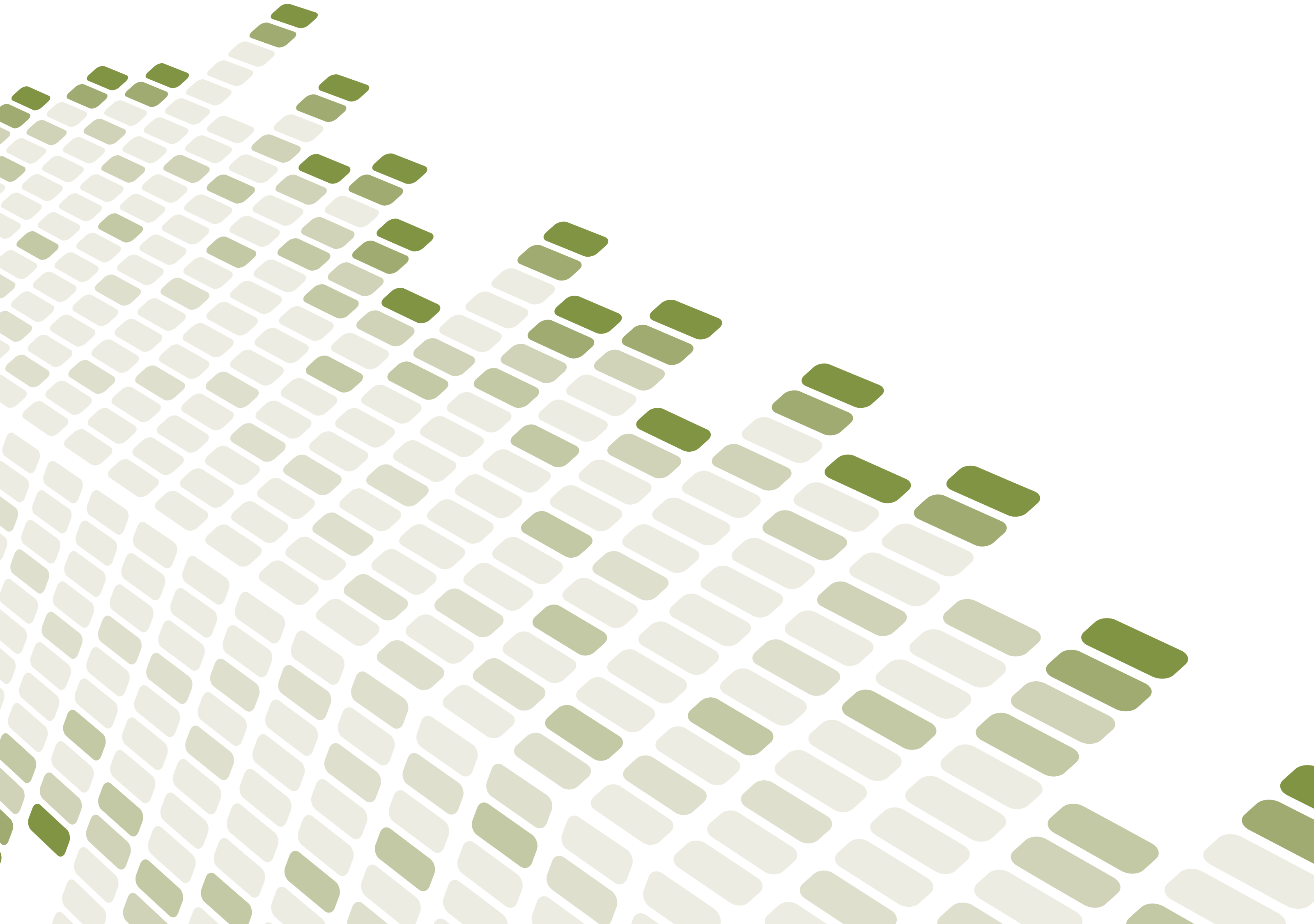
HM Government

FTSE 350
Cyber Governance Health Check Report 2017

July 2017



FTSE 350 Cyber Governance Health Check Report 2017

Contents

Foreword

We want the UK to be the best and safest place to do business online. This means a dynamic business environment and world-class cyber security. The WannaCry and NotPetya attacks, which affected core public services and private companies at home and abroad, and other high-profile cyber incidents reinforce the need for effective cyber security as part of our digital economy. It is crucial businesses get cyber security right, and boards take ownership of cyber security as a part of core business.

Since 2013, the Government has undertaken a regular survey of the UK's top 350 companies, to understand how they are managing their cyber risks. The Health Check survey indicates how the leading businesses in the country are managing their cyber security, serving as an example for their peers and others within their sectors. As we publish the latest version of the Health Check, I am encouraged by the findings that indicate FTSE 350 businesses are now more aware of the importance of good cyber security.

I would like to thank all the FTSE 350 board members and staff who have helped to inform this year's report. I would also like to express my thanks to our audit partners - Deloitte, EY, KPMG and PwC - for their invaluable support as part of producing and delivering this year's Health Check report.

An increasing number of organisations who responded to the survey relayed the importance of cyber security in terms of the need to protect their services, reassure the public on the safety of their personal data and measure their organisation's own exposure to cyber risk. Decisions about cyber are increasingly being taken at the board level, which reflects a significant, positive culture shift amongst FTSE 350s since the launch of the scheme.

However, cyber maturity among FTSE 350s needs to improve at a faster rate to ensure we can stay ahead of future cyber security challenges. This year's report shows that a small number of FTSE 350 businesses are continuing to operate without plans in place for managing cyber incidents. This is increasingly irresponsible. Furthermore, as we approach the deadline to introduce new regulation such as the General Data Protection Regulation, businesses should continue to prepare themselves for the responsibilities that come with these new requirements.

The National Cyber Security Centre provides practical advice for businesses through their 10 Steps to Cyber Security. Businesses are encouraged to consider obtaining Cyber Essentials certification and promote it through supply chains. Acquiring Cyber Essentials will provide companies with a good, basic level of cyber security, which they will need to supplement with further protection based upon their own risk profile. This will be particularly important as we approach the May 2018 deadline for GDPR to come into force.

Our economy is a digital economy. Cyber security is critical to the successful growth of this digital economy. Working together, Government and businesses can help to deliver the shared goal of making the UK the safest place in the world to do business online. I hope the findings of this report help with progress towards this shared ambition.

Matt Ha

Matt Hancock
Minister of State for Digital

Executive Summary

57%

of Boards have a clear understanding of the potential impacts resulting from a loss of, or disruption to, key information or data assets

✓ Up from 49% in 2015/16

54%

of Boards view cyber risk as a top / group risk, when compared with all the risks faced by their company

✓ Up from 49% in 2015/16

31%

of Boards receive comprehensive and informative management information on cyber risk

✓ Up from 21% in 2015/16

68%

say they have not received any training to deal with a cyber incident

10%

of Boards do not have a plan in place to respond to a cyber incident

6%

of Boards describe their business as completely prepared to meet the requirements of the General Data Protection Regulation (GDPR)

Introduction

Much of the UK's prosperity now relies upon our ability to secure our networks, data and technology from the many cyber threats we face from a variety of sources. The Government is committed to working together with industry and businesses to tackle these threats. These efforts are designed to ensure that the UK is one of the most secure places in the world to do business online.

The Cyber Governance Health Check survey supports this ambition. The Health Check offers insights into the cyber governance of the UK's top businesses, specifically those listed in the FTSE 350.

What is the Cyber Governance Health Check?

The Cyber Governance Health Check is a non-technical governance questionnaire which assesses the extent to which Boards and audit committees of FTSE 350 companies understand and oversee risk management measures that address cyber security threats to their businesses.

Completion of the questionnaire has resulted in this aggregated report, as well as confidential benchmarking reports for each participating company. The results of the tracker should be discussed with your company's trusted advisors.

