Facing the cyber risk challenge

20 September 2016

A report by Lloyd's

LLOYD'S

Contents

Section 1
Executive summary

1.1 Executive summary

These days almost every business, regardless of size or location, relies on digital technology. While it helps companies become more efficient, reduces their costs and opens up new markets, it also makes them more vulnerable to cyber attacks. Over the past couple of years, a number of high-profile cyber incidents – many of them data breaches involving the leaking of customer information – have brought cyber security to the fore.

Adding additional urgency is the fact that, in 2018, the European Union is introducing the General Data Protection Regulation (GDPR), which will set rigorous requirements for any businesses that deal with European consumers' data.

Lloyd's – the global centre for cyber insurance – commissioned this survey to find out what European businesses are doing to tackle cyber security and how they are preparing for the GDPR.

The survey questioned 346 senior decision-makers at large businesses (with revenues of €250m or more) across Europe. Respondents' job titles included Chief Executive Officer (CEO); Chief Financial Officer (CFO); Chief Operating Officer (COO); Chief Information Officer (CIO); Chief Technology Officer (CTO); Chief Risk Officer (CRO); and general counsel.

Most large European businesses have suffered a data breach in the past five years but are not worried about the possibility of another breach happening again.

- 92% of respondents said their company had suffered a data breach in the past five years, yet only 42% are worried about suffering another breach in the future.

Cyber risk has risen substantially up the boardroom agenda in the last year – it's now the CEO, not the CIO, driving cyber security strategy.

- Plans to protect against and plans for data breaches are now being driven by CEOs in a majority (54%) of those questioned. By contrast, CIOs are driving the decision-making process in just 10% of companies. This follows a number of recent high-profile cyber incidents in businesses around the world, many of which resulted in significant impacts on the bottom-line or share price and which, in some cases, led to senior executives losing their jobs.

Awareness of the EU General Data Protection Regulation is high but the understanding of its implications is low – with potentially serious consequences.

- 97% of respondents have heard of the GDPR but only 7% said they know "a great deal" about it; 57% said they know "little" or "nothing" about the new regulations, despite the serious financial and legal consequences of not complying with its rules.

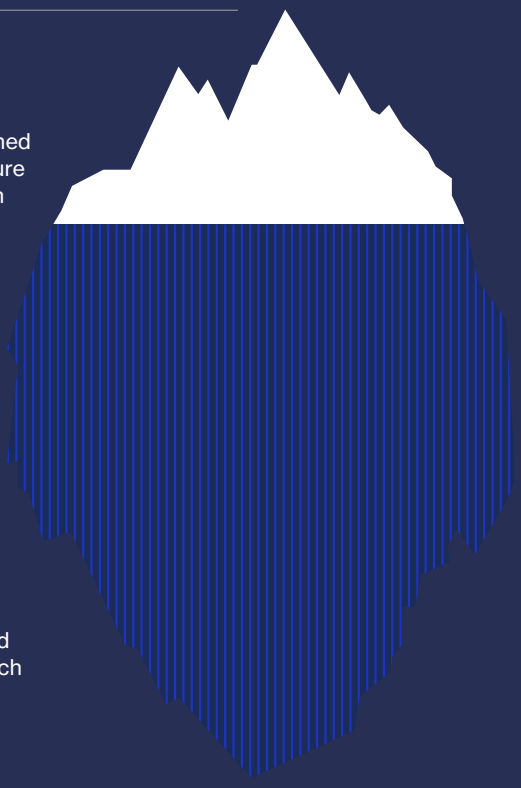
- More than half the businesses surveyed were aware the GDPR could impact them in terms of regulatory investigation (64%), financial penalties (58%), share price (57%) and reputation (52%), but only 13% believed they could lose customers.

1.2 Conclusion

European businesses face a constantly evolving landscape of cyber threats. The introduction of the GDPR will increase the focus on the data security aspect of their operations, because regulators, shareholders and customers will use it to hold companies accountable to higher cyber security standards. By working with expert partners, such as lawyers, cyber security experts and insurers, businesses can better understand the risks they face and help mitigate them in order to protect their balance sheets.

42%

businesses are concerned about a future data breach



92%

businesses experienced a data breach in the past five years

97%

businesses have heard about the new EU regulation (GDPR)

