MARSH

MARSH REPORT | September 2016

UK Cyber Risk Survey Report: 2016

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

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 data in this report was collected from both risk and finance professionals in large and medium-sized corporations across the UK.

The study provides pertinent data and reference points against which readers can assess their position.

BOARDROOM DISCUSSION

Spotlight on Cyber Risk to UK Companies

30.3%

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

75%

of organisations do not have a "complete" understanding of cyber risk.

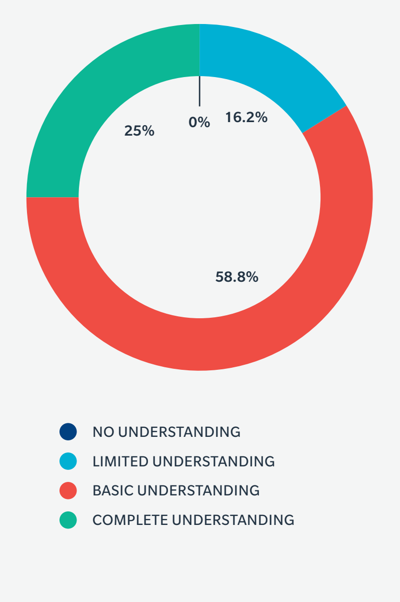
55.9%

of UK companies are engaged with the cyber insurance market.

SECTION 1: AWARENESS OF CYBER RISK ON THE RISE, ALTHOUGH STILL WORK TO BE DONE

Cyber incidents continue to increase in frequency and sophistication[1]. This, together with a series of high-profile cyber-attacks that have taken place over the past 12 months, has contributed to the elevation of cyber risk to the top of boardroom agendas.

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



Levels of understanding around cyber risk have increased compared to last year, with 83.8% of respondents having a basic or complete understanding of their company's exposure to cyber risk compared to 60.8% last year.[2]

This increase suggests that a series of recent high-profile cyber incidents has resulted in UK organisations recognising that cyber risk is serious; however, the fact that as little as one-quarter of respondents believe their organisations to have a complete understanding suggests there is still a lot of work to do to improve understanding and management.

The next step for the majority of respondents whose companies have a basic understanding is to conduct in-depth analysis into the issues, involving multiple groups within the organisation, including information technology (IT), executive management, legal, and risk management. Forming a cross-disciplinary team of colleagues to focus on identification of the risks and the impacts they may have on your business is an important first step you should take. However, from discussions with UK organisations, we don't yet see a large proportion making this commitment, so the survey findings are consistent with our experience.

Nevertheless, the overall increase in risk understanding is up consistently across the board, and it may be possible to explain this from the results in FIGURE 2, which shows a similar rise in the percentage of companies placing cyber risk on their risk registers. More than half of companies represented by respondents to this year's survey (71.8%) place cyber as a top-five or top-10 risk on their corporate risk registers compared to 45.8% in 2015. Naturally, those that place cyber in their risk registers are likely to undertake a more thorough investigation and, therefore, a greater understanding, of cyber risks.

Developing an accurate picture of the risks that an organisation faces via a risk register is a significant step in the risk management process. What happens next, of course, is crucial. We see many companies develop good 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.

[1] *Internet Security Threat Report, v. 21, Symantec, April 2016.*

[2] Comparisons are with the *2015 UK and Ireland Cyber Risks Survey*, Marsh, London, June 2015.

FIGURE 2
Where does cyber risk feature on your corporate risk register?
Source: Marsh Cyber Survey

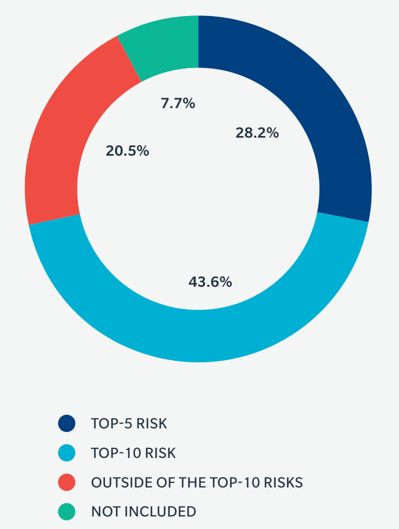
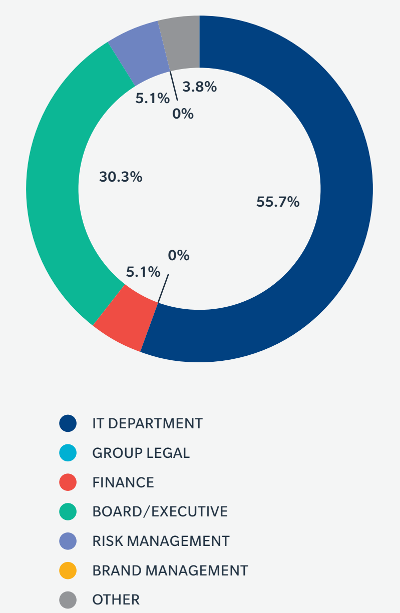