The UK Government is delivering this project in partnership with firms that currently audit the FTSE 350: Deloitte, EY, KPMG and PwC. The governance behaviours, findings and guidance contained within this report should enable many large and small businesses, both within and outside of the FTSE 350, to improve their understanding and management of risks that have the potential to cause major damage to their own organisations.

Annex B of this report contains important links to key Government cyber security guidance and support which is applicable to all businesses.

Interpreting the results

The Health Check is open to all FTSE 350 businesses on a voluntary basis. This may lead to self-selection bias, where those participating in the survey may have different traits and characteristics to those that do not take part. For example as a group they may be more aware of cyber security issues than those that did not take part.

The findings of this survey provide valuable insight into attitudes and behaviours towards cyber security by large companies, however readers should not interpret the results as being representative of all FTSE 350 companies.

Respondent Profile

Summary of findings

Overall 105 companies responded to the 2017 Health Check survey. This compares with 113 respondents in 2015/16 and 108 in 2014.

Financial services companies lead the way in engaging with the Health Check

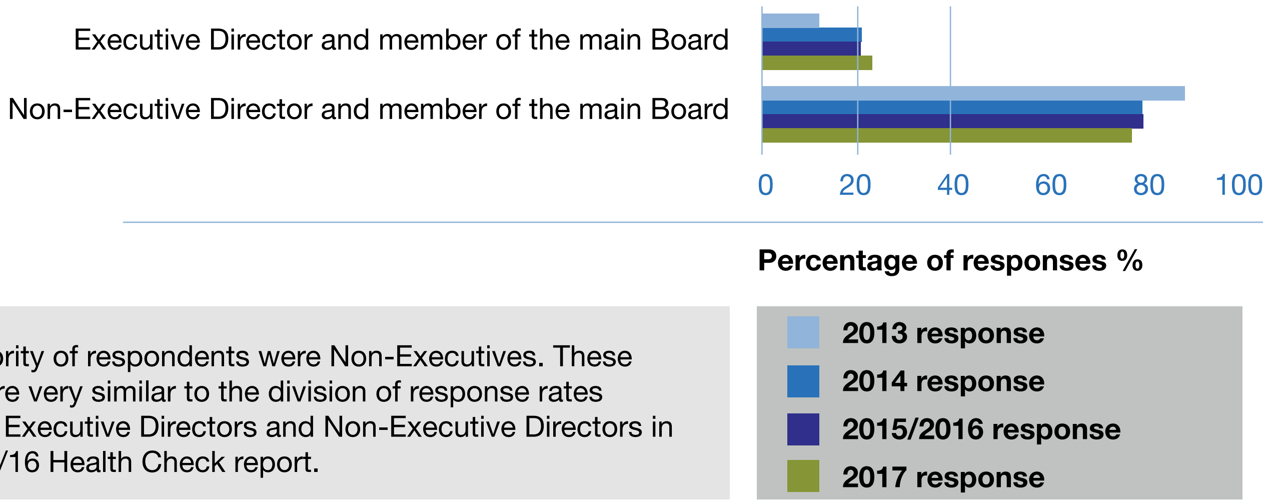
Response rates were divided between a variety of sectors, remaining consistent with the previous report in terms of sector classification. The largest proportion of respondents came from the financial services sector (23%), while companies from the retail, travel and leisure sector (17%) also feature prominently.

Chairs of audit committees tend to reply on behalf of their organisations

The majority of respondents described themselves as non-executives (77%), a similar proportion to the last Health Check report. Of those non-executives, the majority were the Chair of their company’s audit committee (65%).

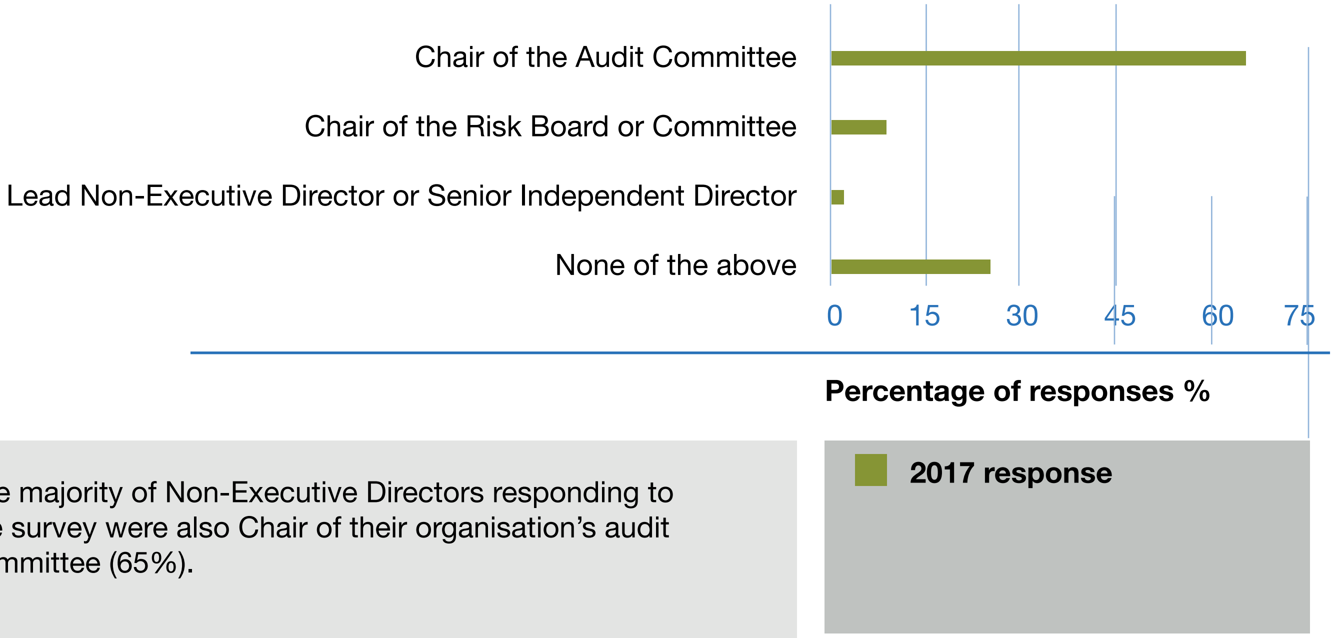
Respondent Profile

Which of the following describes you?



The majority of respondents were Non-Executives. These figures are very similar to the division of response rates between Executive Directors and Non-Executive Directors in the 2015/16 Health Check report.

