HM Government

FTSE 350
Cyber Governance Health Check Report 2015

May 2016

FTSE 350 Cyber Governance Health Check Report 2015

Contents

Foreword

I'm delighted to present the third annual Cyber Governance Health Check of FTSE 350 companies.

As we continue to witness a worldwide digital revolution I am pleased so many UK companies are embracing modern technological developments and pioneering new digital products and services. The digital economy in the UK is strong and growing - and is now embedded in our everyday lives.

We expect our online services to be quick, efficient and user-friendly. We also expect them to be secure. We trust businesses to look after our personal data and financial information. So whilst UK businesses are leading the way in digital innovation, they also need to lead the way in cyber security. This is why the Government's national cyber security strategy aims to make the UK the safest place in the world to do business in cyber space.

As part of our strategy we launched the cyber governance health check in 2013 to test how well the UK's top 350 companies are managing cyber risks. As well as providing a picture of how well corporate Britain is responding to the threat, the health check also enables individual firms to benchmark themselves against their peers and identify where they need to take action to better protect themselves.

The companies involved recognised the benefits and embraced the initiative, paving the way for a second year which allowed us to benchmark progress and demonstrate the positive action being taken in many areas. However, it also showed there was much more for companies to do in understanding of the impact a cyber attack and what needs to be done to protect their business.

I launched this year's cyber health check in the wake of the TalkTalk cyber attack and several other high profile breaches. There is no doubt that since then the issue has shot up the public agenda and industry is more aware of the threat than ever.

The UK's biggest companies have recognised this and are taking action. This report shows company boards are improving their understanding of cyber risks and taking them more seriously than ever before. However progress needs to be made in understanding where key data is shared with third parties and the impact if this goes wrong.

I would like to thank all of the FTSE 350 board members and staff who have contributed towards this report. I am also very grateful to our partners in the audit community - Deloitte, EY, Grant Thornton, KPMG and PWC - for their crucial support in helping to deliver the Cyber Governance Health Check.

I'm determined to ensure the UK leads the way in cyber security. I urge all businesses to use the findings in this report and, together with your trusted advisors, act on them.

Ed Vaizey - Minister of State for Culture and the Digital Economy

Executive Summary

63%
of boards
clearly set out their risk management approach in their annual reports

33%
of boards
have clearly set and understood their appetite for cyber risk

UP from **18%** in 2014

49%
of businesses
place cyber risk as a top risk (compared to other risks faced)

UP from **29%** in 2014

16%
of boards
have a very clear understanding of where the company's key information/data assets are shared with third parties

UP from **11%** in 2014

49%
of boards
have a clear understanding of the potential impact of loss/disruption of key information and data assets

77%
of businesses
have allocated budget specifically to protect consumer data

Introduction

The UK faces a growing threat of cyber attacks from states, serious crime gangs, hacking groups as well as terrorists. The industrial-scale theft of intellectual property, as well as the numerous phishing and malware scams that waste time and money, threatens our economic well-being. The government is committed to working in partnership with industry to address this and make the UK one of the most secure places in the world to do business online.

The Cyber Governance Health Check supports this objective. Focused on FTSE 350 companies, it offers significant insight into the cyber governance of the UK's highest-performing businesses.

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 business.

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 the firms which currently audit the FTSE 350: Deloitte, EY, Grant Thornton, KPMG and PwC. The governance behaviours, findings and guidance contained within this report should enable many large and small businesses to improve their understanding and management of risks that have the potential to cause major damage to their business.

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

Respondent Profile

Summary of findings

The vast majority of respondents (79%) were non-executives, the same proportion as the previous year.

Of those that were executive directors 75% were Chief Financial Officers and 20% were the Chief Executive Officers. In 2015 there were no responses from those who are Chair of the Main Board, compared to 25% in 2014 and 85% in 2013.

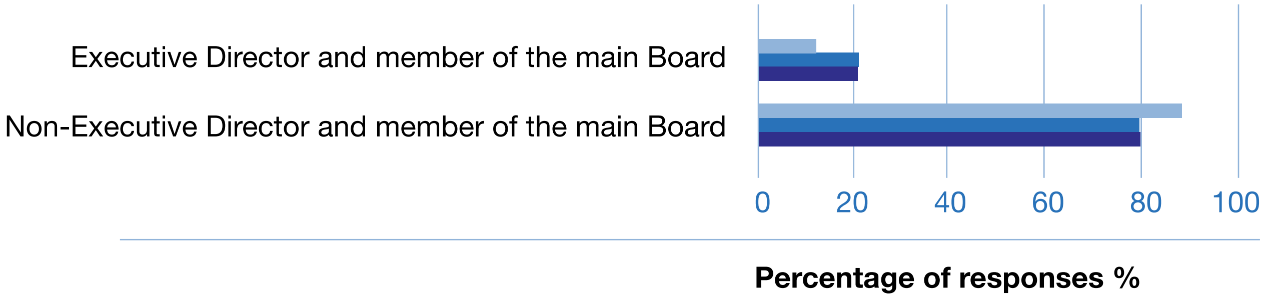
Of the non-executives almost all were the Chair of the Audit Committee in the last three years (92% in 2015, 96% in 2014 and 93% in 2013).

Overall 113 companies responded to the survey in 2015, compared to 108 in 2014 and 218 in 2013, this was an increase of 5% between 2014 and 2015. When compared to 2014, response rates varied considerably between sectors. The greatest fall was seen in ‘Real estate and support services’ (-22%) and the greatest increase was found in ‘Tech, comms and healthcare’ (+45%).

Over two thirds (65%) of respondent companies’ shareholder value was significantly dependent on securing critical information assets (down from 66% in 2014 but an increase from 53% in 2013). In addition to this, 42% of respondent companies handle high value financial transactions or other assets at high risk from theft or fraud (up from 39% in 2014 and 38% in 2013). Only 18% of respondents had more than 50% of their revenue from online interactions (14% in 2014, 19% in 2013).

Respondent Profile

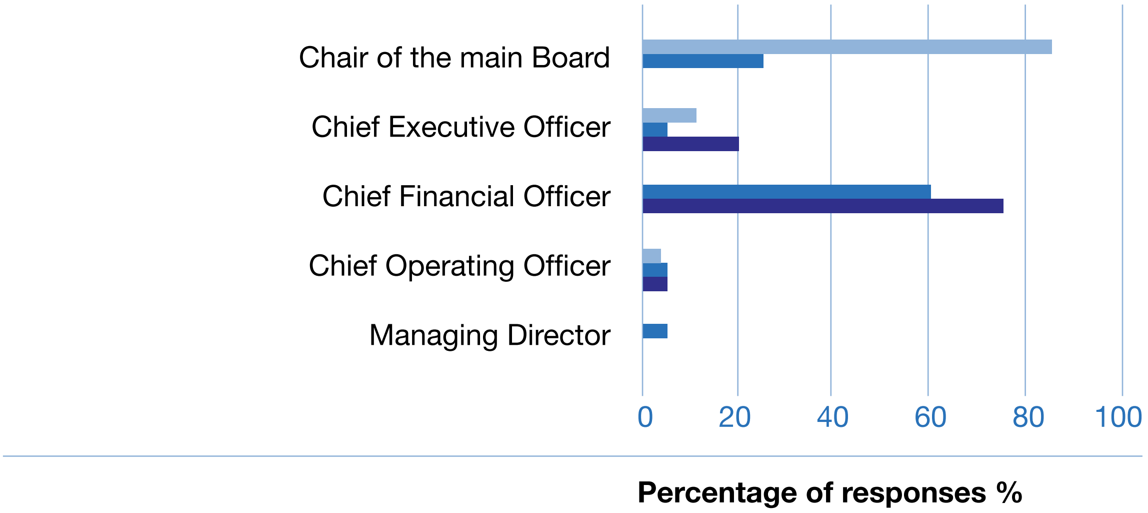
Which of the following describes you?