57%

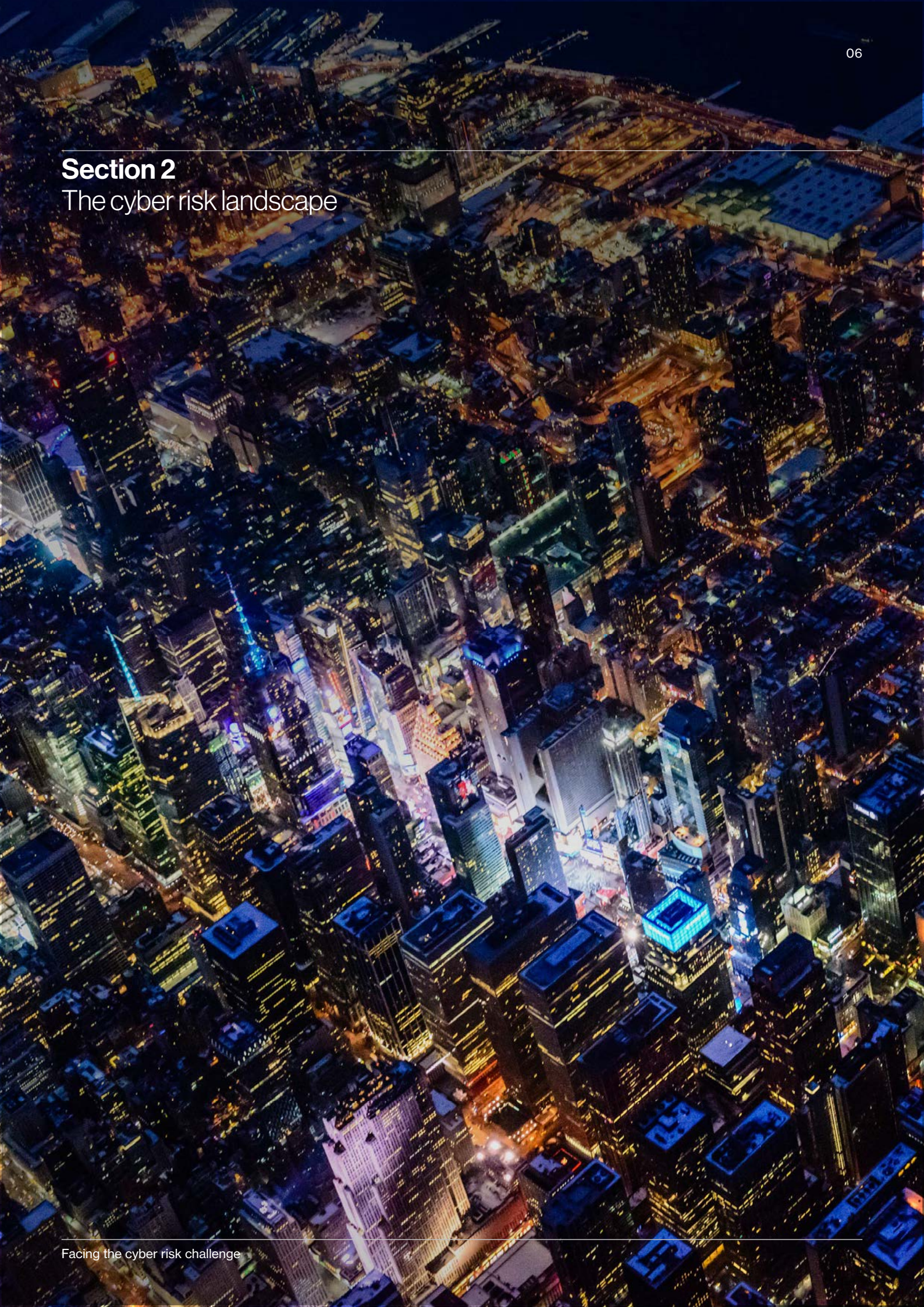
businesses know little or nothing about the new EU regulation (GDPR)

How cyber insurance can help

- According to this survey, 73% of business leaders have a limited knowledge of cyber insurance and 50% don't know that cyber cover for data breaches is available
- Cyber insurance not only provides a financial pay-out after a cyber-attack, but also offers expert consultancy to improve security and on-the-ground support during the crisis period
- Working with underwriters who understand this risk from the beginning will benefit a company's security strategy. Underwriters can help businesses identify risks and vulnerabilities, and can therefore mitigate the likelihood of a breach happening in the first place
- All these help protect company balance sheets, as well as drives up cyber security and risk mitigation standards across the industry.

Visit www.lloyds.com/cyber

Section 2
The cyber risk landscape



2.1 Cyber risks on the rise

These days almost every business, regardless of size or location, relies on digital technology. Retailers, financial service companies, FMCG brands now use digital technologies to run their businesses, monitor stock, design products, communicate and store customer data.

But while digital technologies help companies become more efficient, reduce their costs and develop new markets, it also makes them more vulnerable to cyber-attacks.

Because of this, cyber security has become a major issue for businesses. Cyber now stands alongside well-established risks such as property damage, terrorism and natural disasters, as a threat every business has to assess, mitigate and manage.

The increased awareness of cyber risks among businesses has been driven by some high-profile incidents around the world in recent years. The most recent prominent cyber-attack in the UK was against telecoms provider TalkTalk in autumn 2015. In other parts of Europe, there have been attacks against French TV station TV5 Monde, Sweden's air traffic control system, Norwegian oil and energy companies, and a German steel mill, among others. In the US, a series of cyber incidents have made headline news since 2014, including attacks on Sony, Target, Home Depot and Experian.

Correspondingly, the Lloyd's market, which pioneered the first cyber insurance policy 10 years ago, has seen the cyber insurance market grow rapidly. There are now 65 insurers in the Lloyd's market offering cyber insurance, with a combined capacity of £300m. Their business represents a quarter of the global cyber insurance market, making Lloyd's the global centre for cyber insurance.

This report – based on a survey of 346 senior business decision-makers from large companies across Europe – analyses how business leaders are approaching the challenge of cyber security and what they are doing to ensure their organisations are well prepared in the event of a cyber attack.

The report also investigates how ready European businesses are for the implementation of the EU's General Data Protection Regulation (GDPR), which is due to come into force in 2018. This new regulation will considerably strengthen the existing rules and responsibilities around how businesses process and safeguard consumer data. It also introduces a series of requirements for businesses that suffer a data breach, including having to report a cyber breach within 72 hours or face significant fines.

This report focuses on one type of cyber incident: data breach. This is because protecting confidential data – especially customers' financial or health records – is considered a priority for most businesses. Data is their main digital asset and therefore the target of most cyber attacks.

2.2 Data breaches

How big an issue is data breach for European businesses today? To quantify the scale of the problem, the survey asked respondents if they had experienced a data breach at their organisation.

92% of respondents said their company had suffered a data breach in the past five years, while 3% said they had “come close”. Only 5% said they had not suffered a breach or were unaware that they had.

Which of the following best describes your company’s experience of a data breach, in the last 5 years:

Base: Total Respondants (346): UK (100) France (31) Germany (34) Italy (30) Spain (30) The Netherlands (31) Norway (30) Denmark (30)

2.3 Internal and external threats

Data breaches can be caused by various cyber attack methods, some highly sophisticated and malicious, others relatively innocent or accidental. The survey asked which of the threats worry companies the most.