FIGURE 3
Please indicate which of the following potential stakeholders takes primary responsibility for the review and management of cyber risks in your organisation.
Source: Marsh Cyber Survey



Another positive finding of this survey is that board-level ownership of cyber has increased by more than 50% (from 19.4% in 2015 to 30.3% this year). This would suggest that, as high-profile events, government initiatives, and legislation have pushed cyber to the top of boards' agendas, they are increasingly taking ownership of the risk, further illustrating that cyber has increasingly evolved into a business risk as opposed to a technical matter.

Today, it is no longer just about data security – although obviously this remains a key issue – it has the potential to result in operational disruption, physical damage, bodily injury, and perhaps most important of all, reputational and brand damage.

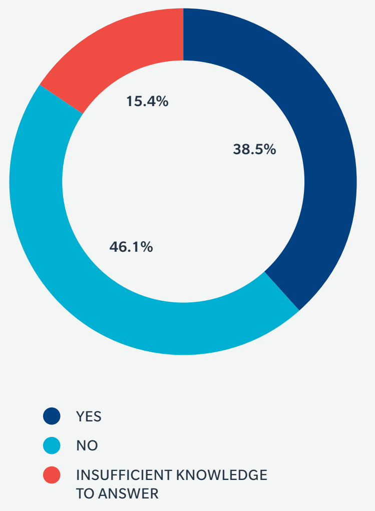
When looked at together, FIGURES 1, 2, and 3 would suggest that boards are taking greater control of the issue and communicating its importance down to the rest of the organisation. However, this is the case in less than a third of organisations, demonstrating there is still a lot of work to be done.
IT departments remain responsible for review and management of cyber risks in the majority (55.7%) of organisations. While IT departments might know how to implement cyber security, they will not be able to identify business-critical elements and, therefore, map the potential operational and financial impacts an event could have.

> As high-profile events, government initiatives, and legislation have pushed cyber to the top of boards' agendas, they are increasingly taking ownership of the risk.

SECTION 2: COMPANIES UNABLE TO MEASURE THE IMPACT OF CYBER THREATS

Roughly in line with last year's report (40.3%), 38.5% of respondents say their firms have experienced a cyber-attack in the past 12 months (see FIGURE 4).

FIGURE 4
Has your organisation been subject to a cyber-attack in the past 12 months?
Source: Marsh Cyber Survey



This is a markedly low percentage in comparison with other statistics. The recent *Cyber Security Breaches Survey 2016* report published by the UK Government, for example, found that 65% of large organisations and 51% of medium organisations have suffered a security breach in the past 12 months.[3]

Perhaps unsurprisingly, 15.4% of respondents felt they had insufficient knowledge to answer this question. This may be because of the fact that it is not always clear what a cyber-attack really is – there are so many ways cyber risk can manifest itself in an organisation that it can often create confusion in terms of how to define it. One useful method can be to place a cyber event into an assessment matrix, which is split into four categories divided between malicious and non-malicious on one axis and internal and external sources on another boundary (see APPENDIX 1). Such a tool can help organisations to think through the types of cyber events that are likely to befall them and to create some initial scope for the cyber risks they may face.

Interestingly – and despite the findings in section 1 of this report suggesting greater awareness of cyber risk compared with 12 months ago – the percentage of organisations that have conducted or estimated the financial impact of a cyber event (35.4%) has actually reduced (from 39.9% in 2015).