The majority of respondents were non-executives.

- **2013 response**
- **2014 response**
- **2015 response**

Which of these titles best describes your role?

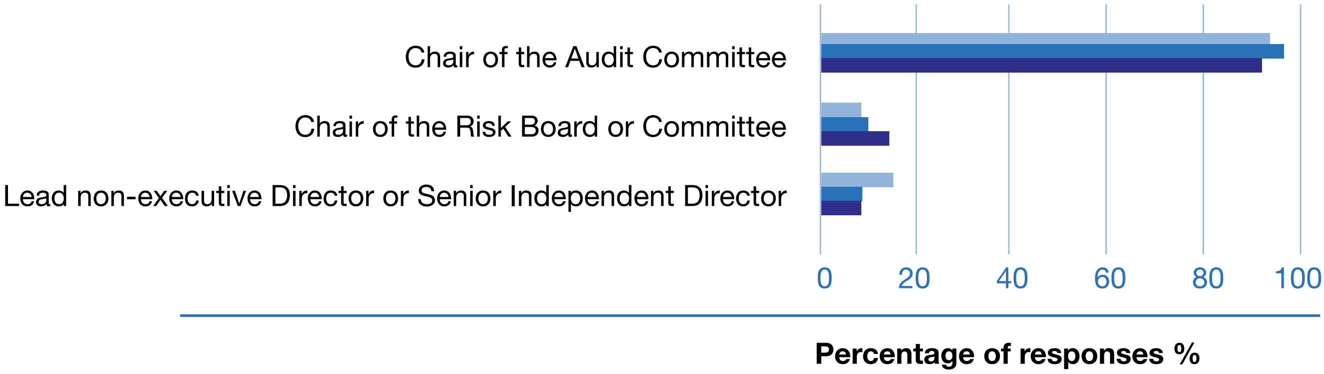


Executive director respondents were most likely to be Chief Financial Officers, similar to 2014. This differs to 2013 where respondents were most likely to be Chair of the Main Board

- **2013 response**
- **2014 response**
- **2015 response**

Respondent Profile

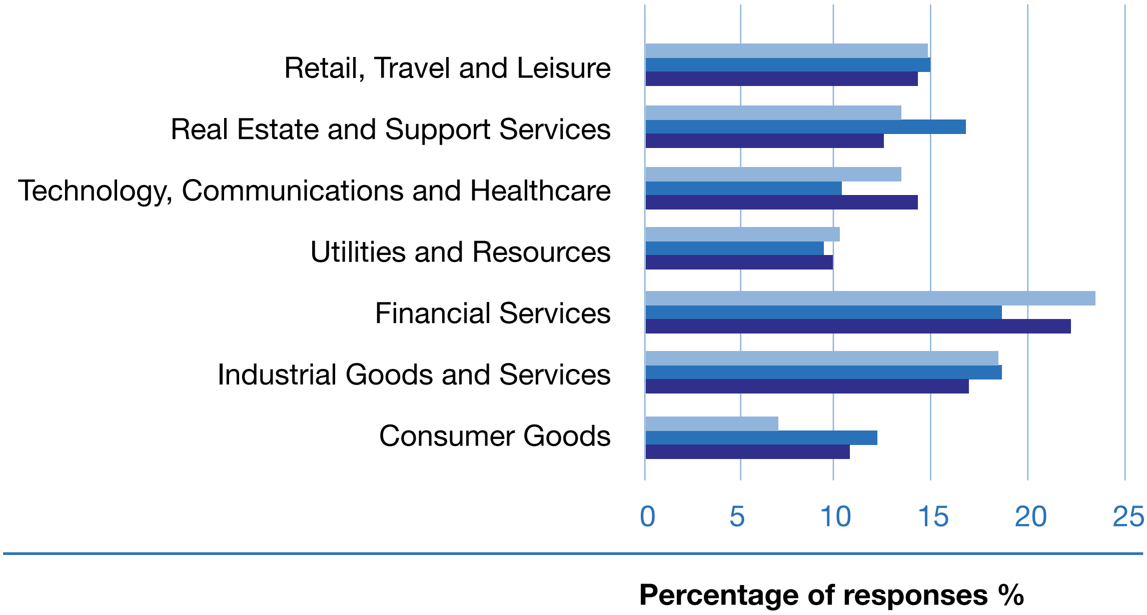
As a non-executive Director, are you also:



Non-executive directors were almost all audit committee chairs.

Respondent Profile

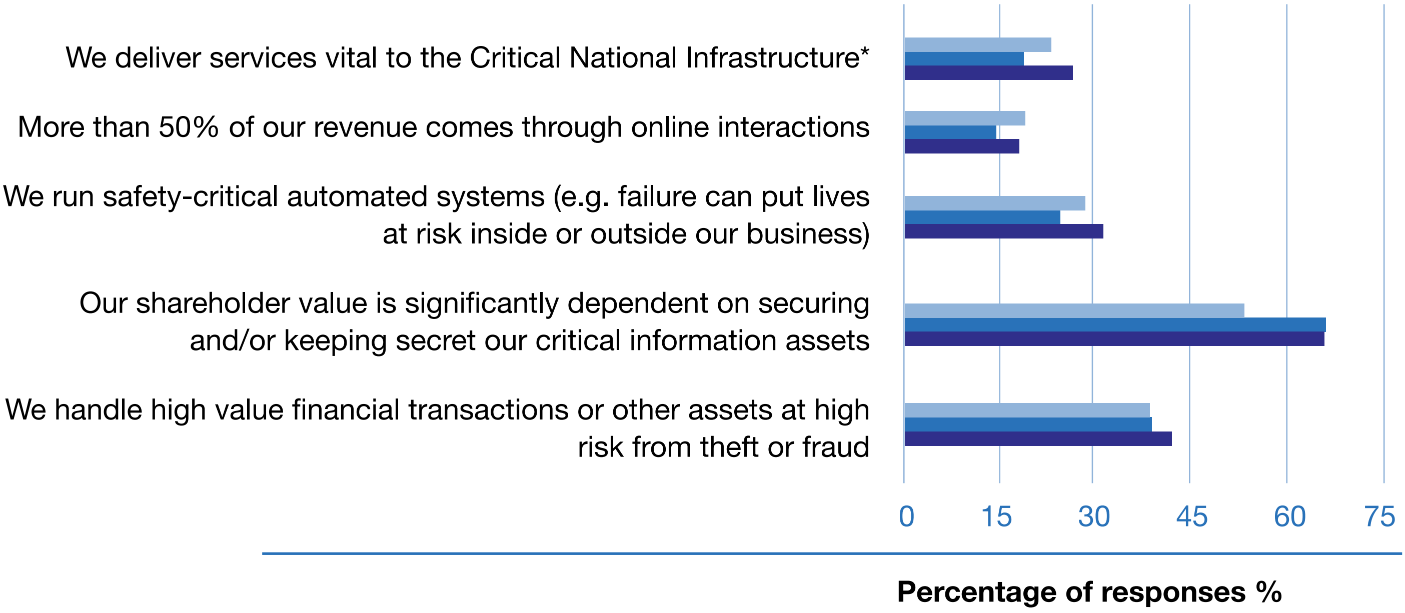
Which sector classification best applies to the company's main business?



The spread of industries was similar to previous years. The largest sector was 'Financial services' and the smallest sector was 'Utilities and resources'.

Respondent Profile

Please indicate if any of the following risk factors apply to your company



In all three years, a large proportion of respondents had shareholder value that was significantly dependent on security critical information assets or were involved in handling high value financial transaction or other assets at high risk of theft or fraud.