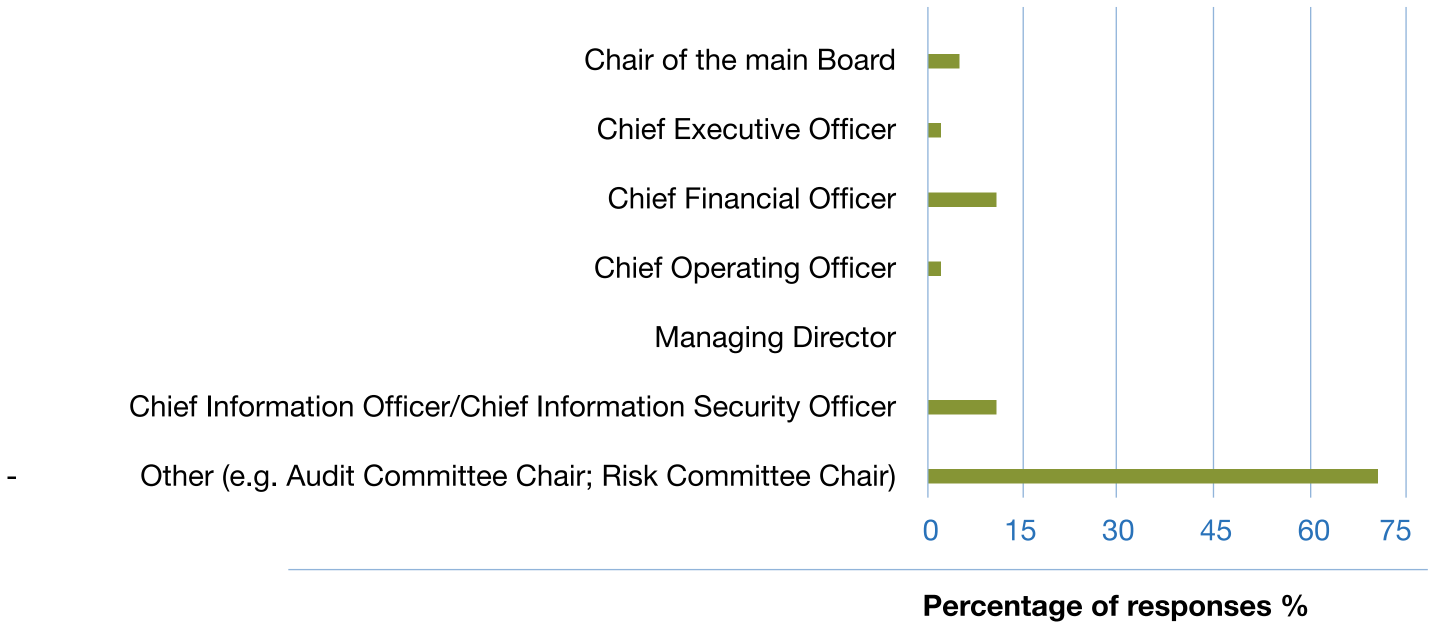
As a Director, are you also:



The majority of Non-Executive Directors responding to the survey were also Chair of their organisation’s audit committee (65%).

Respondent Profile

Which of these titles best describes your role?

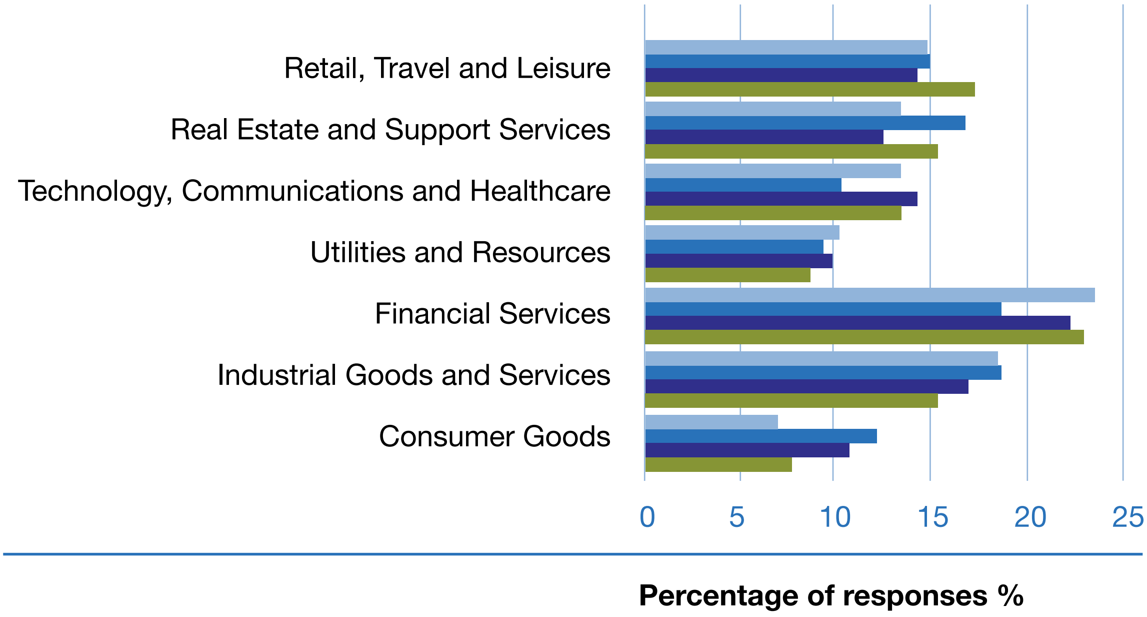


🟩 **2017 response**

The majority of individuals who took part in the survey were doing so in their role as Chair of the company's Audit Committee. The Executive Directors who took part in the survey tended to be either the Chief Financial Officer or Chief Information (Security) Officer for their organisation.

Respondent Profile

Which sector classification best applies to the company's main business?



▨	2013 response
▨	2014 response
▨	2015/2016 response
▨	2017 response

The spread of respondents by industry has remained broadly consistent throughout the different versions of the Health Check survey. For the second year running, financial services organisations provided the largest number of respondents.

Board management of cyber risk

Summary of findings

Almost all respondents indicated that their organisation's Board had either an acceptable (52%) or clear (43%) understanding of their company's key information and data assets. A larger proportion of respondents said the Board now had a clear understanding in this area, as compared with previous years.

There is a growing understanding of how businesses could be impacted by a cyber incident that affects their key assets

57% of respondents reported a clear understanding of the potential resulting impact of loss of / disruption to key information or data assets. This represents the first time that a majority of Health Check respondents reported a clear understanding of the possible impacts to their business from such an incident.

Cyber risk is seen as a top priority risk for Boards

Cyber risk is now seen as a top, or group-level risk amongst the majority of Boards (54%). Only 13% of respondents now say cyber risk is viewed as a low, or an operational-level risk for their Boards. This signifies a change in perceptions among Boards of the magnitude of cyber risk to their organisation since the Health Check survey began in 2013.

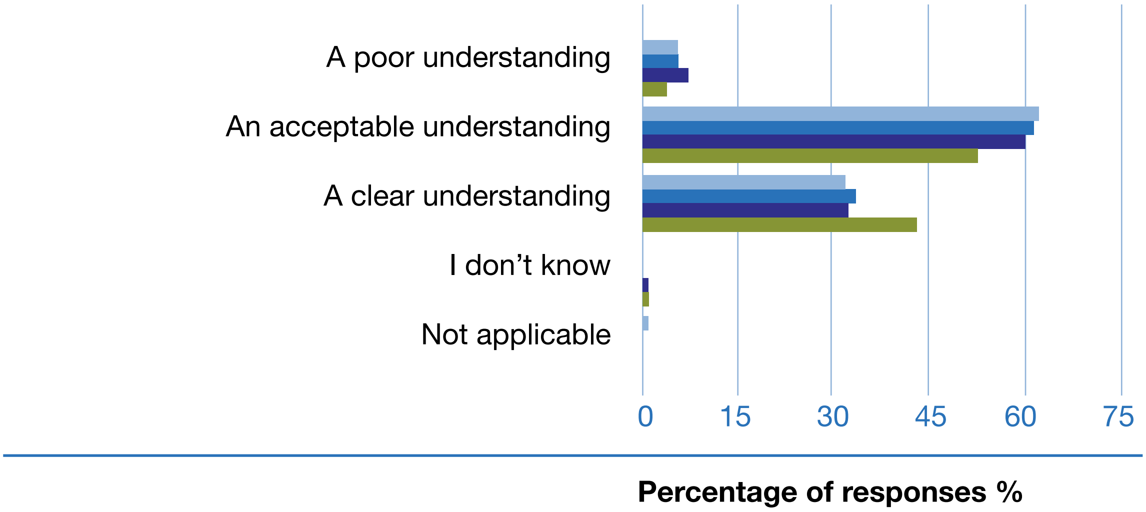
As compared with the 2015/16 Health Check, more businesses now say that their main Board's consideration of cyber risk is underpinned with comprehensive, generally informative management information (31%). However, the majority of respondents continue to say that the Board is only provided with some information on cyber risk (53%).