The cyber threats were categorised as either “internal” or “external”. Internal threats are typically those that originate from the company itself, either through human error, such as lost or stolen information or equipment, or by a rogue employee intentionally leaking confidential details. External threats tend to be more hi-tech and include techniques such as hacking, phishing, ransomware and malware (see below glossary).

The survey found that most businesses were more concerned about external rather than internal threats. The internal threats that businesses were most worried were low-tech with 42% of respondents stating physical loss of paper documents as a key concern. The same percentage also listed an insider intentionally breaching information as a key threat.

The number one external threat is hacking. Half (51%) of the businesses questioned said they were worried about the possibility of being hacked for financial gain, compared to 46% who were concerned about being hacked for political reasons. 41% listed hacking by a competitor as a serious threat.

It is not surprising that hacking is the number one threat given recent high-profile data breaches. TalkTalk, Sony and Home Depot, to name just three, have all been victims of cyber-attacks recently. While the true motivation of these sorts of incidents is often unclear, attacks of this nature can be used to steal customer information that can be sold to the highest bidder.

There can be political motives too, especially for businesses operating in geo-politically sensitive industries such as energy or natural resources. Increasingly, rogue groups of hackers with specific political objectives are attacking individual organisations. While levels of corporate espionage are hard to measure accurately, the fact that hacking by competitors comes third on the list suggests this is considered a serious threat by business leaders.

Cyber-threat glossary

- Hacking – seeking and exploiting weaknesses in a computer system or network, typically for financial gain
- Phishing – attempting to obtain sensitive information by masquerading as a trustworthy person or organisation in an email
- Whaling – a phishing attack that involves masquerading as a senior executive, often a CEO
- Malware – (short for malicious software) is any software used to disrupt computer operations, gather sensitive information or gain access to private computer systems
- Ransomware – a type of malware that adversely affects a computer and demands a ransom payment to restore it.

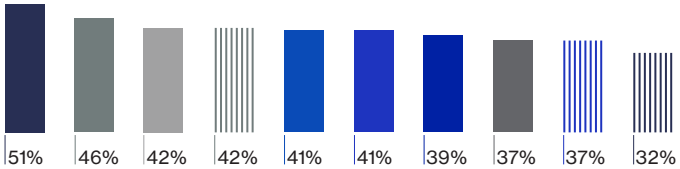
51%

are worried about the possibility of being hacked for financial gain

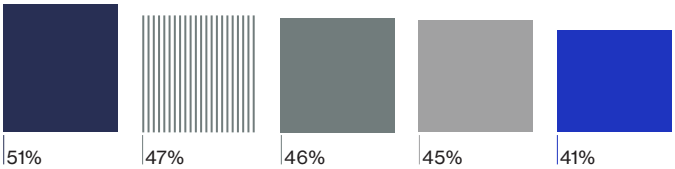
2.3 Internal and external threats

- Hacking – financial gain
- Hacking – by competitor
- Hacking – political motivations
- Human error/unintended disclosure
- Phising
- Lost, discarded or stolen equipment
- Ransomware
- Malware
- Physical loss of paper or non-electronic devices
- An insider intentionally breaching information