**defined as "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends"*

Understanding the Threat

Summary of findings

All respondents reported that the main boards they served either had an acceptable understanding (60%) or a clear understanding (32%) of what their key information and data assets were. This result is almost exactly the same as in previous years. The tech, comms and healthcare industry had the highest proportion of audit chairs reporting a clear understanding of the threat.

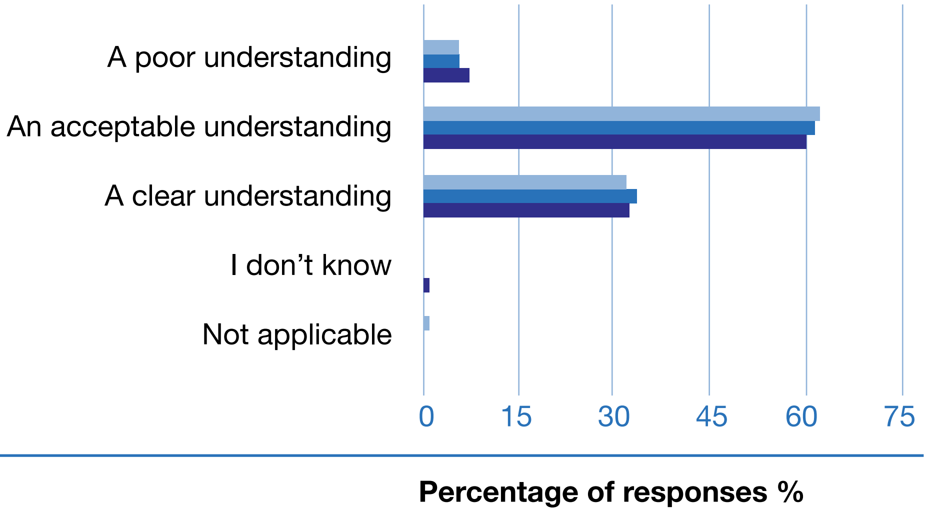
When asked about their main board's understanding of the potential resulting impact of loss or disruption to their key information and data assets, just under half (49%) of audit chairs thought they had a clear understanding, with a further 47% having an acceptable understanding and 3% a poor understanding. The retail, travel and leisure industry were the most likely to have a more favourable view of their boards in this respect, with 63% reporting a clear understanding.

Whilst few (12%) of main boards regularly and thoroughly review their key information and data assets, this has increased on previous years. A quarter (25%) report that they do so regularly and somewhat thoroughly, and much like in previous years the majority rarely (41%) or never (19%) do so. These results are consistent with previous years, however are slightly more positive than in 2014, with fewer boards rarely or never reviewing this information (60% in 2015 and 65% in 2014).

Over half (57%) of boards' discussion of cyber risk is underpinned by "some" up-to-date management information and a further 21% received "comprehensive, generally informative" management information. Of the remaining boards, 17% received very little insight. Businesses in the utilities and resources sector were more likely to base their discussions on more complete information (with 36% receiving comprehensive, generally informative management information).

Understanding the Threat

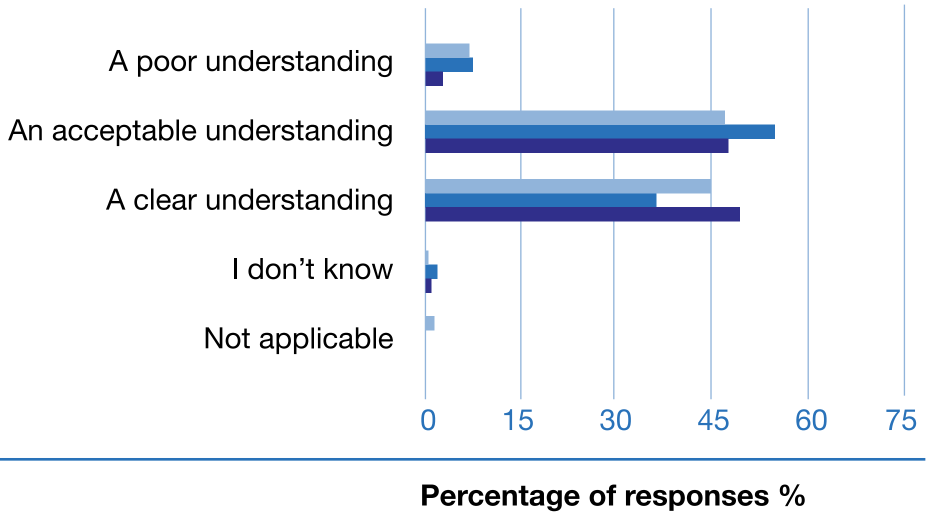
Does the main Board have a good understanding of what the company's key information and data assets are (e.g. IP, financial, corporate/strategic information, operational / transaction data, customer/personal data, etc), their value to the Company and to a competitor or criminal?



As in previous years, most respondents believe their main boards only have a basic or acceptable understanding of what their company's key information and data assets were.

Understanding the Threat

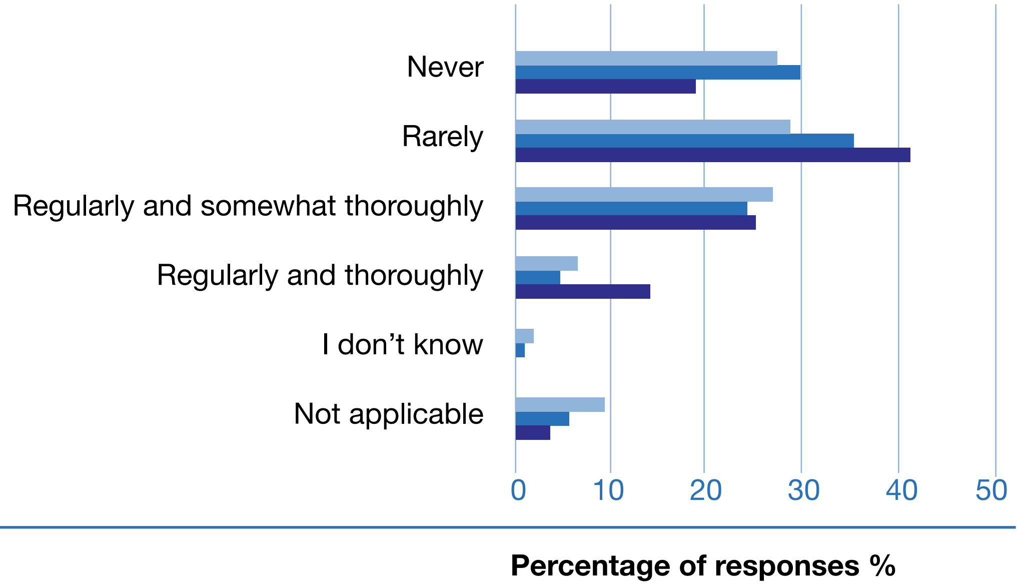
Does the main Board have a good understanding of the potential resulting impact (for example, on customers, share price or reputation) from the loss of/disruption to key information and data assets (e.g. IP, financial, corporate/strategic information, operational / transaction data, customer/personal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



Almost all respondents thought that the main board had a clear or acceptable understanding of the potential resulting impact from the loss of/disruption to key information and data assets. A small proportion reported a poor understanding.

Understanding the Threat

Does the main Board periodically review key information and data assets (especially personal data) to confirm the risk management, legal, ethical and security implications of retaining them?