Boards remain split over their approach to reviewing the security of customer's data

For the first time, the largest proportion of respondents say their Board does review and challenge reports on the security of their customer's data (50%). However, there is still a small margin between those who review and challenge reports, and those who do not (46%).

Board management of cyber risk

Does the main Board have a good understanding of what the company's key information and data assets are (e.g. intellectual property, financial, corporate/strategic information, operation data, customer/personal data etc), their value to the company and to a competitor or criminal?

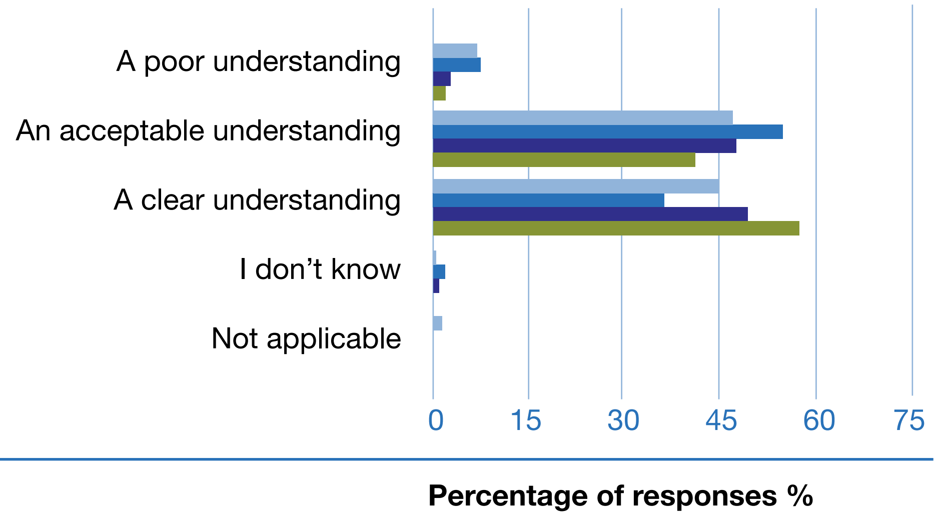


- 🟦 **2013 response**
- 🟦 **2014 response**
- 🟦 **2015/2016 response**
- 🟩 **2017 response**

There has been an increase in businesses reporting a clear understanding amongst their Boards of what the company's key information and data assets are, along with their value to different groups (43% in 2017 compared with 32% in 2015/16). The proportion of respondents reporting a poor understanding of their key information and data assets has never been higher than 7%, but there has always been a small number of organisations in this category in previous Health Check reports.

Board management of cyber risk

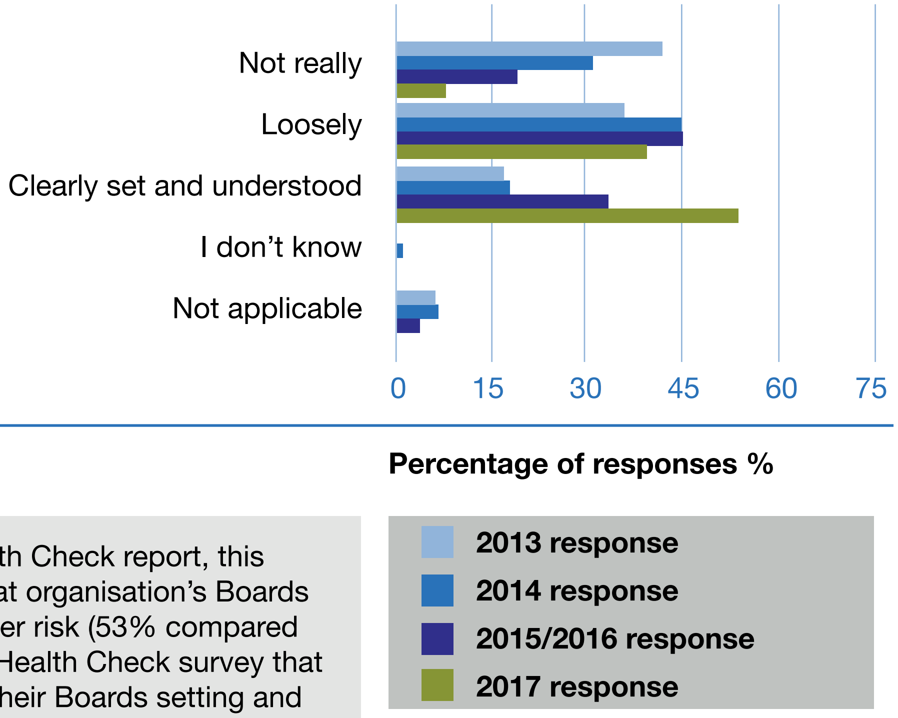
Does the main Board have a good understanding of the potential resulting impact (for example on customers, share price or reputation) from the loss of/disruption to key information and data assets (e.g. intellectual property, financial, corporate/strategic information, operation data, customer/personal data etc)?



For the first time, a majority of respondents indicated that their Board clearly understood the potential resulting impact from the loss of, or disruption to, key information and data assets for their organisation. Those organisations who continue to report either a poor / acceptable understanding of their information and assets should consider reviewing the impact of previous high-profile attacks (e.g. Bangladesh Bank, TalkTalk) upon those organisations, in terms of both financial and / or reputational impacts.

Board management of cyber risk

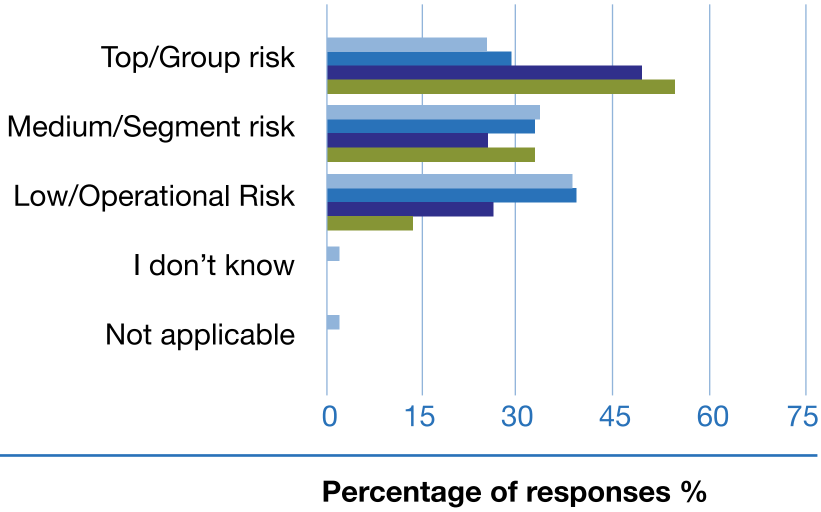
To what extent has your Board explicitly set its appetite for cyber risk, both for existing business and for new digital innovations?



As compared with the 2015/16 Health Check report, this year saw an increase in reporting that organisation's Boards had explicitly set its appetite for cyber risk (53% compared with 33%). This is the first time in a Health Check survey that a majority of respondents reported their Boards setting and understanding cyber risk appetite.

