are expecting European cyber premium volume to equal the size of the US cyber market.

SUPPLIERS CONTINUE UNCHECKED AS STAKEHOLDERS DEMAND GREATER SECURITY STANDARDS

Up and down the supply chain, organisations may utilise hundreds of different suppliers as part of their daily operations. And each supplier brings their own set of cyber-related risks linked to the entire company.

Just 20% of organisations actively appraise suppliers in order to assess and manage potential risks, identifying, quantifying and analysing them before setting out a strategy to prevent or at least prepare for them (see Figure 12).

This widespread exposure to third parties comes on the back of a rise in stakeholders who are now requiring companies to demonstrate certain standards of IT security, from banks to regulatory bodies via final customers. In 42% of cases, an organisation has been asked to provide guarantees for the level of IT security, up from the 29% in 2015 (see Figure 13).

The rise is not surprising, and this upward trend is expected to continue as more and more businesses become increasingly reliant on IT systems and computer-enabled processes. Combined with the overall increased awareness witnessed in Section 1 of this report, organisations will progressively need to gear themselves towards a greater overall focus on defining key cyber risks.

FIGURE 12 **Do you assess key suppliers you trade with for cyber risk?**
Source: Marsh Continental European Cyber Risk Survey

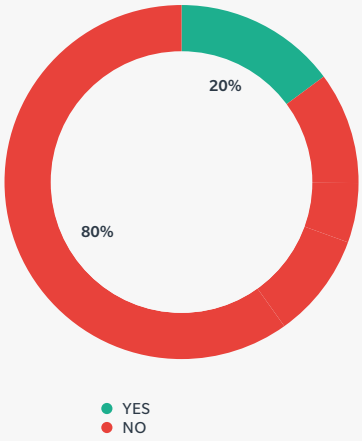
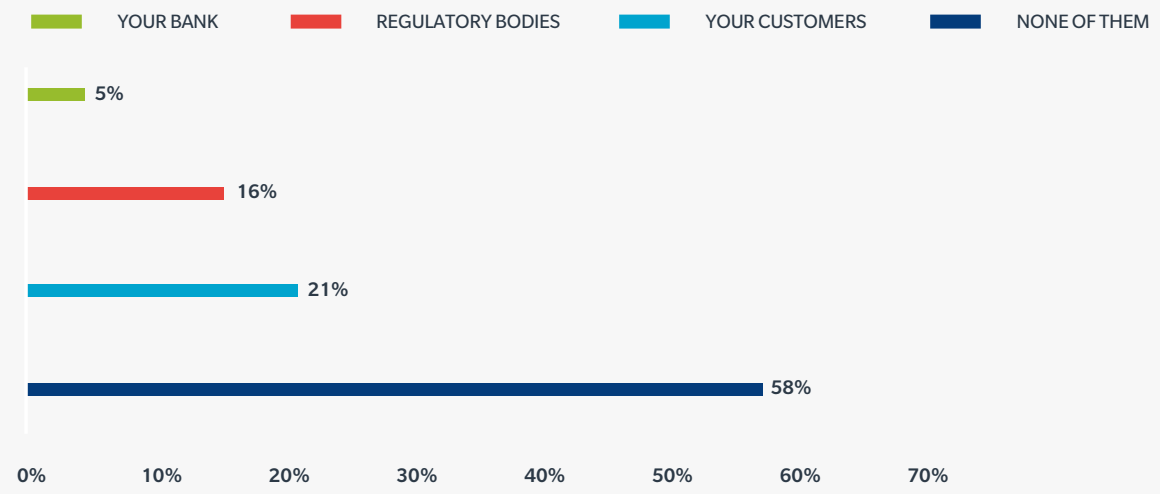


FIGURE 13 **Have any of the following required you to demonstrate a certain standard of IT security?**
Source: Marsh Continental European Cyber Risk Survey



CONCLUSION

From an overall cyber risk management perspective, Continental European companies have increased their awareness of and proactivity with regards to addressing cyber threat. When comparing the data with last year's results, we noticed a positive evolution in some of the indicators, but had to conclude that much work still needs to be done in terms of awareness and ownership of cyber risk.

Many companies continue to delegate ownership of cyber risks to technical functions and, conversely, the complexity of cyber/IT risk universe is not attracting sufficient interest from other stakeholders in the organisation, including risk managers and insurance buyers.