This may suggest that, despite it being made clear in section 1 that an increasing number of UK organisations are identifying the risk, they still have some way to go in terms of applying basic risk management techniques, such as impact measurement and quantification of potential losses. Conducting financial impact analysis is the next step for these organisations and one which is necessary to put them in a strong position to eventually mitigate and/or transfer the risk.

Loss severity analysis for cyber risk requires well-developed loss scenarios that include enough detail to be able to identify the specific financial impact on the organisation.

[3] *Cyber Security Breaches Survey 2016*, UK Department for Business Innovation & Skills, London, May 2016.

FIGURE 5
Has your organisation conducted or estimated the financial impact of a cyber-attack?
Source: Marsh Cyber Survey

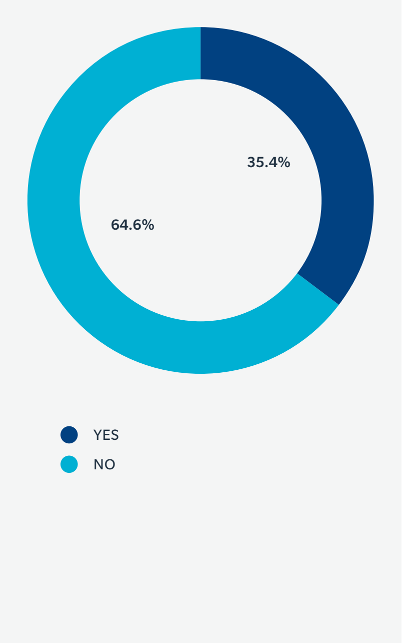


FIGURE 6
If yes, what is the worst loss value?
Source: Marsh Cyber Survey

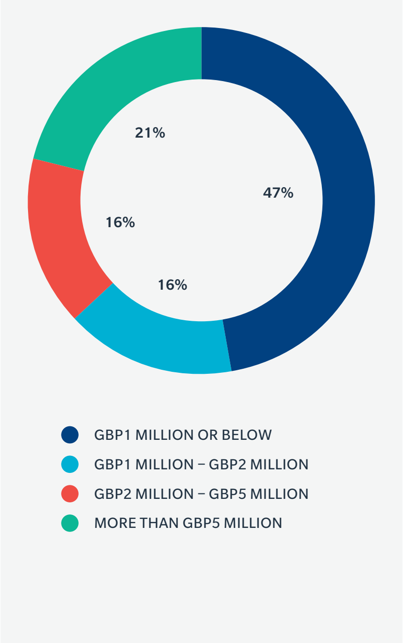
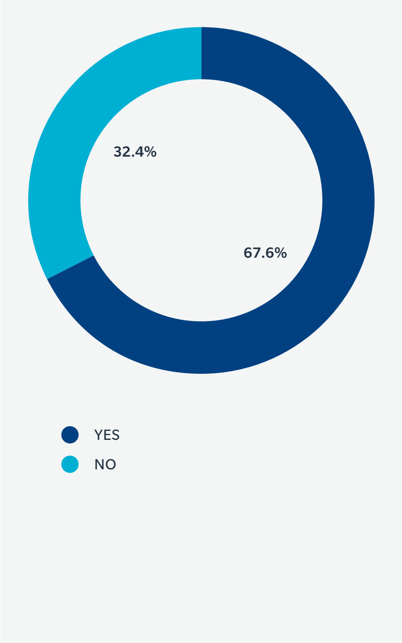


FIGURE 7
Does your finance function have a plan in place to access sources of appropriate funding to deliver both the required amount of funds and be accessible at the point when it is needed?
Source: Marsh Cyber Survey



Once loss scenarios are developed that include enough detail, these specific impacts can be evaluated with input from different groups within the organisation, such as IT, finance, legal, and risk management.

Those that have made loss estimates appear to have arrived at figures ranging across the spectrum, which may be indicative of the spread of respondents' organisations that were surveyed.

That more than two-thirds (67.6%) of organisations have planned for sources of funding in the event of a cyber-attack is encouraging; however, we would question the adequacy of these methods when just 35.4% of them have conducted or estimated the financial impact.