Board management of cyber risk

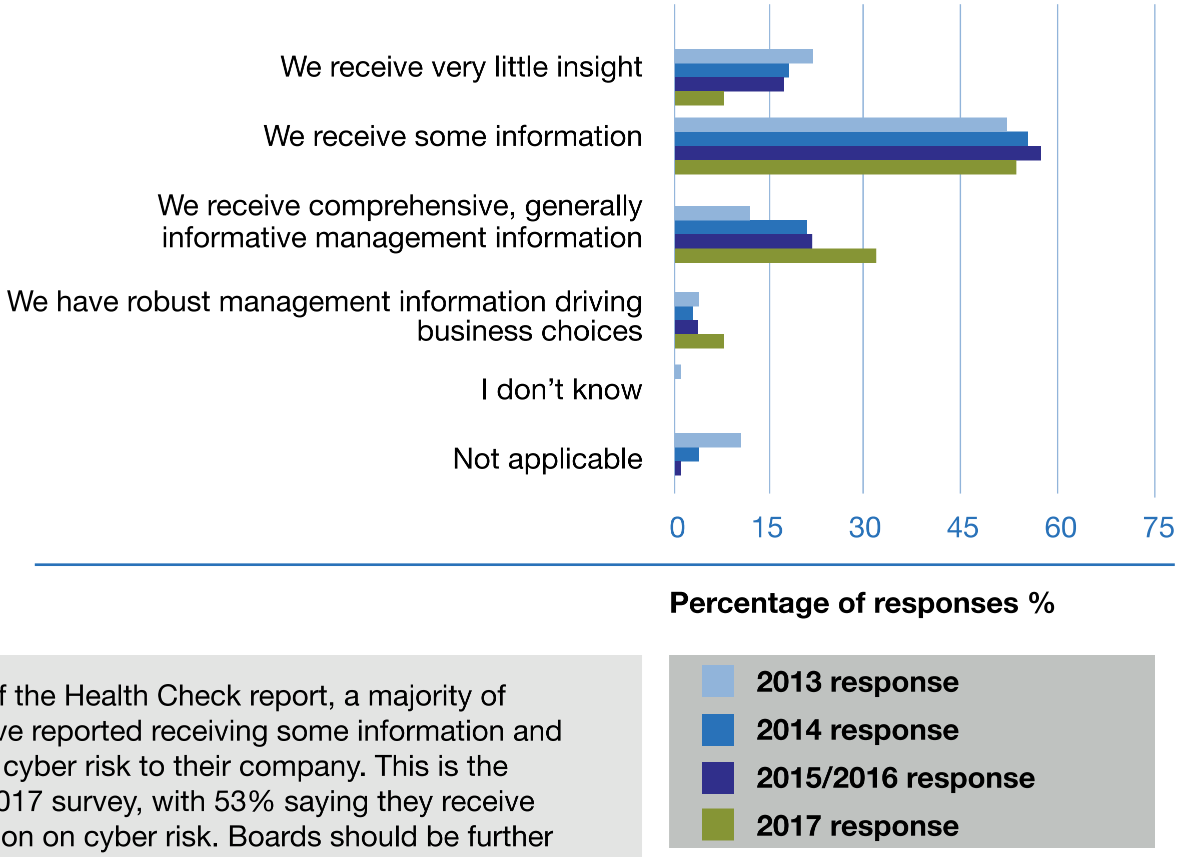
How significant or important is cyber risk, where risk is a product of likelihood and magnitude, when compared with all the risks the company faces?



Although there was only a slight increase in the proportion of respondents saying their Boards viewed cyber risk as a top, or group-level risk as compared with the 2015/16 Health Check report (54% compared with 49%), this still represents the first time that a majority of replies were in this category. Those describing cyber as a low / operational risk for their business has fallen from a high of 39% in the 2014 Health Check report.

Board management of cyber risk

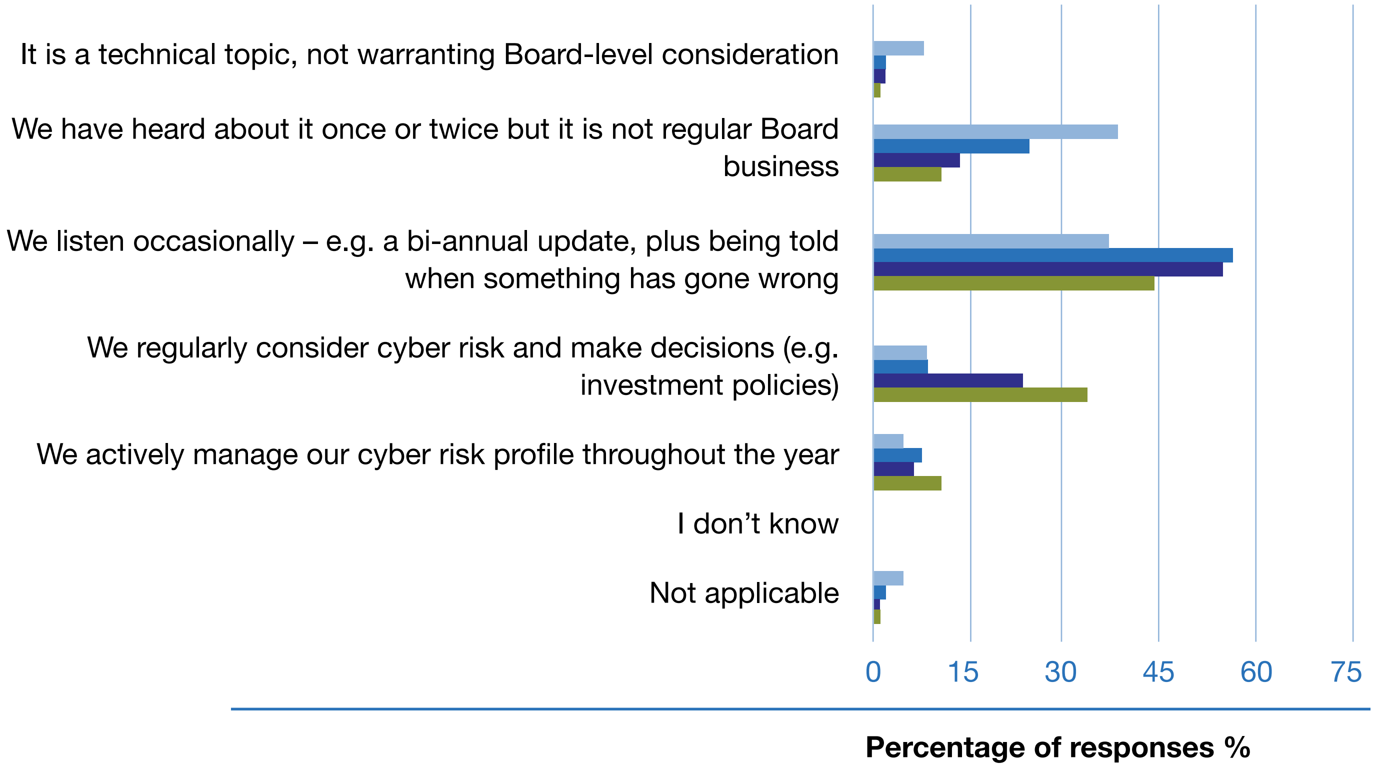
To what extent is your Board's discussion of cyber risk underpinned with up-to-date management information and threat intelligence?



In every year of the Health Check report, a majority of businesses have reported receiving some information and intelligence on cyber risk to their company. This is the same for the 2017 survey, with 53% saying they receive some information on cyber risk. Boards should be further encouraging their cyber and information security teams to make progress in this area and provide comprehensive, informative details on cyber risk where possible, in order to stay fully appraised of their organisation's capacity to handle cyber threats.

Board management of cyber risk

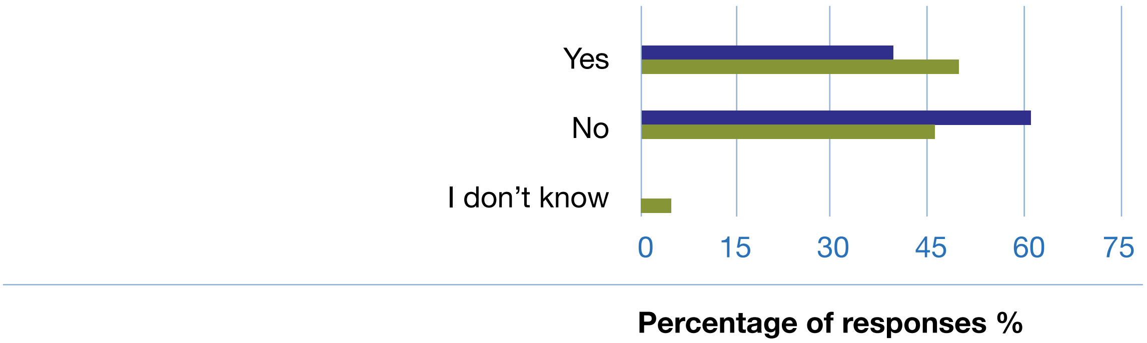
Which of the following statements best describes how cyber risk is handled in your Board governance process?