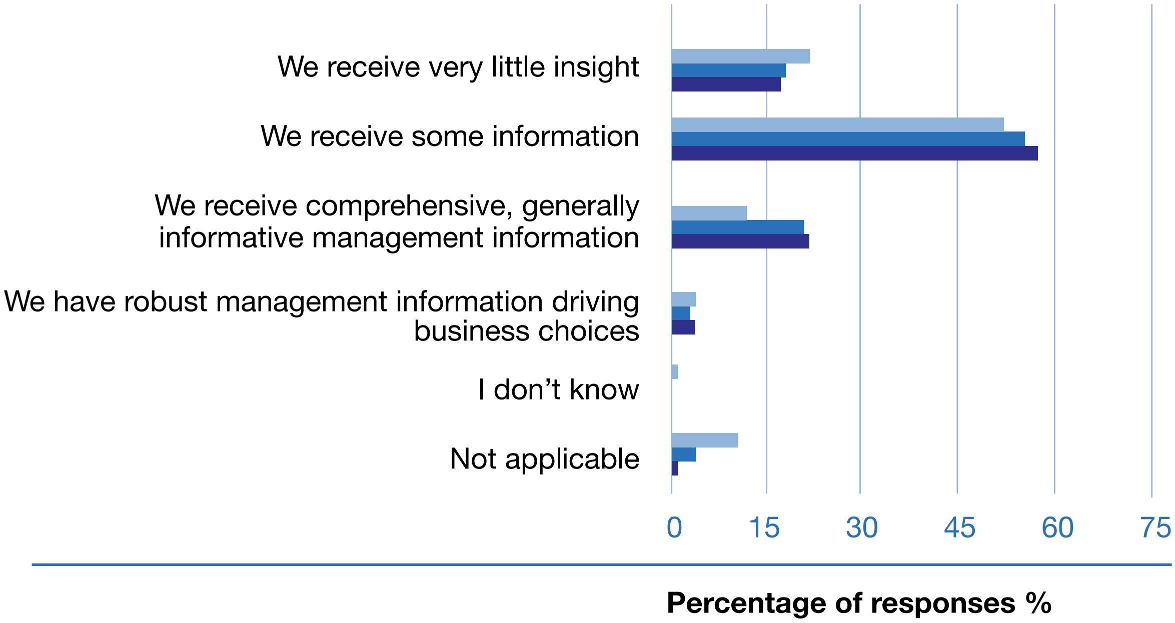


In 2015, audit chairs reported that main boards were more likely to regularly and thoroughly review key information and data assets on a regular basis than in previous years.

- ▨ **2013 response**
- ▨ **2014 response**
- ▨ **2015 response**

Understanding the Threat

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



In 2015, over half of boards' discussion of cyber risk was underpinned by some up-to-date management information and threat intelligence

Leadership

Summary of findings

Audit chairs anticipated that net cyber risk would increase slightly (57%) or stay the same (19%), with a smaller proportion (13%) foreseeing a significant increase. This is less optimistic than in previous years, with a greater proportion (71%) anticipating that there will be a slight or significant increase, compared to 58% in 2014 and 65% in 2013.

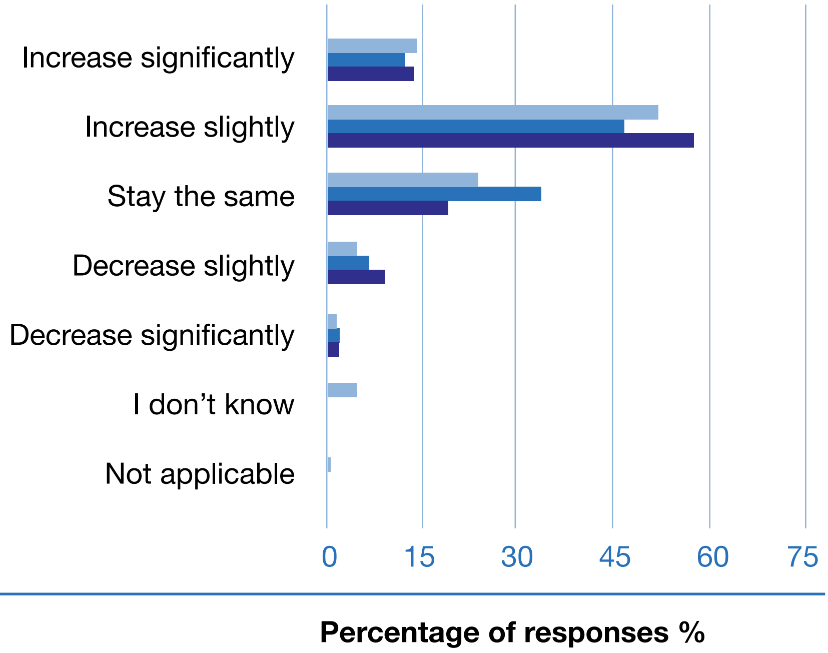
For a large proportion of boards (54%), cyber risk is a subject that they only hear about occasionally – either bi-annually or when something has gone wrong. This is a similar proportion to 2014, however an increase on 2013 (37%). A further 23% of boards regularly consider cyber risk and make decisions – an increase on previous years (8% in both 2014 and 2013). Despite this, 15% of boards reported that they have either heard about it once or twice, or view cyber risk as a technical topic that does not warrant board level discussions. This has decreased from 26% in 2014 and 46% in 2013. There have been positive increases across the board, with a greater proportion regularly considering cyber risks and making decisions in almost every sector since 2013.

Almost half (49%) of audit chairs said that their boards had the right skills, to a "significant degree" to manage innovation and risk in the digital world, this is an increase on previous years (38% in 2014 and 39% in 2013). A further 41% responded that their boards had the right skills "to a limited degree", and only 6% believed that their board were fully informed and skilled. This was consistent with 2013 (7%), however dropped to 1% in 2014.

In 2015, almost two thirds (63%) of respondent boards had outlined their approach to risk management clearly in their annual reports, with a further 5% outlining this on their websites. A small proportion (3%) admitted that they had not yet outlined a robust approach to cyber security.

Leadership

Is net cyber risk*expected to increase or decrease, in terms of likelihood of occurrence, over the next year or so?