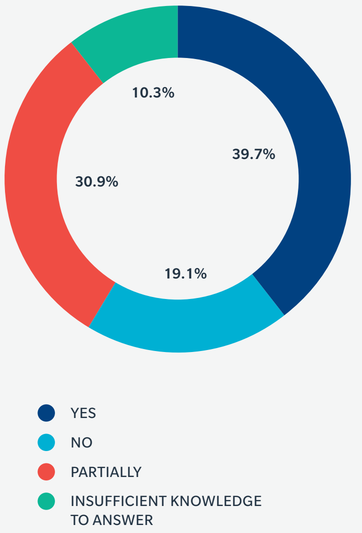
Since just 20.6% of companies are buying insurance (see FIGURE 11), it is assumed that the remainder are bypassing the insurance market and relying on alternative methods, such as lines of credit, balance sheet funding, and/or other assets. However, without an idea of the quantum of a potential loss, many of these could prove to be too large or, more likely, too small for what is required.

Without an idea of the quantum of a potential loss arising from a cyber-attack, many sources of funding could prove to be too large or, more likely, too small for what is required.

Given the fact that the majority of the respondents are clearly considering their cyber risk exposures, it comes as no surprise that nearly two-thirds (70.6%) of respondents either have an incident response plan in place or one that is partially developed.

The benefits of having a crisis management and/or IT disaster recovery plan in place (see SPOTLIGHT) have been proven to have a very positive effect on the operational, financial, and reputational impact of a cyber-attack.[4] However, some companies can focus too much of their energies on handling threats that have already surfaced as opposed to those that could one day emerge in the future – this is not risk management; it is crisis management.

FIGURE 8
Does your organisation possess an incident response plan for material cyber events?
Source: Marsh Cyber Survey



SPOTLIGHT

Benefits of incident response plans

A crisis management plan will help companies strategically deal with an incident and minimise the overall damage. They include aspects such as:

- A pre-established vision on the right level of communication to provide to the media, general public, and clients.
- A communications spokesperson, potentially including a script, for both internal and external stakeholders.
- A list of pre-selected and briefed vendors in legal, forensic, and crisis communications.

An IT disaster recovery plan will provide prescriptive guidance about what to do to get the IT systems back up and running, including:

- Technical actions to get the IT systems back up and running.
- Identification of any sparing/vendors.
- Clearly defined roles and responsibilities.

[4] *2015 Cost of Data Breach Study*, Ponemon Institute, London, May 2015.

SECTION 3: EXTERNAL USERS EXPOSE NEARLY TWO-THIRDS OF COMPANIES

One of the major and most surprising findings of last year's report was that the majority of organisations did not assess the suppliers and/or customers they trade with for cyber risk, and it would seem that the same can be said in 2016.[5]

FIGURE 9
Do you assess suppliers and/or customers you trade with for cyber risk?
Source: Marsh Cyber Survey

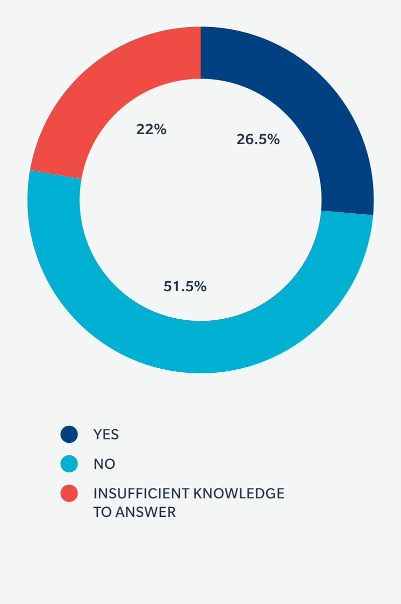
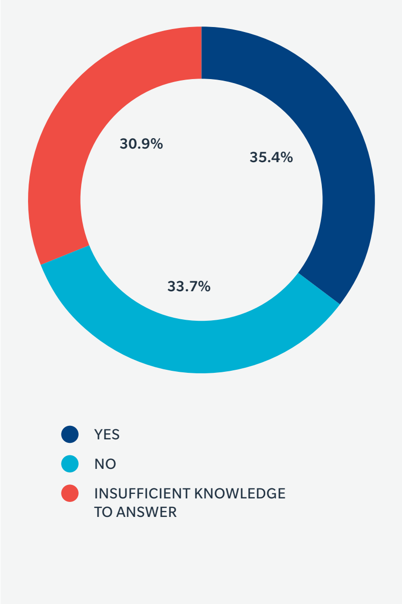


FIGURE 10
Has your bank or your customers required you to demonstrate a certain standard of IT security practice in order to do business?
Source: Marsh Cyber Survey



The overwhelming majority of companies are leaving themselves exposed to third parties, from service providers to customers.