One third (33%) of responding businesses make investment decisions on their cyber security at Board level, up from 8% in the 2014 Health Check report. However, Boards should ultimately be aiming to actively manage their organisation's cyber risk profile throughout the year, such is the ever-present and significant threat posed towards FTSE 350 companies by cyber attacks.

Board management of cyber risk

Does the board review and challenge reports on the security of your customer's data?



For the first time, a majority of respondents say that their Board does review and challenge reports on the security of customer's data. With customer data being a valuable and frequent target for cyber attackers, it is important for Boards to take the lead in securing the data of their company's customers. Failure to do so could have considerable reputational costs for businesses, while also potentially resulting in fines for the loss of customer data.

Incident response

Summary of findings

Some FTSE 350 companies continue to operate without a plan for responding to a cyber incident

The vast majority of respondents reported having a plan in place to respond to a cyber incident faced by their company (90%). However, one in ten businesses surveyed said they did not have a plan in place.

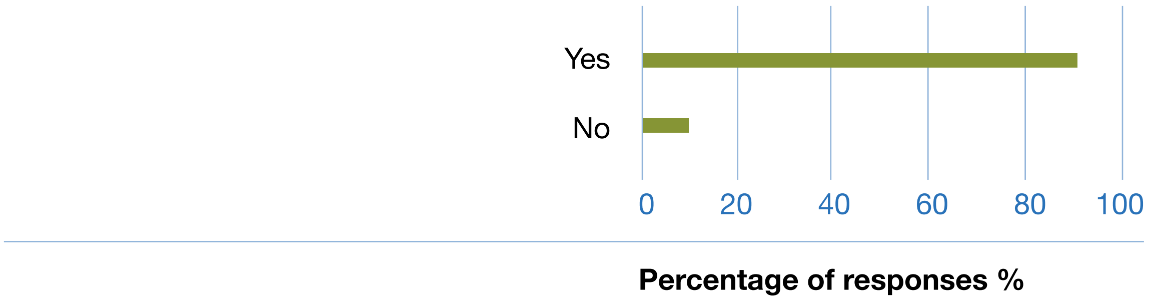
More than a quarter of Boards have no defined role in a company-wide response to a cyber incident

For those businesses with a cyber incident response plan in place, the majority said their Board had a major (17%) or minor (52%) role in their organisation’s incident response. However, over a quarter of respondents said the Board has no role to play in a response (27%).

On training for the Board to respond to a cyber incident, over two-thirds (68%) of businesses said their Board had not yet received any incident response training. While over a quarter (26%) had received some training, only 2% reported comprehensive training for their Board relating to incident response.

Incident response

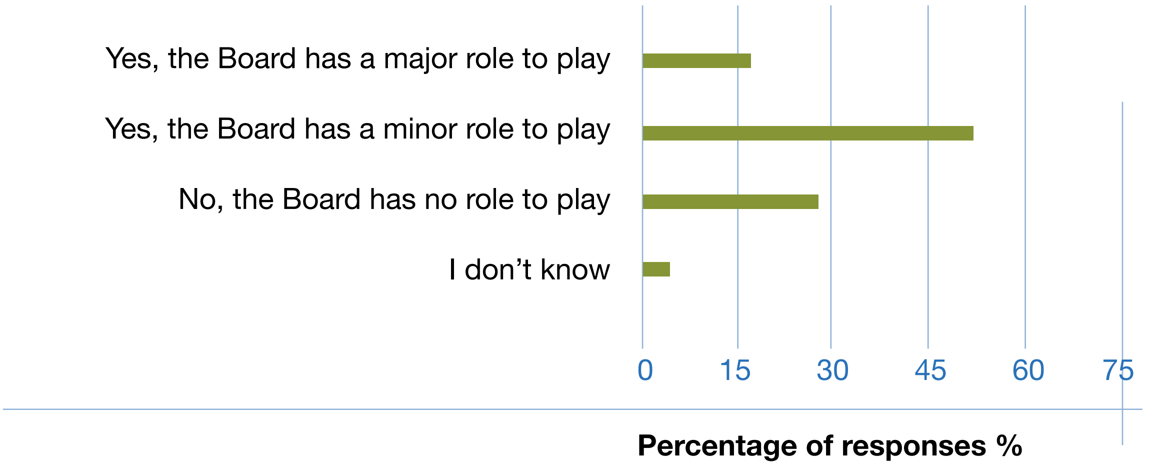
Does your company have a plan in place to respond to a cyber incident?



The findings show that one-tenth of FTSE-listed companies responding to the Health Check survey currently operate without a cyber incident plan. Boards representing this 10% of respondents should consider prioritising the development of a cyber incident response plan as soon as possible, given that their organisations are likely to be subject to regular attempts at cyber breaches owing to their high-profile status.

🟩 **2017 response**

If you do have a plan in place to respond to cyber incidents, does the Board play a role in the incident response?

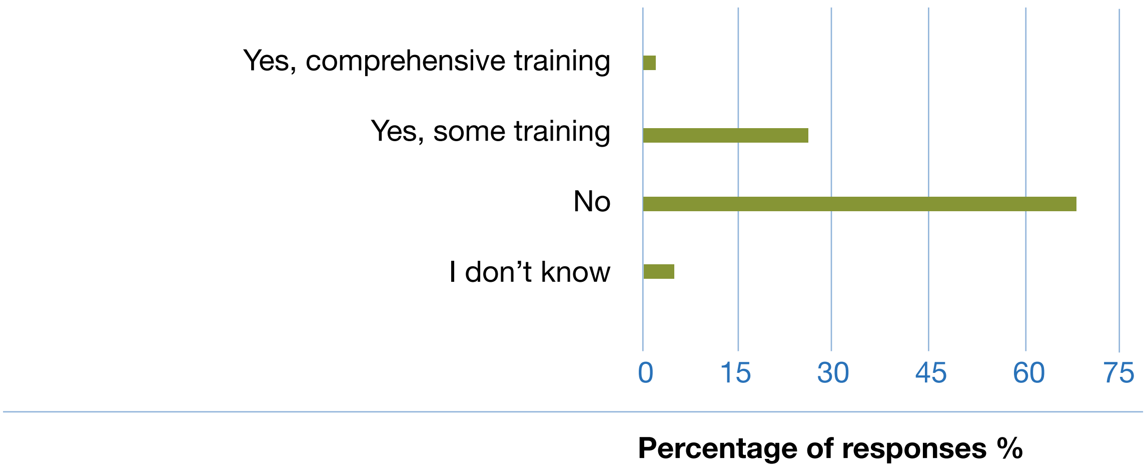


The figures show that over a quarter of Boards currently have no role in any organisational response to a cyber incident. Board members who do not currently have a role should ask why this is the case, while also trying to identify how they could offer support to their organisations should they suffer a cyber attack.

🟩 **2017 response**

Incident response

Has your board received any training to deal with a cyber incident?



More than two-thirds (68%) of respondents say that their Board has received no training in order to deal with a cyber incident within their organisation. Having a Board member trained to handle a cyber incident sends a positive message throughout a business on the importance of being prepared to handle such problems. Businesses should therefore consider designating a Board lead on cyber incidents, or facilitating training for all Board members if deemed necessary.