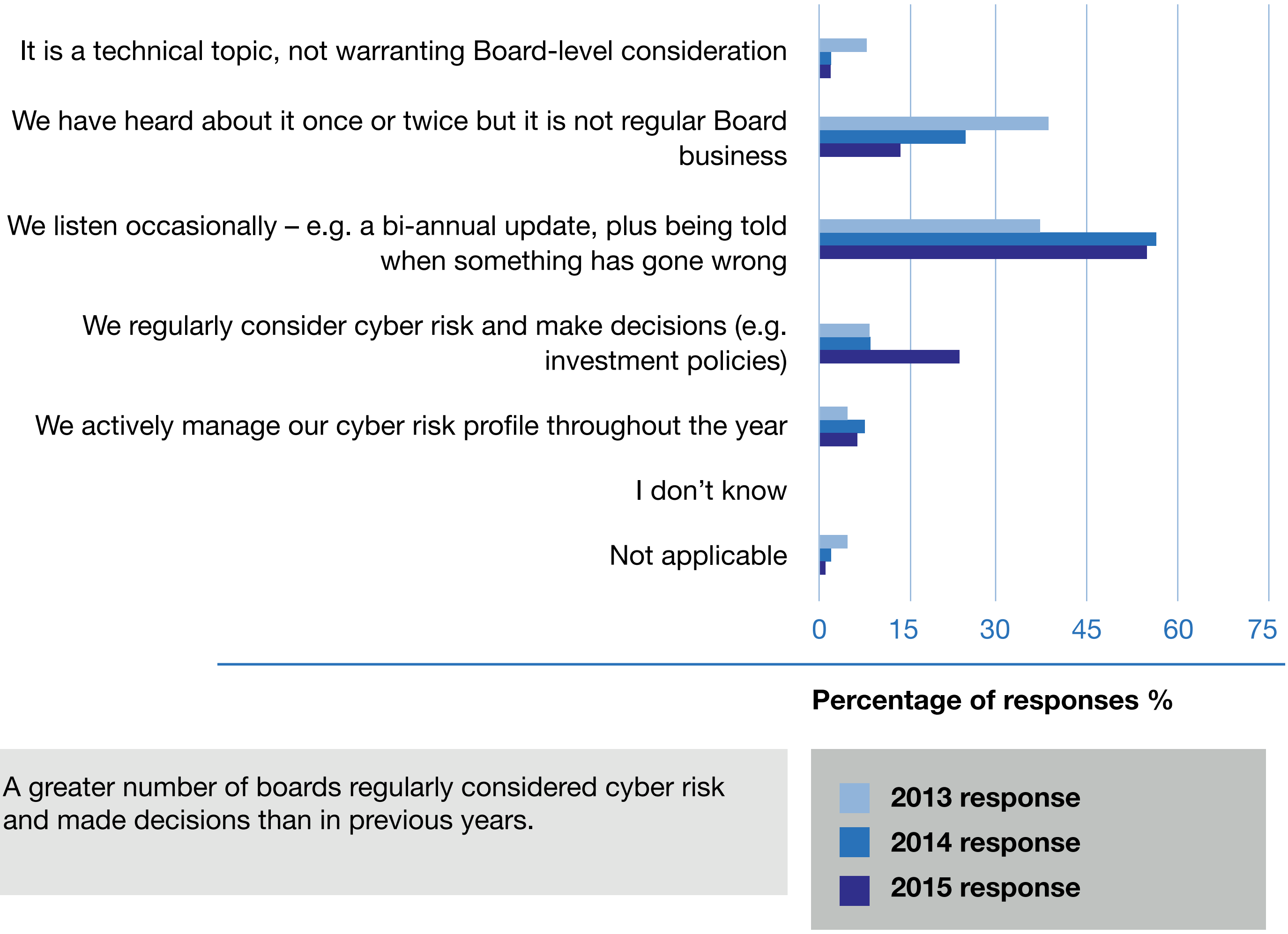


Boards expect net cyber risk to increase rather than decrease over the next year or so, and are less optimistic about this than in previous years.

***i.e. the assessment of cyber risk once company controls and processes already in place have been taken into account.**

Leadership

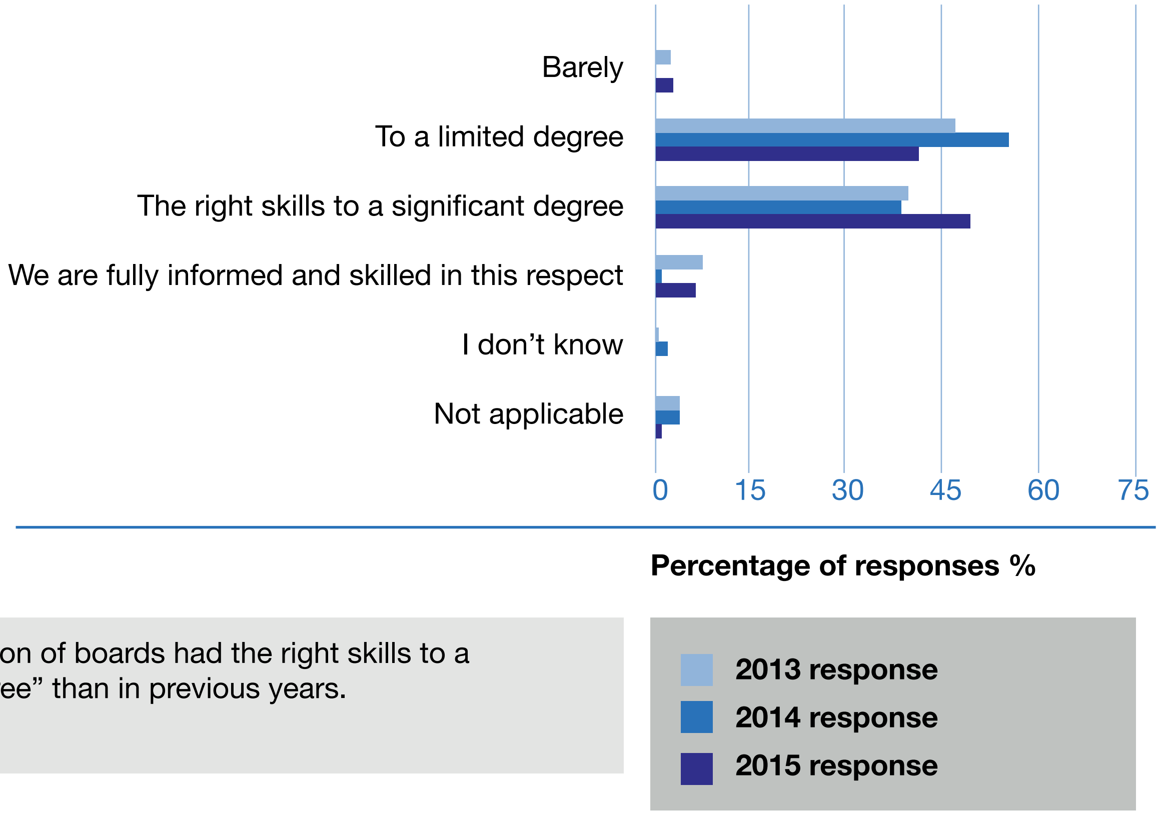
Which of the following statements best describes how cyber risk is handled in your Board governance process?



A greater number of boards regularly considered cyber risk and made decisions than in previous years.

Leadership

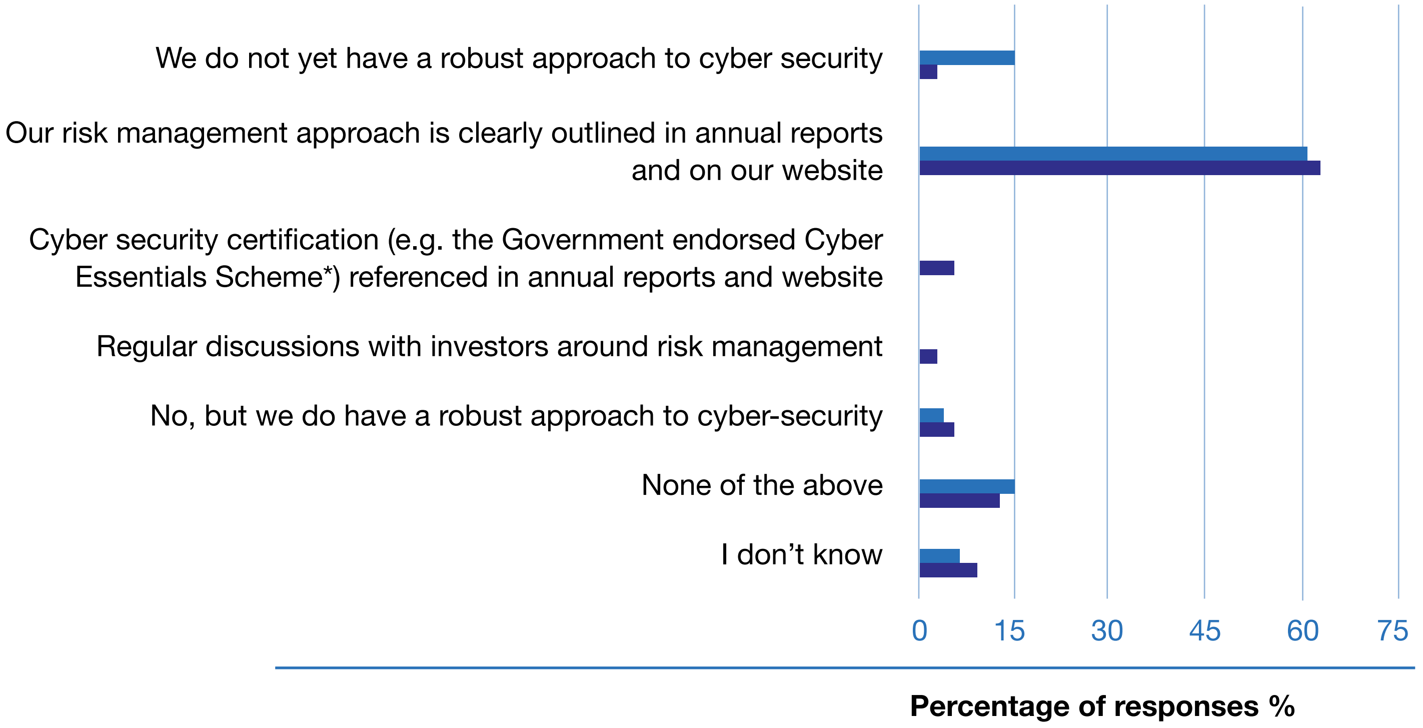
Taking account of the differing contributions of both executive and non-executive members, to what extent does your board have the right skills and knowledge to manage innovation and risk in the digital world?