While formal implementation of the EU General Data Protection Regulation and the NIS Directive is still more than a year away, the Continental European cyber scenario continues to be different from that in the US, where risk managers cannot afford to ignore the transfer of cyber losses to insurers. At the same time, risk managers understand that cyber-attacks could result in prolonged service disruption. However, the estimate of business interruption losses is, in the majority of cases, neither routinely done nor requested by senior management.

Despite greater focus shown by Continental European organisations to improve their understanding and management of cyber risk, they need to do more to identify cyber loss scenarios, understand the impact on the business, and adopt cyber risk financing strategies. Insurance is not yet utilised widely enough as a risk transfer and financing mechanism.

The focus must now fall on building-up greater cyber risk resilience in organisations, and this needs to be led by senior management. Cyber risk is constantly transforming and protecting the interests of both your business and your clients is imperative.

APPENDIX 1: CYBER RISK ASSESSMENT MATRIX

	INTERNAL	EXTERNAL
MALICIOUS	• Unauthorised system access by internal actor. • Unauthorised system access by internal actor resulting in manipulation of operations technology (OT). • Rogue employee purposely introduces malicious code into product embedded software. • Internal colleague releases, destroys, steals, or corrupts confidential data. • Unauthorised system access allows the creation of false transactions.	• Unauthorised system access by external actor. • Unauthorised system access by external actor resulting in manipulation of OT. • Computer virus, malware, or similar introduced, for example, by phishing. • Encrypting key data, etc. • Valid threat to release, destroy, corrupt, steal data, or introduce virus/malware, etc. • Phishing to gain banking access credentials from employees.
NON-MALICIOUS	• Operational error of authorised personnel. • Lost or stolen paper records or computing device. • Transmission of a computer virus, malicious code, or similar to a third party. • Use of owned or operated network to perform a denial of service (DOS) attack against a third party. • Digital media content is found to be defamatory or infringes another's intellectual property rights.	• Introduction of computer virus or malware by vendor or customer. • Vendor supplies component parts that are infected with virus/malware, etc. • Vendor or customer releases your confidential data in their control. • Operational error of vendor or customer impacts your IT or OT network.

APPENDIX 2: GENERAL DATA PROTECTION REGULATION

GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR came into effect on 24 May 2016 with a two-year implementation period.
The key points of this new piece of legislation are as follows:

- Fines increase to the greater of EUR20 million or 4% of global turnover.
- Single lead regulator for enforcement action.
- Extra-territorial scope – covers all organisations gathering data on EU citizens, not just EU companies.
- Explicit consent required to collect personal information.
- New restrictions on the profiling of data subjects.
- Requirement for organisations to be able to demonstrate and verify compliance.
- Requirement to appoint a data protection officer if the organisation processes in excess of 5,000 data-subject records annually.
- Data privacy impact assessments are required for certain new or changed products and services.
- Organisations are required to notify both the regulator and data subjects "without undue delay" of a data breach.
- New and enhanced rights for data subjects, including the right to erase and subject access rights.

About this Continental European Cyber Risk Survey: 2016 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 Continental Europe, the practice:
- Maintains close relationships with EU institutions and local authorities.
- Manages premium volume in excess of EUR 25 million. (Continental Europe is a key market for cyber insurance after the US).
- Has more than 20 cyber risk experts dedicated to serving clients across the region.

At Marsh, we have a proven track record of helping our European clients of all kinds (irrespective of sector or size) 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 European 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 Europe can benefit from access to our global team - named for the third year in a row, as best cyber broker[2] - which works out of more than 30 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 our financial and professional 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:
- Unique online self-assessment tool – www.marsh-stresstest.eu
- Quantification of cyber scenarios (through big data, for instance)
- Coverage gap analysis
- Cyber placement benchmarking
- Enhanced cyber insurance policy wordings (including our unique broker wording).

[2] *Advisen Cyber Risk Awards 2016.*

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

For more information, contact the colleagues below or visit our website at:
www.marsh.com.

JEAN BAYON DE LA TOUR

Cyber Development Leader,
Continental Europe
+33 1 41 34 50 05
Jean.bayondelatour@marsh.com

NILAY OZDEN

Managing Director, FINPRO Practice Leader,
Continental Europe
+44 (0)7825 228454
nilay.ozden@marsh.com

CORRADO ZANA

Business Resilience Regional Leader,
Continental Europe
Marsh Risk Consulting
+39 3469498790
Corrado.Zana@marsh.com