General Data Protection Regulation (GDPR)

Summary of findings

Awareness of GDPR and preparations to meet compliance requirements are variable

Almost all respondents reported having some level of awareness about the forthcoming GDPR and its new requirements. This level of awareness ranged from organisations being very aware (37%) to somewhat aware (45%) and slightly aware (15%).

Almost three-quarters (71%) of respondents said they were somewhat prepared to meet the new compliance requirements brought about by GDPR. However, only 6% reported being completely prepared to meet their compliance requirements.

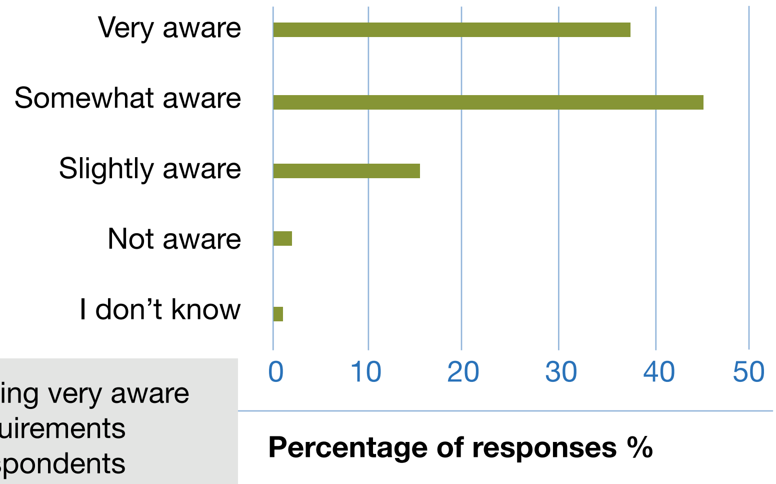
When asked which GDPR requirements were causing businesses the greatest concern in terms of meeting compliance, 45% of respondents cited an individual's rights to personal data deletion.

Boards are only occasionally giving consideration to GDPR in their meetings

On Board handling of GDPR, the largest proportion of respondents said that the matter was discussed once or twice at Board level, but was not regular Board business (42%). Just 13% said that GDPR was regularly considered by their Board.

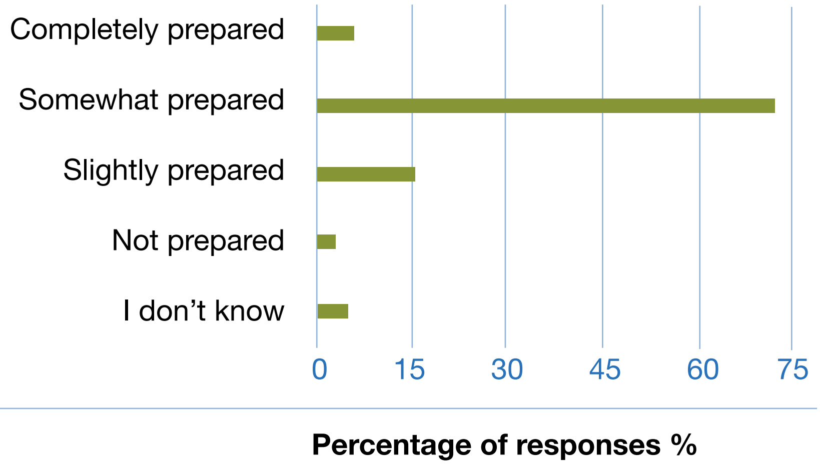
General Data Protection Regulation (GDPR)

How aware are you of the General Data Protection Regulation (GDPR) and what these new requirements will mean for your business?



Over a third of respondents (37%) reported being very aware of the forthcoming GDPR and consequent requirements for their business. However, the majority of respondents (combined 60%) reported being at best somewhat or slightly aware of the requirements for their business. Boards should be aware of how GDPR requirements will impact upon their organisation, as these requirements could have a knock-on impact for a company's cyber security services and cyber investment decisions.

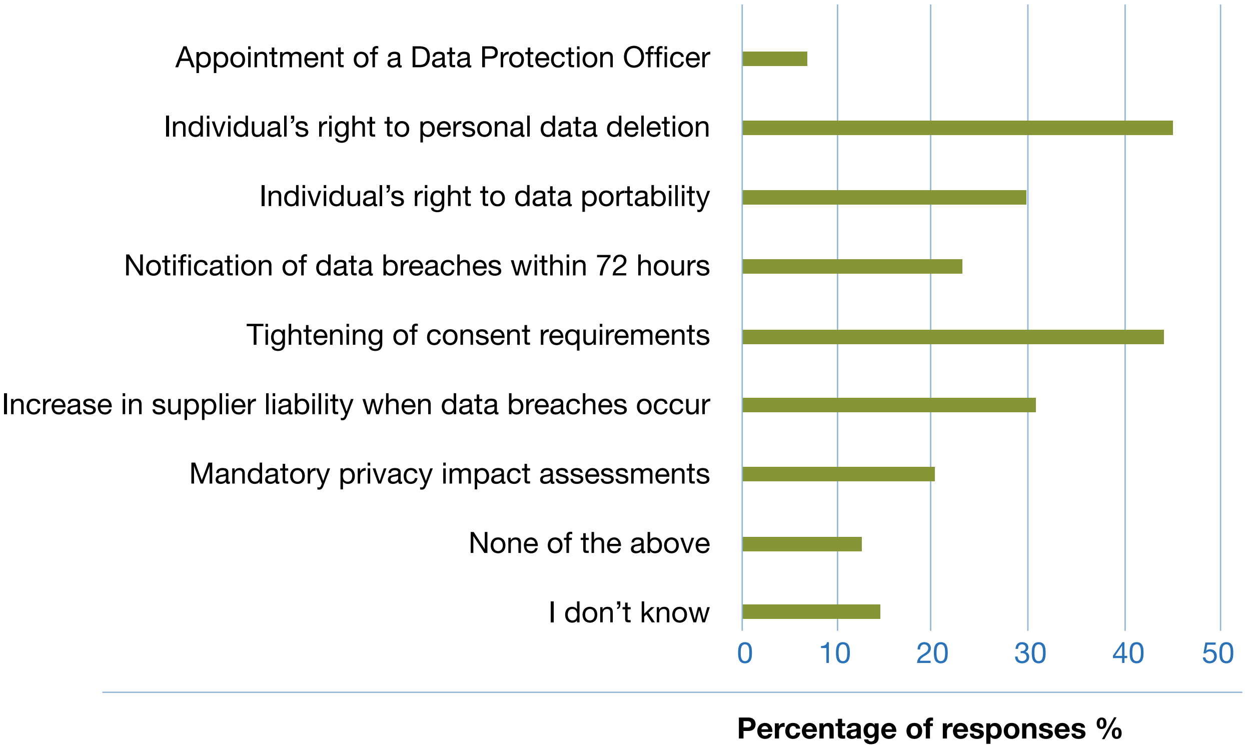
How prepared is your organisation to meet the General Data Protection Regulation (GDPR) requirements?



Only 6% of respondents reported being completely prepared to meet their GDPR requirements. With GDPR set to come into force in less than a year's time (May 2018), it is crucial for companies to be stepping up their preparations for meeting compliance requirements.

General Data Protection Regulation (GDPR)

Which of the General Data Protection Regulation (GDPR) requirements are causing you the most concern in terms of meeting compliance? Please tick all that apply.