A larger proportion of boards had the right skills to a "significant degree" than in previous years.

Leadership

How has the board sought to reassure investors and customers of its robust approach to the cyber security of personal data?



Many companies publicise their cyber security policy in their annual reports or on their website. A small proportion have no approach to cyber security of personal data.

** Cyber Essentials Scheme* https://www.cyberstreetwise.com/cyberessentials/

Risk Management

Summary of findings

The majority of respondents (90%) felt that cyber risks were either reasonably or clearly described in the company's risk register. There were not really notable sectoral differences in those who felt that cyber risks were either reasonably or clearly described, with high results across the board.

Boards were more likely to explicitly set their appetite for cyber risk in 2015 than in previous years. One third (33%) had this "clearly set and understood", an increase on 18% in 2014 and 17% in 2013, and a further 45% had loosely set their appetite (a similar proportion to 2014 and an increase on 2013). Only 19% thought that their boards had "not really" set this, a decrease from 31% in 2014 and 41% 2013.

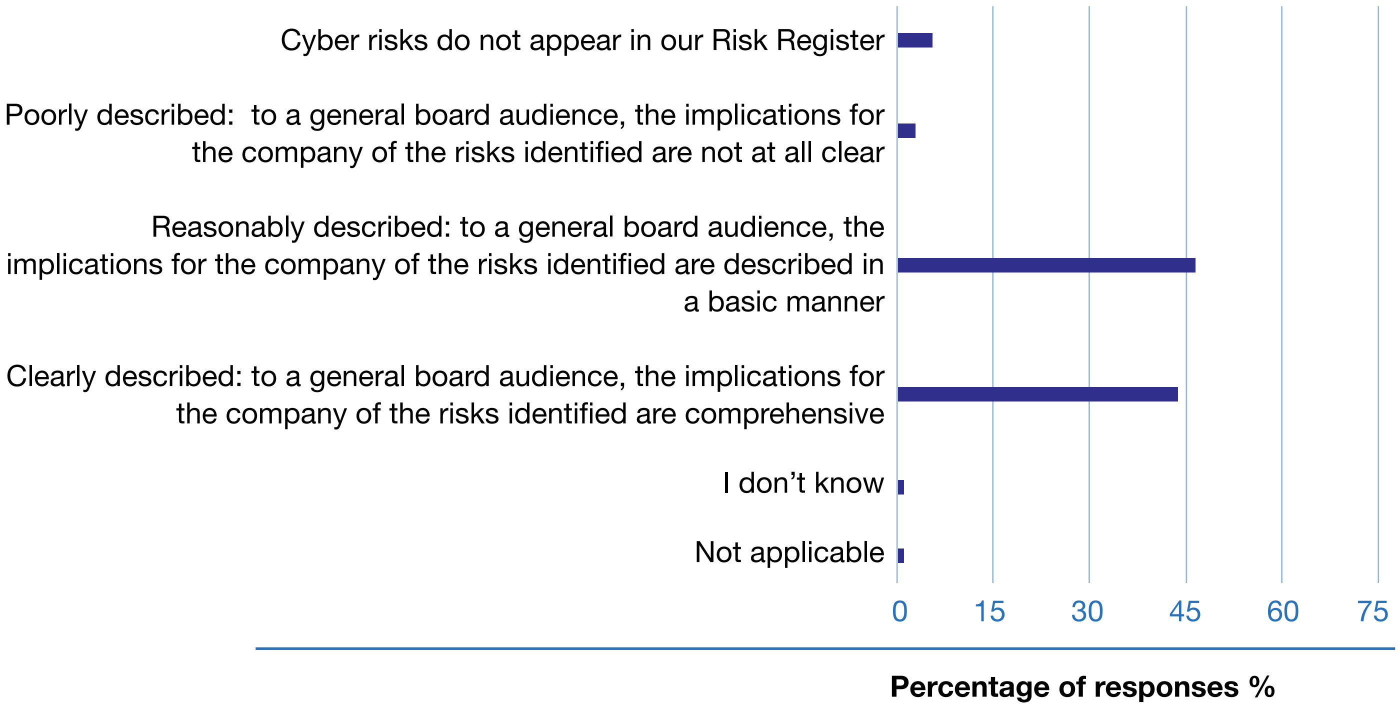
In 2015, when balanced against all types of risk, companies were more likely to rate cyber risk as being of top/group risk (49%), and least likely to rate it as a medium/segment risk (25%). This has changed compared to previous years, where companies were more likely to rate cyber risks as low/operational risks and least likely as top/group risks.

Marginally fewer respondents (46%) credited their boards with a basic understanding of key information/data sharing arrangements than in 2014 (48%) - this was however still an increase on 2013 (40%). The proportions stating a "very clear" understanding (16%) increased on previous years and with a "marginally acceptable" understanding (13%) had decreased.

Audit chairs were also asked to reveal how their companies addressed cyber risks with their suppliers and other third parties. Over two thirds (66%) of respondent boards used contract clauses to address cyber risks with suppliers and 56% of respondent boards utilising pre-contact due diligence. Both of these were slightly higher proportions than in 2014 (48% and 44% respectively). 38% of respondent boards used third party audit and third party self-assessments – both higher than the previous year.

Risk Management

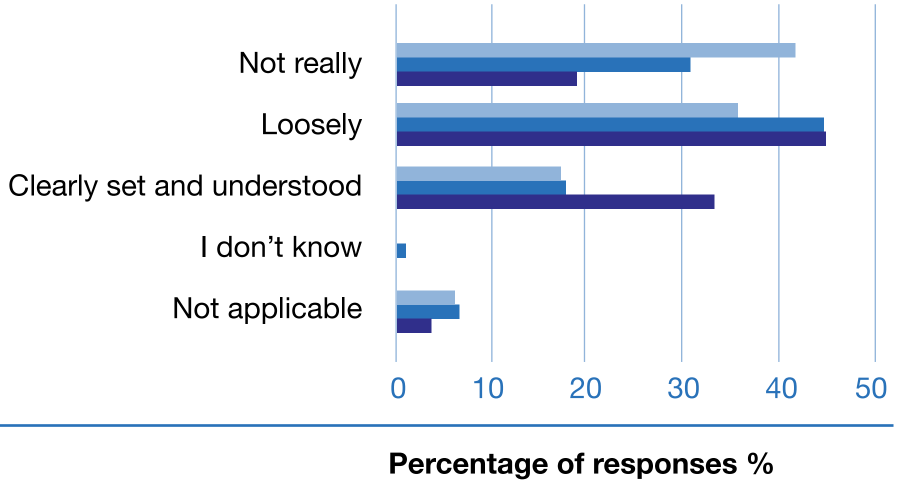
In the Risk Register, how well described (i.e. understandable to a general board audience) are cyber risks, and the potential consequences for the business?