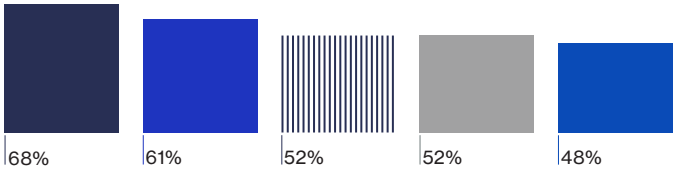
Total



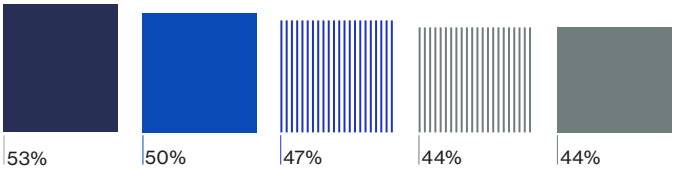
UK



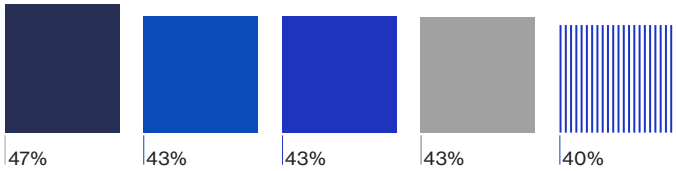
France



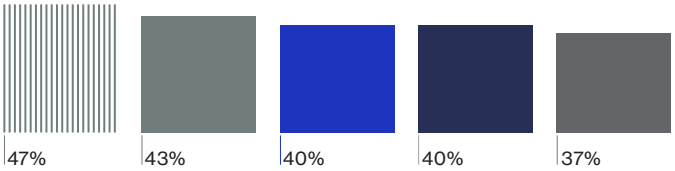
Germany



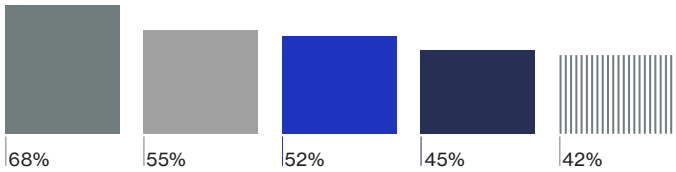
Italy



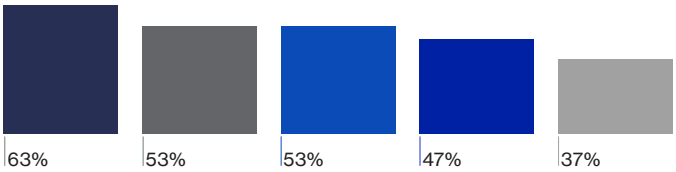
Spain



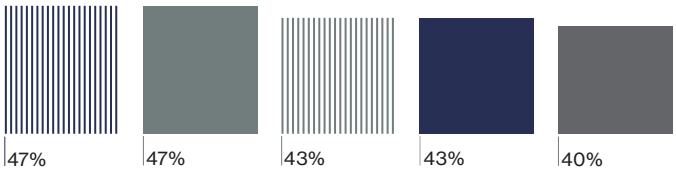
The Netherlands



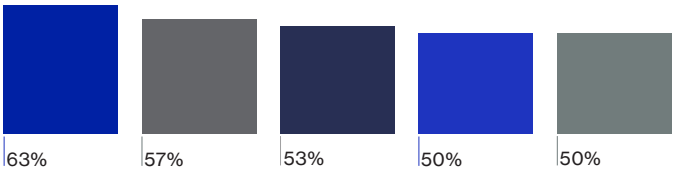
Norway



Sweden



Denmark



Base: Total Respondants (346): UK (100) France (31) Germany (34) Italy (30) Spain (30) The Netherlands (31) Norway (30) Denmark (30)

2.4 A false sense of cyber security

Although 92% of businesses have suffered a data breach in the past five years, only 42% of respondents expressed concern about suffering a future data breach.

92%

suffered a data breach

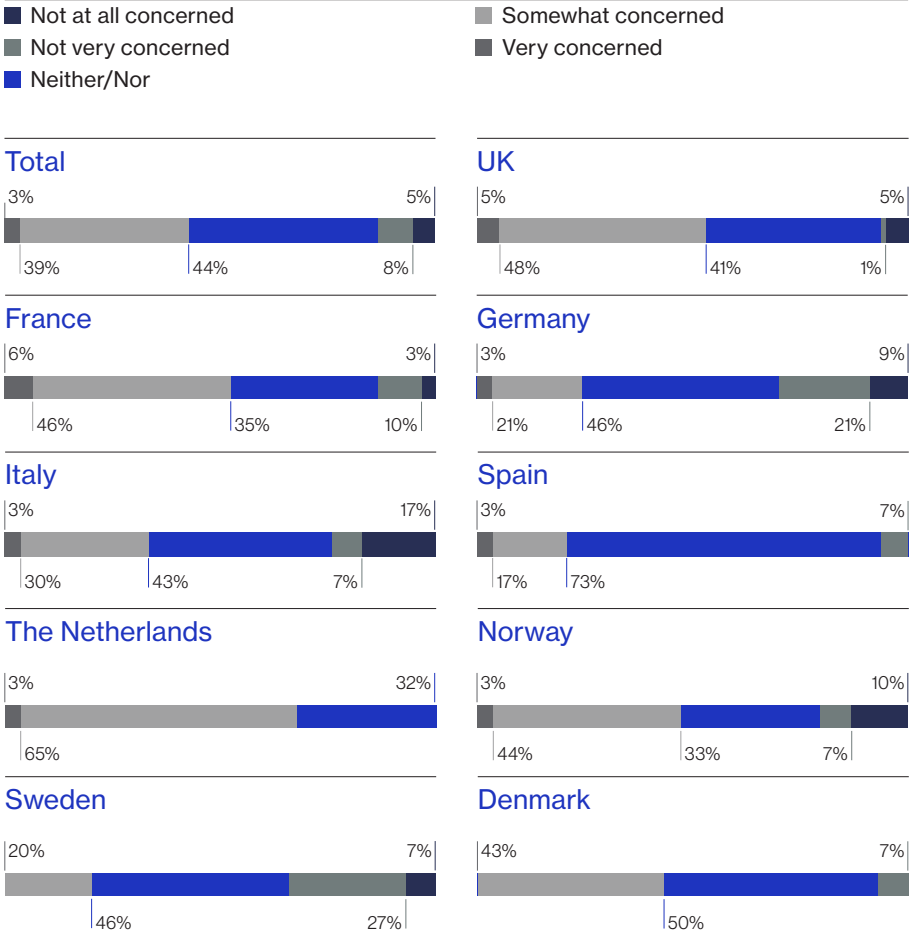
42%

are concerned about suffering a future data breach

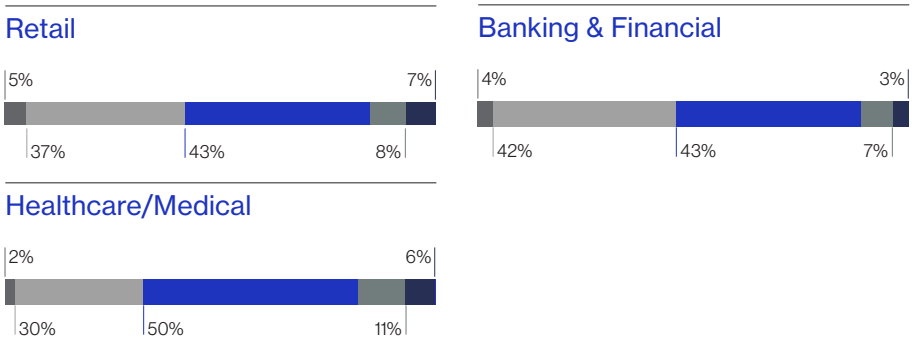
The results differed slightly from sector to sector. Financial services companies were most likely to be worried about a breach (46%), understandable given the volumes of sensitive information they hold on their customers. Companies in the healthcare sector were less concerned (32%) – surprising given that health records are more valuable and, as such, are increasingly sought-after by hackers.

These results show that either companies have confidence in the cyber security measures they have in place or they are complacent about their resilience to cyber-attacks. Whatever the answer, the fact is that cyber-attack technology is constantly evolving, making it almost impossible for companies to make themselves 100% secure. Unless businesses take cyber security seriously, they will be vulnerable to cyber-attacks in the future.