With 26.5% of respondents saying that their organisations' supply chains are assessed for cyber risks, the overwhelming majority of companies are leaving themselves exposed to third parties, from service providers to customers.

The figure is up slightly from 22.2% in 2015, indicating a small increase in supply chain management as organisations realise the porous nature of their IT and operational technology (OT) systems and how this increases their vulnerability to cyber-related events. However, while this increase should be welcomed, there remains a lot of work to be done by just under three-quarters [73.5%] of organisations.

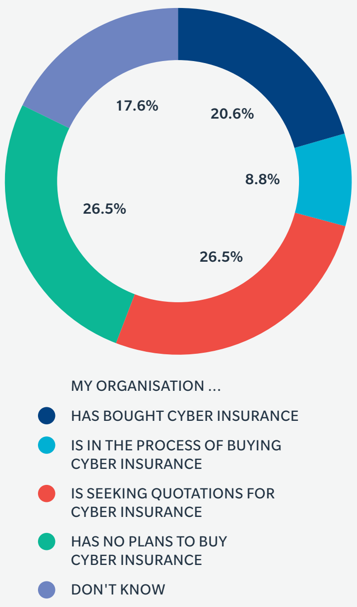
In addition, just 35.5% of respondents' organisations have been asked to demonstrate a competent standard of IT security practices by their own bank and/or customers in order to do business with them. We expect this number to increase in the near future as business process and, therefore, business income becomes increasingly reliant on IT and OT systems. As more and more industries become driven by computer-enabled processing, banks will likely refocus their lending due diligence around these technology-driven issues.

[5] *UK 2015 Cyber Survey Report*, Marsh, London, June 2015.

SECTION 4: ONLY HALF OF COMPANIES ENGAGING WITH CYBER INSURANCE MARKET

Around half (55.9%) of respondents have either bought cyber cover or are engaged with the insurance market in one way or other.

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



As we learnt in section 2 of this report, many organisations still have some way to go in terms of measuring and quantifying the potential impact of cyber risk which, we would suppose, is preventing them from approaching the insurance market.

Without a complete understanding of their company's exposure to cyber risk (75%) and/or a calculation of the financial impact should an event occur (64.6%), these organisations are in a poor position to approach the insurance market and place a value on transferring the risk. With that in mind then, that 55.9% of respondents are engaged with the insurance market in one way or the other is actually higher than we would expect.

Respondents' greatest concerns continue to be breach of customer information (32.4%) and business interruption (19.1%) – issues that can be covered against in a basic cyber policy. This would suggest that the insurance market is focusing on the right areas.

In our experience, breach of customer data is often cited as the most serious cause for concern.

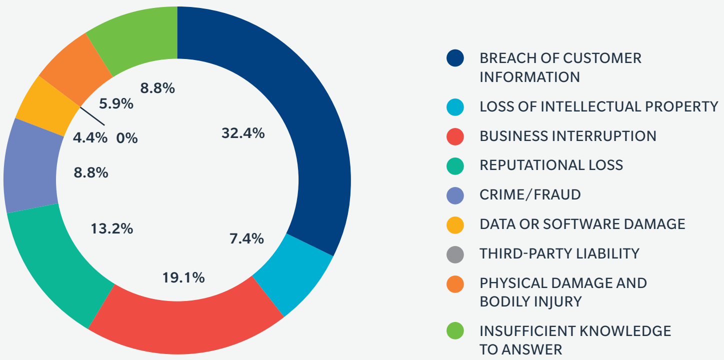
However, with the European Parliament having just passed the General Data Protection Regulation (GDPR) – which will now also impose disclosure rules on any organisation that collects data on European Union (EU) subjects, regardless of the domicile of the company – this concern has no doubt increased even further.

Interestingly, concern about reputational loss increased from 8.4% in 2015 to 13.2%, overtaking crime/fraud into third place. This is no doubt as a result of recent high-profile cyber events having had a huge impact on brand and reputational value, for example, with TalkTalk and Carphone Warehouse. Fortunately for these organisations, the insurance market has developed several products that provide cover for reputational loss in the past 12 months.