Almost all respondents felt that cyber risks were either reasonably or clearly described in their company's risk register.

Risk Management

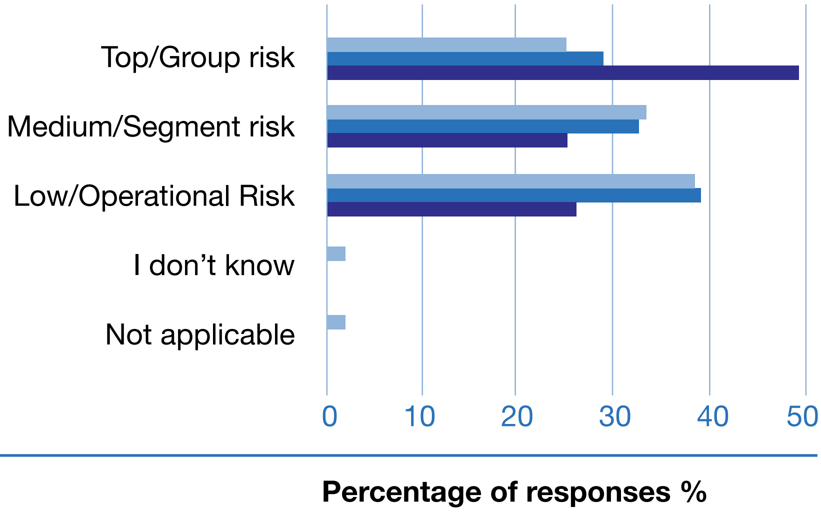
To what extent has your Board explicitly set its appetite for cyber risk, both for existing business and for new digital innovations?



A larger proportion of boards were more likely to explicitly set their appetite for cyber risk in 2015 than in previous years.

Risk Management

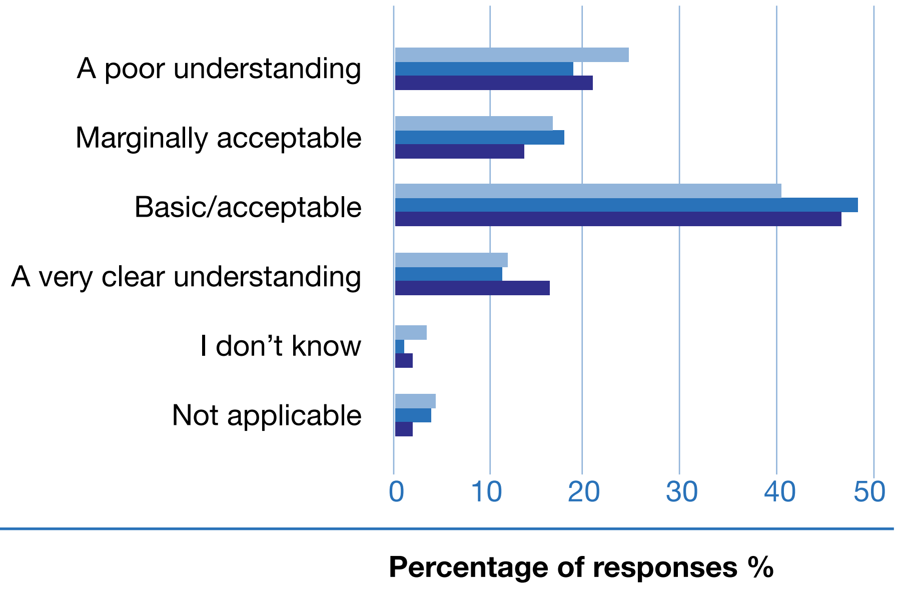
How significant or important is cyber risk, where risk is a product of likelihood and magnitude, when compared with all the risks the company faces?



Almost half of boards felt that cyber risk was a top/group risk, an increase on previous years.

Risk Management

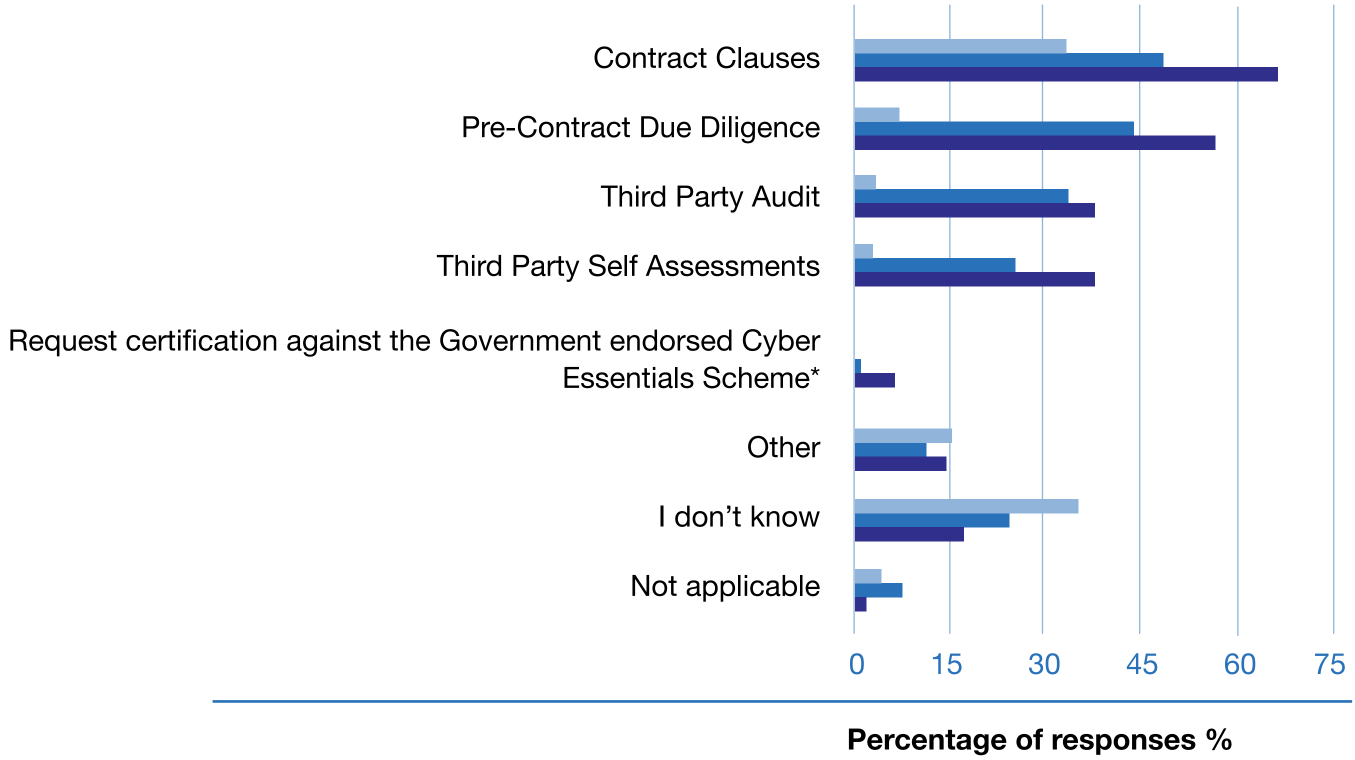
Does the main Board have an understanding of where the company's key information or data assets are shared with third parties (including suppliers, customers, advisors and outsourcing partners)?