Thinking about your company - on a scale of 1 to 5 where 1 is 'not at all concerned' and 5 is 'very concerned', how concerned are you that your comppany will suffer a data breach?



Base: Total Respondants (346): UK (100) France (31) Germany (34) Italy (30) Spain (30) The Netherlands (31) Norway (30) Denmark (30)



Base: Total Respondants (346): Retail (109) Banking & Financial (95) Healthcare / Medical (90)

Section 3
Preparation and response

3.1 Fail to prepare...

As discussed in the previous chapter, 92% of businesses have experienced a data breach in the past five years. The survey asked respondents how prepared they felt for such an incident happening again. Businesses were asked how they would describe their level of preparedness for a data breach based on three criteria:

1. Putting together a crisis response: e.g. communicating the news to customers and updating IT systems.
2. Managing reputational damage: e.g. through public relations, advertising and other marketing activities.
3. Regulatory implications: e.g. co-operating with an investigation or responding to regulatory changes.

93%

of businesses would be "prepared" or "very prepared" to put together a crisis response

89%

said the same about managing reputational damage

87%

about handling regulatory implications

Most businesses will have processes and procedures in place for cyber incidents; this is not the same as being fully prepared. Many companies focus on developing a response plan that sets out what they will do if they experience a data breach, yet there are a whole series of measures – covering before and after a breach – that must be implemented if an organisation is to be fully prepared.

Companies should ensure their systems are rigorously tested and externally validated before they can feel confident about their level of preparedness. Even then, it's essential they remain constantly vigilant and regularly update their plans as new threats emerge.

3.2 Who is taking responsibility?

Data security, was once wholly the domain of the IT department. Today, the importance of data security is such that it has risen up the list of priorities for the C-suite.

This change has taken place remarkably rapidly. Last year [2015], a Marsh survey showed that only 17% of European businesses listed cyber in their top five corporate risks, while 25% didn't have it on their risk register at all. Almost two-thirds of businesses (65%) said their IT departments had primary responsibility for cyber risks in their organisations, while just 11% said it was their board that had responsibility.

Lloyd's survey, conducted nine months later, found that European company boards are now taking a much more hands-on approach in an effort to get to grips with cyber risk.

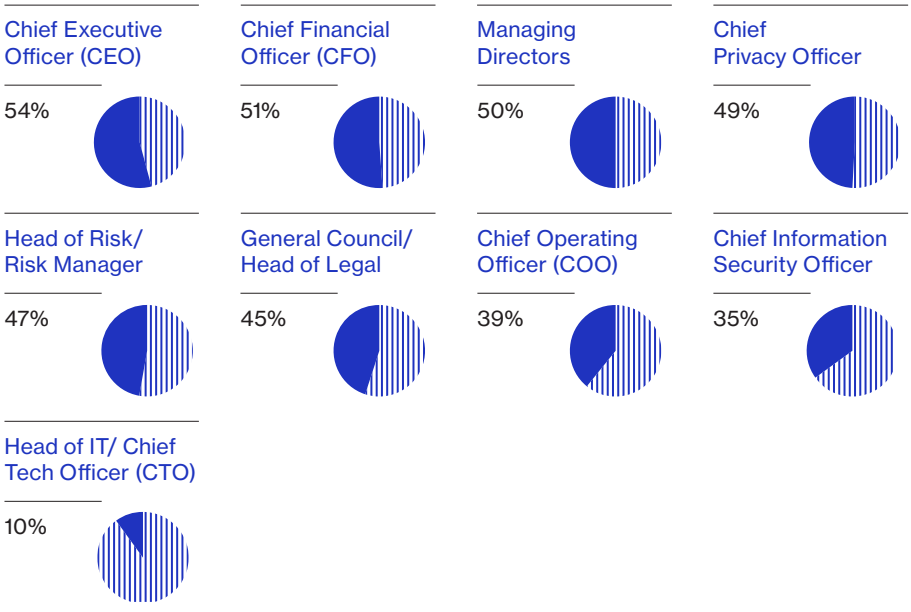
Respondents were asked who within their company made the decisions about protection from, and planning for, a data security breach. The majority of respondents (54%) said it was the CEO. Those executives for whom cyber is part of their day-to-day remit were much lower down the list: only 35% said the chief information security officer was driving this in their company, and just 10% named the CIO or CTO. In 96% of cases, a representative of the C-suite was named as being the driving force.

It's likely the recent run of widely publicised data breaches and their consequences – share price crash, costs, litigation – has prompted CEOs to develop rigorous cyber security strategies. Shareholders expect the CEO to take accountability for cyber security and do all he or she can to mitigate the risks, which ultimately impact on the company's financial performance.

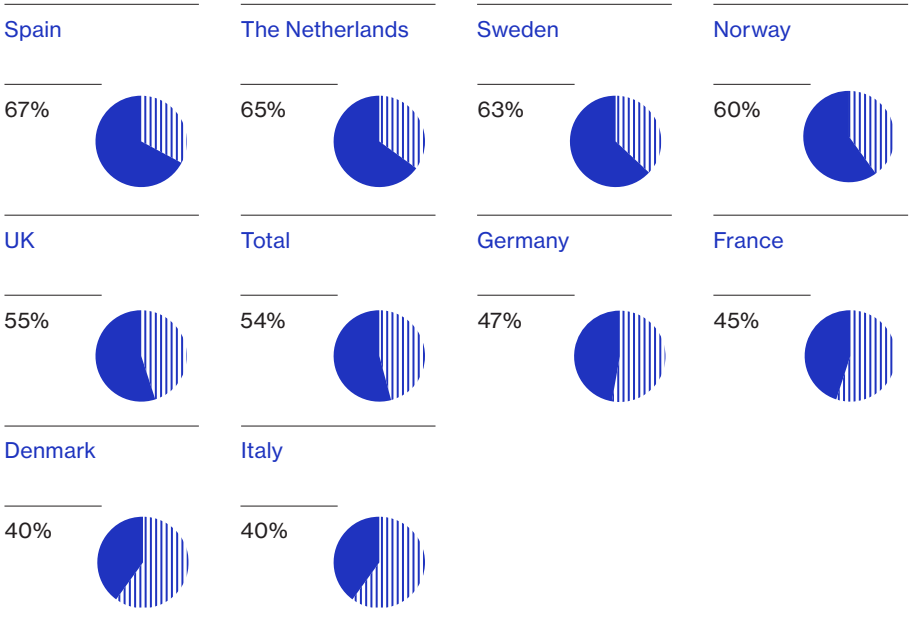
CEOs have a clear reason to take this issue seriously too as their jobs are linked to the consequences of cyber security breaches. The CEOs of US retailer Target and Austrian aerospace firm FACC both lost their jobs for reasons connected to cyber incidents.