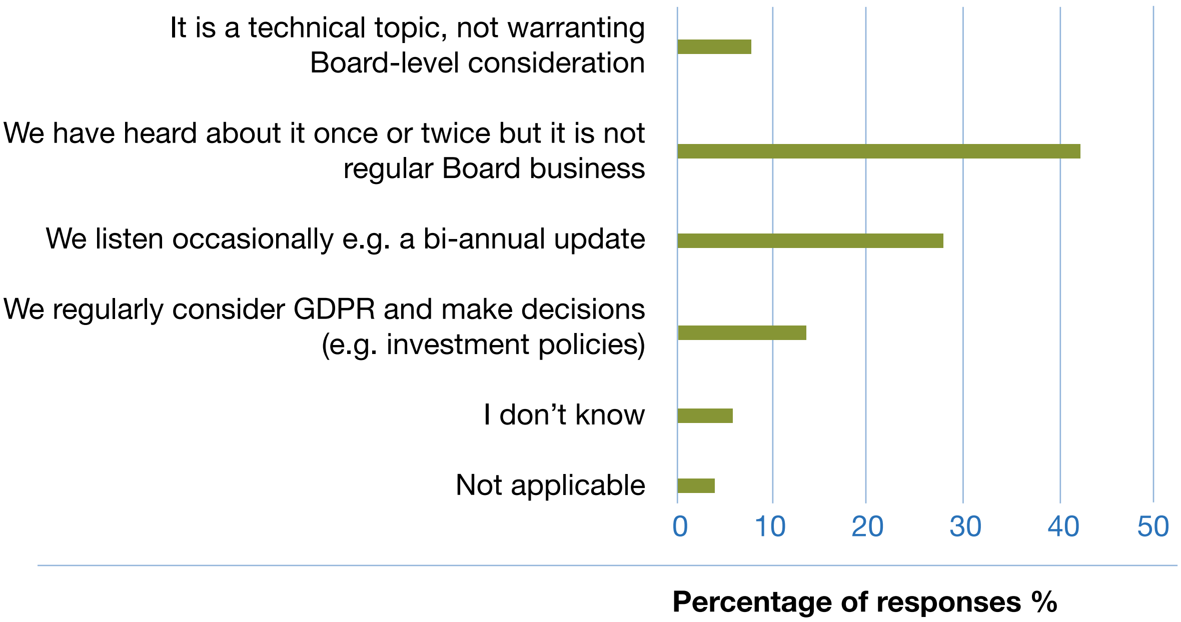


The largest proportion of respondents cited either an individual's right to personal data deletion, or the tightening of consent requirements (or potentially both) as their main concerns, in terms of their business meeting new GDPR compliance requirements. The majority of requirements are likely to affect respondents to this survey; they should therefore consult the Information Commissioner's Office's guidance on what the various new measures mean for their business, while also ensuring employees are aware of their company's requirements.

🟩 **2017 response**

General Data Protection Regulation (GDPR)

Which of the following best describes how the General Data Protection Regulation (GDPR) is being handled by your board?



The majority of respondents say that at most, their Board currently receives bi-annual updates on the GDPR, with only 13% regularly considering GDPR at Board-level. It is also notable that 4% of respondents suggest in their survey response that the GDPR requirements will not apply to their organisation. GDPR will almost certainly apply to all respondents to this survey, and all those within the FTSE 350. Therefore, Boards should now have GDPR as a regular agenda item in their Board discussions.

Methodology

This report is a collation of the anonymous responses of the FTSE 350 company Board members that responded to the survey. The report provides a picture of the respondents' approaches to cyber security governance and should be indicative of the views of large companies on these issues.

For the 2017 Health Check report, audit partners engaged with their clients to identify the most suitable Board member, executive or non-executive, to respond to the survey. The majority of respondents were non-executives, many of whom were Chair of their organisation's audit committee.

In the 2014 and 2015/16 surveys, the primary focus was also on engaging the audit committee Chair, with a recommendation that questions were discussed with the Board Chair and colleagues prior to final submission.

Figures in charts

Where figures in charts do not add to 100% this is due to rounding of percentages or because the questions allow more than one response.

Naming of Health Check surveys

Please note that this year's Health Check ran from 18th April 2017 to 14th June 2017. The previous report is described as the '2015/16 Health Check' as the fieldwork took place across both 2015 and 2016.

Annex A

Aggregated Sectors

Consumer Goods
Electronic and Electrical Equipment
Food and Beverages
Tobacco
Automobiles and Parts
House, Leisure, and Personal Goods

Financial Services
Financial and General
Banks
Insurance

Industrial Goods and Services
Industrial Engineering
Industrial General
Industrial Transportation
Chemicals
Aerospace and Defence
Construction Materials

Retail, Travel and Leisure
Retailers
Travel and Leisure

Real Estate and Support Services
Real Estate
Support Services

Technology, Communications and Healthcare
Health Care Equipment and Services
Media
Pharmaceuticals and Biotech
Tech Hardware
Tech Software and Services
Telecommunications

Utilities and Resources
Mining
Oil and Gas
Basic Resources (excl mining)
Utilities

Annex B

HMG Cyber Security Initiatives

Action Fraud
Action Fraud is the UK's single point for reporting all fraud and online financial crime. Crime can be reported online 24 hours a day, seven days a week, and the Action Fraud call centre can also be contacted to report crimes during working hours and at the weekend.

When a serious threat or new type of fraud is identified, Action Fraud will place an alert on its website, which contains advice for individuals and businesses to protect themselves from becoming victims of fraud.

www.actionfraud.police.uk

Cyber Aware
Cyber Aware (formerly Cyber Streetwise) aims to drive behaviour change amongst small businesses and individuals, so that they adopt simple secure online behaviours to help protect themselves from cyber criminals. These include: using strong passwords made up of three random words and always downloading the latest software updates as soon as they appear.

www.cyberaware.gov.uk

Cyber Essentials
Cyber Essentials is a Government-backed and industry supported scheme to guide businesses in protecting themselves against cyber threats. The Cyber Essentials scheme provides businesses - large and small - with clarity on good, basic cyber security practice. By focusing on basic cyber hygiene, companies will be better protected against the most common cyber threats. The Cyber Essentials badge allows your company to demonstrate that it adheres to a Government-endorsed standard. These technical essentials form part of the broader agenda described in the Ten Steps to Cyber Security guidance.

All suppliers must be compliant with the Cyber Essentials controls if bidding for government contracts which involve handling of sensitive and personal information and provision of certain IT products and services.

www.cyberaware.gov.uk/cyberessentials

HMG Cyber Security Initiatives

Cyber Security Information Sharing Partnership (CiSP)
CiSP facilitates the sharing of information and intelligence on cyber security threats in order to make UK businesses more secure in cyberspace. CiSP includes a secure online collaboration environment, where government and industry (both large businesses and SMEs) partners can exchange information on threats and vulnerabilities in real time.

www.ncsc.gov.uk/cisp

National Cyber Crime Unit (NCCU)
The NCCU, as part of the National Crime Agency (NCA), is the UK lead for the investigation of the most serious and organised incidents of cyber crime. The NCCU supports domestic and international law enforcement, and the wider NCA, to take responsibility for tackling cyber and cyber-enabled crime affecting the UK.

The NCCU is accessible to partners; responding dynamically to threats, providing expert advice, guidance and feedback. The NCA is not a crime reporting agency, so any reports of crime should be reported to Action Fraud (see above).

www.nationalcrimeagency.gov.uk

National Cyber Security Centre (NCSC)
The National Cyber Security Centre (NCSC) is the UK's authority on cyber security. The NCSC is a part of GCHQ, bringing together and replacing the information security arm of GCHQ (CESG), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT-UK) and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI).

The NCSC's main purpose is to reduce the cyber security risk to the UK by improving its cyber security and cyber resilience. It works together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. This is underpinned by world class research and innovation.

www.ncsc.gov.uk

FTSE 350 Cyber Governance Health Check Report 2017

This publication is also available on our website at
www.gov.uk/dcms

Any enquiries regarding this publication should be sent to:

Department for Digital, Culture, Media and Sport
100 Parliament Street
London SW1A 2NH

Tel: 020 7211 6000

enquiries@culture.gov.uk

If you require this publication in an alternative format, email enquiries@culture.gov.uk ,
or call 020 7211 6000.