Of course, reputational risk is very difficult to measure and treat. In some industries, reputational risk can be measured in customer churn and, therefore, may fall under business interruption risks.

> Without a complete understanding of their companies' exposure to cyber risk and/or a calculation of the financial impact should an event occur, organisations are in a poor position to approach the insurance market and place a value on transferring the risk.

FIGURE 12
Which cyber loss scenario presents the greatest threat to your organisation?
Source: Marsh Cyber Survey



BOARD DISCUSSION

Impact of Brexit on UK Cyber Risk Profiles

On 23 June, the UK voted to leave the European Union (EU), creating uncertainty surrounding the future of the UK's future regulatory landscape. In order to progress the process of exiting the EU, the UK Government intends to trigger Article 50, after which it will have a two-year transitional period to negotiate the terms of an exit.

One thing is for certain; until that process is complete, existing UK regulation will not be impacted. Taking all of this into consideration, clients should keep the following in mind:

- The General Data Protection Regulation (GDPR) will become directly applicable in all EU Member States from 25 May 2018. Since Article 50 is yet to be invoked, it is likely that the GDPR will, at least temporarily, become law in the UK. Companies will therefore need to be fully prepared for the GDPR regardless of future negotiations.
- Given the expanded territorial scope of the GDPR, companies offering goods or services to, or monitoring the behaviour of, individuals in the EU will still be required to comply with the GDPR after the UK exits the EU.
- Following an exit from the EU, the UK could implement cyber-related regulation in addition to GDPR, placing greater regulatory requirements on companies. We therefore recommend companies begin preparing for GDPR as early as possible.
- Companies should keep an eye on negotiations regarding passporting and know how it would affect their multinational cyber insurance coverage. We recommend testing insurance coverages to ensure that policies will continue to respond to a cyber loss in the EU.

Companies should continue to monitor developments around the UK's exit from the EU and be aware of how it will impact their cyber risk profile.

SPOTLIGHT

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.

Concern over operational errors reduced significantly suggesting that organisations have been putting internal IT security measures in place, such as paperless offices and bring-your-own devices, and are confident in their implementation.

FIGURE 13
Where do you view the greatest threat to your organisation originating from?
Source: Marsh Cyber Survey

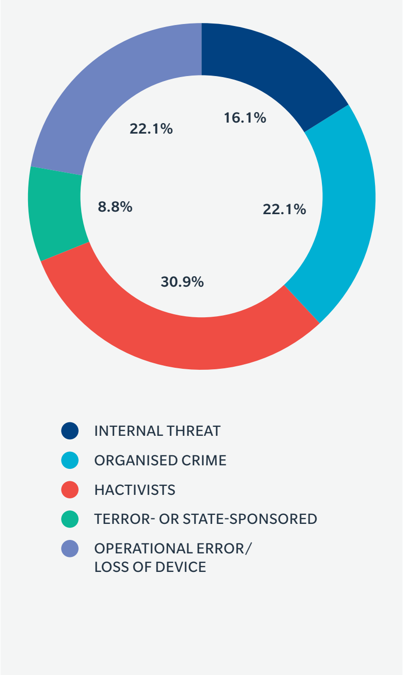
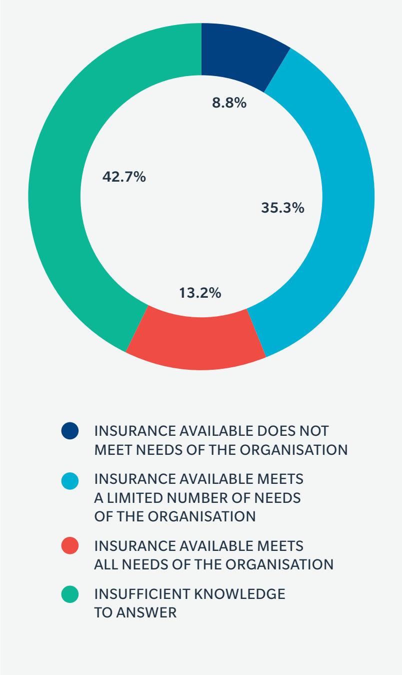


FIGURE 14
Which statement best reflects your attitude to cyber insurance based on your current knowledge?
Source: Marsh Cyber Survey



Identification of the source of the threat is a useful way for an organisation to consider the cyber risks it faces (see APPENDIX 1). Respondents identified hactivist groups as the greatest threat (30.9%), followed by organised crime and operation errors (both with 22.1%).