It is encouraging that, as this survey shows, more and more CEOs are taking cyber risks seriously. Upcoming changes in EU regulations should bring this issue to the fore for all businesses across Europe.

Who within your company is driving the decision about protection against and planning for a data security breach?



Chief Executive Officer (CEO)



Base: Total Respondents (346)

Section 4
Understanding of the GDPR

4.1 A new era of cyber regulation

The introduction of the General Data Protection Regulation (GDPR) in 2018 will transform cyber regulation in Europe. It also has significant implications for businesses across the world, many of which are not widely understood by the companies themselves.

The GDPR enshrines fundamental privacy rights for consumers, such as "the right to be forgotten" and the right to object to profiling activities, which businesses have to comply with.

Importantly, the GDPR does not just apply to businesses from EU member states. Any company that offers goods and services to EU citizens, or that monitors their behaviour, must also comply with its rules. This means that many businesses from the US and Asia, for example, will be caught within the GDPR's jurisdictional reach.

Clearly the GDPR cannot be ignored. This survey asked respondents what preparations they are making for its introduction, which takes place in less than two years' time.

What is the GDPR?

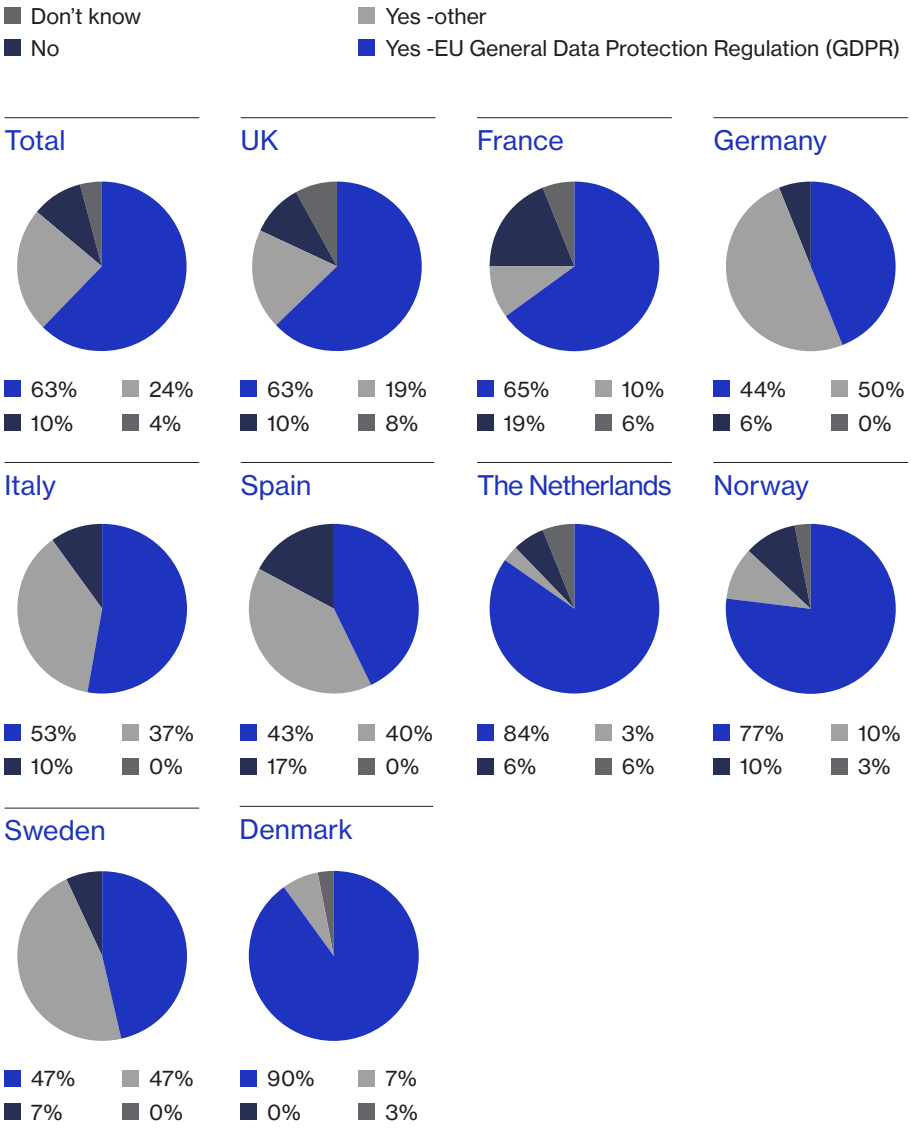
- The General Data Protection Regulation (GDPR) is a piece of EU legislation that harmonises the varied data protection laws across Europe and brings EU legislation up to date with the technological possibilities of the Big Data era
- In particular, it requires businesses to report security breaches to their regulator within 72 hours and to affected citizens without undue delay
- It sanctions fines of up to 4% of annual worldwide turnover or 20 million euros, whichever is higher, for companies suffering data breaches. Individuals may also claim compensation from organisations for financial loss or any distress suffered
- It is coming into force on 25th May 2018 across all EU member states – but it affects any company doing business with EU citizens, regardless of where the company is based.

4.2 Awareness and understanding

Given the importance of the GDPR, the fact that it was first publicly announced in 2012, and its imminent implementation, one would expect businesses to have mature plans in place. The survey revealed a much more mixed picture.

It found the majority of businesses are aware of the GDPR. When asked if they knew of any new regulations that would affect the data protection landscape, 63% mentioned the GDPR. Another 24% referenced other regulations, which could include national-level changes to data protection.

Are you aware of any new regulation or changes in regulation relating to data protection?



Base: Total Respondants (346): UK (100) France (31) Germany (34) Italy (30) Spain (30) The Netherlands (31) Norway (30) Denmark (30)

4.2 Awareness and understanding

When prompted about the GDPR specifically, a total of 97% of businesses said they had heard of it. However, this masks much lower levels of in-depth understanding. Only 7% of respondents said they knew "a great deal" about the GDPR, while more than half (57%) admitted they knew "little" or "nothing" about it. Given what the GDPR means for businesses, this reveals a surprising lack of knowledge.

97%

respondents have heard of the GDPR

57%

admitted they knew "little" or "nothing" about GDPR

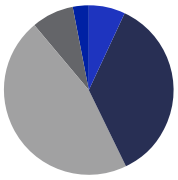
The GDPR rules include, for example, the potential for substantial financial penalties to be levied against companies who fail to comply (up to 4% of global revenues). It also sets higher standards for transparency about how customer data is used, for the security of systems protecting it, and for the speed with which customers must be informed about a breach. None of these requirements are straightforward to comply with – they will take time, investment and effort.

This finding suggests that businesses must do more to understand how the GDPR rules will impact their organisation and what their responsibilities are.

How much do you know about the EU General Data Protection Regulation (GDPR)?

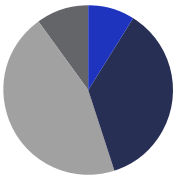
- I know a great deal about the EU GDPR
- I have heard of the EU GDPR but don't know many details
- I haven't heard of the EU GDPR and don't know anything about it
- I have a working knowledge of the EU GDPR
- I have heard of the EU GDPR but don't know any details

Total



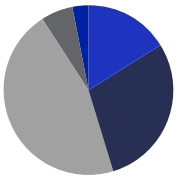
7% 36% 46% 8% 3%

UK



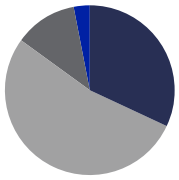
9% 36% 45% 10% 0%

France



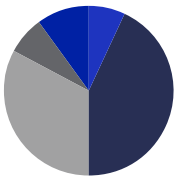
16% 29% 45% 6% 3%

Germany



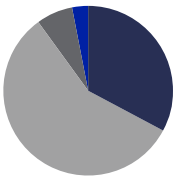
0% 32% 53% 12% 3%

Italy



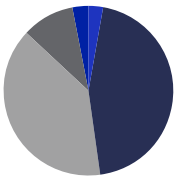
7% 43% 33% 7% 10%

Spain



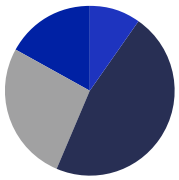
0% 33% 57% 7% 3%

The Netherlands



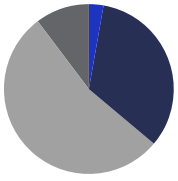
3% 45% 39% 10% 3%

Norway



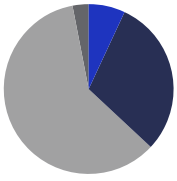
10% 47% 27% 0% 17%

Sweden



3% 33% 53% 10% 0%

Denmark



7% 30% 60% 3% 0%

Base: Total Respondants (346): UK (100) France (31) Germany (34) Italy (30) Spain (30) The Netherlands (31) Norway (30) Denmark (30)

4.3 Recognising the implications for business

Although the majority of senior business leaders admitted to knowing little about the GDPR, 66% said they understood the implications of the GDPR if their business suffered a data breach.

When pressed on this, respondents focused on two key areas: regulatory and financial impacts. Top of the list was regulatory investigation with 64% of companies naming this as the most likely implication. Next were financial penalties or fines (58%) and the impact on profits or share price (57%). Only 13% were worried about the loss of customers.