Hacktivism can be triggered by any number of philosophical or political disagreements with private organisations and result in various forms of attack, including theft and public exposure of internal emails or other records, denial-of-service attack to shut down a company's website, or other types of breaches to wreak confusion, embarrassment, and general loss of reputation. Hacktivists are not motivated by money, but the economic impact on the victim can still be devastating.

Interestingly, concern over operational errors reduced significantly from 2015's results (34.7%), suggesting that organisations have been putting internal IT security measures in place, such as paperless offices and bring-your-own devices, and are confident in their implementation.

When read against last year's results, the findings in FIGURE 13 would suggest that the insurance market is heading in the right direction in terms of promoting its relevancy to consumers: 13.2% believe it meets all of the needs of their organisation (up from 6.8%); 35.3% believe it meets a limited number of needs (up from 31.9%); and only 8.8% say it does not meet the needs (down from 12.5%).

Of course, cyber insurance should not be considered a holistic solution to deal with cyber risk, and instead should be viewed as but one piece of a cyber risk mitigation strategy that treats very specific events and outcomes.

Importantly, 42.6% of respondents believe they have insufficient information to answer just how relevant modern cyber insurance products are to the needs of their organisations. This may suggest the insurance market still has some way to go in terms of promoting its product or, in view of earlier findings, might indicate the extent to which a lack of understanding of their firm's own risk profiles is preventing them from making an informed judgement as to the adequacy of the cover that is available in the marketplace.

CONCLUSION

Awareness of cyber risk has clearly increased from when we carried out this same survey of UK companies last year, at a time when the potential operational and reputational impact of a cyber event has never been greater. Today, 83.8% of respondents have a basic or complete understanding of their company's exposure to cyber risk (compared to 60.8% last year) and 71.8% place cyber as a top-10 risk on their corporate risk registers (compared to 45.8% in 2015).

Increasing awareness is just part of the task facing UK organisations, however, and there is still a great deal of work to be done to improve understanding and management of cyber risk. While it is encouraging that, today, 30.3% of UK businesses have board-level oversight of cyber risk – a 56% rise on the figure from 12 months ago – IT departments continue to take primary responsibility for the review and management of cyber risks in more than half (55.7%) of organisations.

At present, nearly two-thirds (64.6%) of UK companies haven't conducted or estimated the financial impact of a cyber-attack, and this is of great concern. Board-level buy-in is essential if organisations are to map the potential operational and financial impacts an event could have to their business. This will then help move them beyond raising awareness, giving them a better understanding of the business risk posed to their companies and putting them in a good position to place a value on mitigation and/or risk transfer actions.

One of the major and most surprising findings of last year's report was that the majority of organisations did not assess the suppliers and/or customers they trade with for cyber risk, and it would seem that the same can be said in 2016. This leaves the overwhelming majority of respondents' supply chains exposed to third parties and increases the potential for systemic risk.

The insurance industry, meanwhile, continues to focus on the right areas; the cyber loss scenarios presenting the greatest threats to organisations are breach of customer information and business interruption, which can be covered against in a standard cyber policy. However, the insurance industry needs to work together with government and businesses to encourage proper assessment and quantification of cyber risk among UK organisations. Only then will they be able to make the value-based judgments on how to mitigate and/or transfer the risk, which are necessary to improve the cyber security of the country as a whole.

APPENDIX 1: CYBER-ATTACK 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.

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 30,000 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 60,000 employees worldwide and annual revenue exceeding US$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 Cyber Risk Survey Report: 2016*

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 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:

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

MARSH

For more information, please contact:

PETER JOHNSON

Senior Vice President
Marsh Risk Consulting
+44 (0) 20 7357 3527
peter.a.johnson@marsh.com

INSURANCE BROKERS
CII
CHARTERED

MARSH IS ONE OF THE MARSH & McLENNAN COMPANIES, TOGETHER WITH GUY CARPENTER, MERCER, AND OLIVER WYMAN.

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Conduct Authority.

Marsh Ltd, trading as Marsh Ireland is authorised by the Financial Conduct Authority in the UK and is regulated by the Central Bank of Ireland for conduct of business rules.