64% regulatory investigation

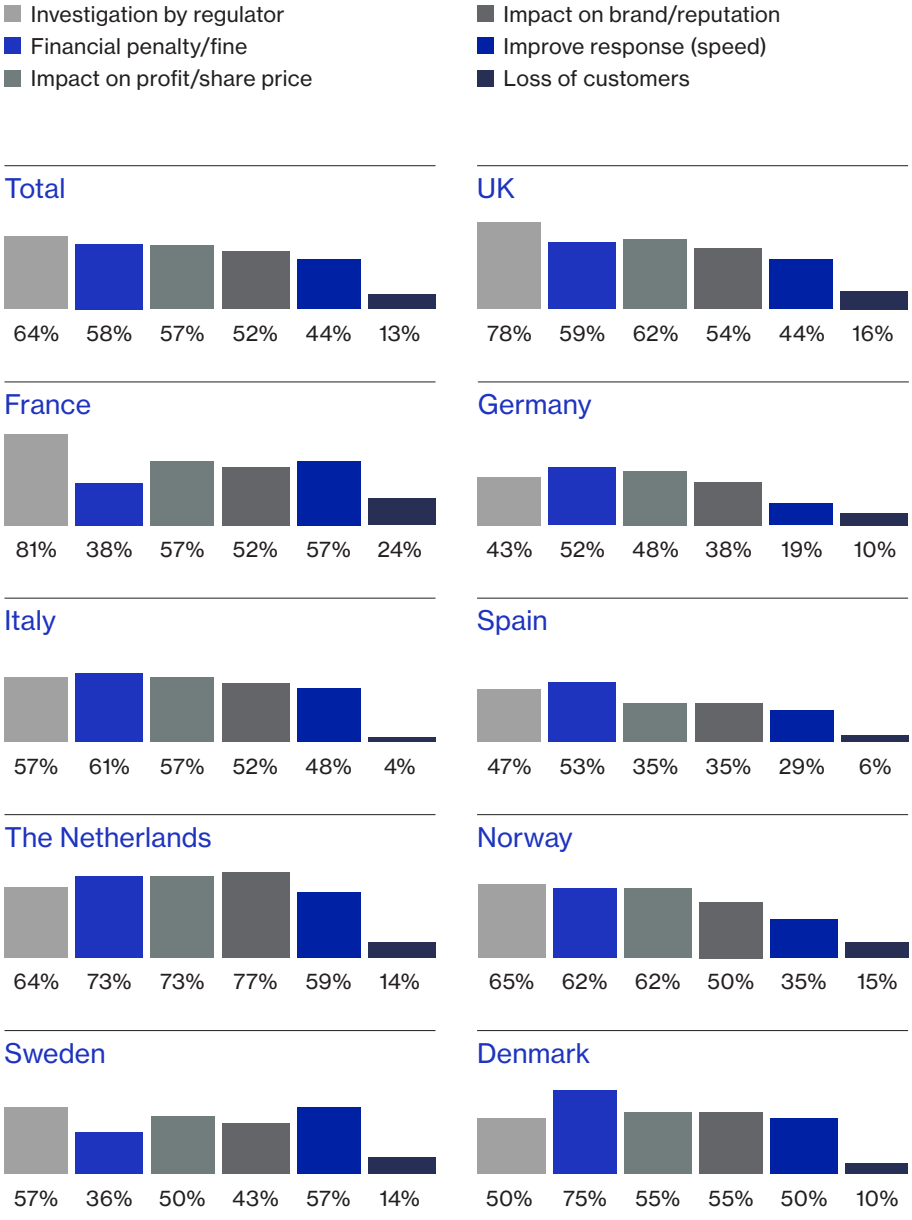
58% financial penalties or fines

57% impact on profits or share prices

13% loss of customers

The survey shows that large European businesses are more concerned about the financial implications the GDPR rules could have in the event of a data breach. The cyber-attack on TalkTalk, for instance, cost the company around £60m and led to its share price dropping 10% on the day the incident was announced. Under GDPR rules, the financial impacts of a data breach are likely to be even greater.

Bearing in mind your company's current data security processes, what implications do you think the GDPR is likely to have on your company?



Base: Total Respondants (227): UK (63) France (21) Germany (21) Italy (23) Spain (17) The Netherlands (22) Norway (26) Denmark (20)

Section 5
Conclusion

5.1 Conclusion

Cyber is the most complex, current and critical risk businesses face today: it is a matter of when not if a business becomes a victim of a cyber breach or attack.

Cyber incidents have the potential to cause business interruption, financial penalties, regulatory scrutiny and reputational damage. All of these are serious threats to a business's revenue, share price or even survival. Against this backdrop, it can be difficult for business leaders to know what they can do to protect their organisations.

The results of this survey show that while many businesses appear confident about their level of readiness for the GDPR, their understanding of its implications is low. And recent examples of data breaches suggest companies are not as prepared for cyber attacks as they think they are.

With 18 months to go until the GDPR comes into force, businesses still have time to get their processes and systems in place to comply with the GDPR. In the meantime, it is vital that businesses keep reviewing their cyber risk strategy and their understanding of the threat. Cyber threats will never go away and will only become more complex as time goes on. It is almost impossible to be 100% protected from cyber attacks.

Here are three steps for business leaders to consider to protect their organisations:

1 Identify the specific risks you face

Map the most likely ways a cyber incident could occur in your organisation. Create specific plans to mitigate these. What are the rare events you haven't considered? Your response plans should be regularly tested and updated. Ask external advisors to audit them. Work together on scenarios and simulations. Ensure you're making preparations for what to do before and after a breach, not just how to contact the affected customers.

2 Drive awareness of cyber risks and regulations through your organisation

Many cyber incidents start with human error, from accidental disclosure to phishing. Awareness of these problems is a cultural issue and needs to come from the top of the company. Ensure everyone is trained and knows, for instance, what the GDPR rules demand of them.

3 Never stop learning

Digital technology keeps evolving; so too do the cyber threats that come with it. Develop a culture of "continuous learning" and information sharing on cyber risks. Understand that 100% cyber security is impossible, which makes mitigating efforts such as cyber insurance all the more essential.

5.2 How cyber insurance can help

1 According to this survey, 73% of business leaders have a limited knowledge of cyber insurance and 50% don't know that cyber cover for data breaches is available.

2 Cyber insurance not only provides a financial pay-out after a cyber-attack, but also offers expert consultancy to improve security and on-the-ground support during the crisis period.

3 While cyber policies differ, they are likely to cover the cost of legal and forensic work to identify how a data breach happened and who is responsible, as well as customer notification and business interruption costs.

4 Working with underwriters who understand this risk from the beginning will benefit a company's security strategy. Underwriters can help businesses identify risks and vulnerabilities, and can therefore mitigate the likelihood of a breach happening in the first place.

5 All these help protect company balance sheets, as well as drives up cyber security and risk mitigation standards across the industry.

Country highlight sheets are available for; Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, Sweden and the United Kingdom.

For more information and to contact a Lloyd's cyber broker, visit www.lloyds.com/cyber