In 2015, an understanding of the sharing of key information and data assets with third parties is said to have improved on previous years.

Risk Management

How has your company addressed Cyber Risks with its suppliers and other relevant third parties? Please select all applicable options.

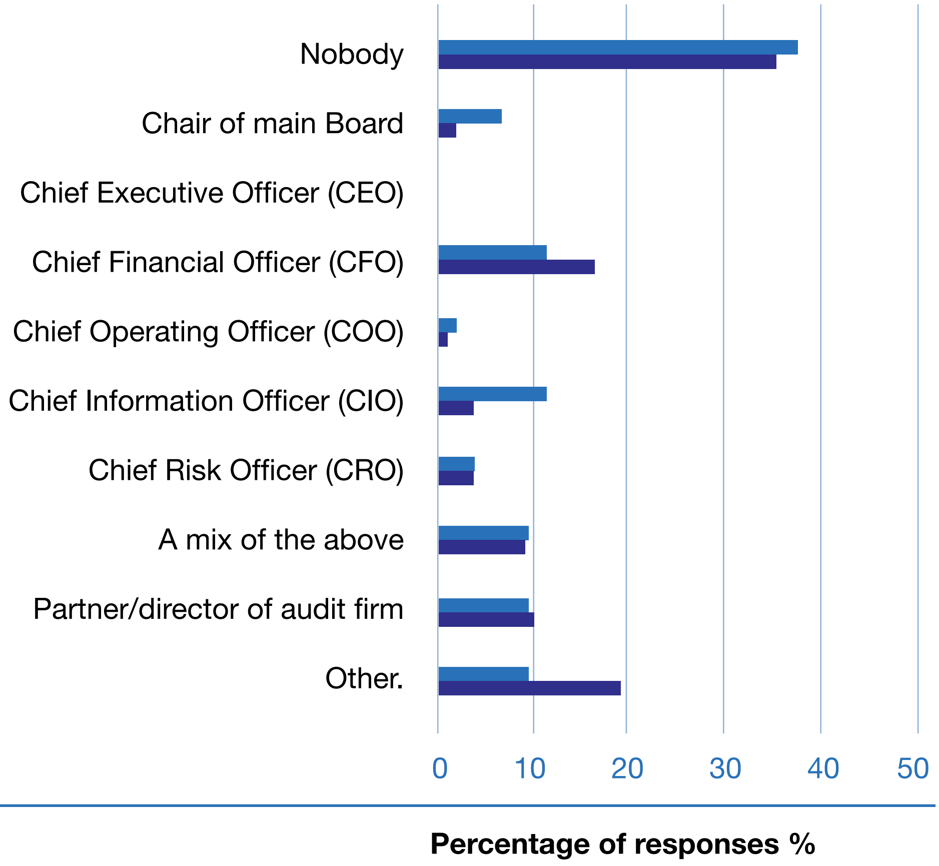


A higher proportion of companies addressed cyber risks with its suppliers and other relevant third parties using contract clauses and pre-contract due diligence than in 2014.

* https://www.cyberstreetwise.com/cyberessentials/

Completion of Tracker

In order to optimise results, we request that this questionnaire is not passed to the Chief Information Officer (CIO) or others to complete on your behalf. However, if you have done so, could you please indicate who has supported you in completing this questionnaire?



A similar proportion of respondents to previous years answered this questionnaire on their own .Those who did not identified a wide variety of different roles they consulted.

Investment and Customer Data

Summary of findings

Over three quarters of respondents (77%) had some budget allocated specifically to ensure the adequacy of protection for consumer data. Over half (56%) of companies had budget determined as a sub-set of IT budget, with a further 10% having a yearly budget that is determined by the board. An additional 11% have budget determined by business, or an ad-hoc budget determined by the board. Despite this, there were still 17% of companies with no budget allocated specifically to ensure the adequacy of protection for consumer data.

When asked whether they thought their customers read and understand their/their suppliers' Privacy Policy, just under one-third (29%) believed that the customers read and understood the privacy – 19% because the privacy policy is in plain English with no technical jargon, and 10% because the customer is well informed through marketing and communications channels if anything changes. A small proportion (5%) admit that the suppliers do not think that they communicate the Privacy Policy clearly to the customer. This varied between sectors, tech, comms and healthcare were most likely to believe that customers read and understood the privacy policy (60% answering yes).

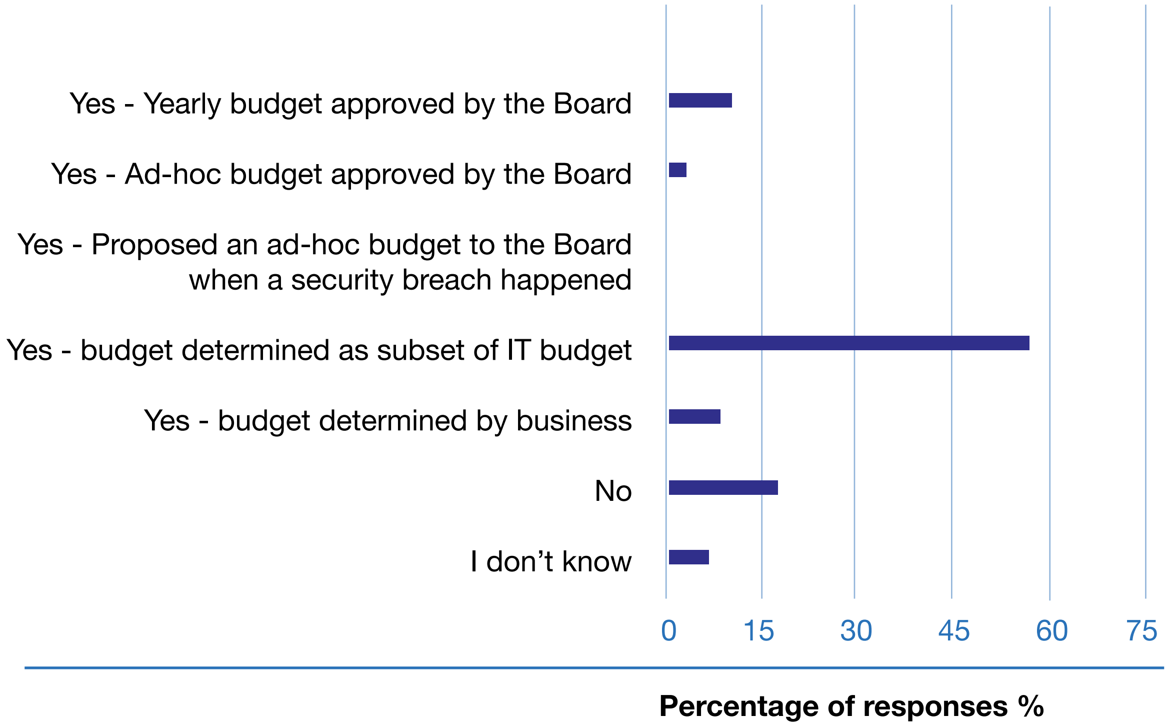
Almost two-thirds (61%) of boards do not review and challenge reports on the security of customers data, whereas the remaining 39% do. This varied considerably between sectors, only 18% of those in Utilities and Resources answered yes, whereas 69% in Retail, Travel and Leisure answered yes.

The main concern for respondents was their reputation with customers, with a large proportion (84%) reviewing and challenging reports on their customers' data due to this concern. A further 11% responded that this was due to the upcoming requirements of the EU General Data Protection regulation, with a smaller proportion (5%) reviewing due to investor concern.

The largest response across all sectors was reputation with customers.

Investment and Customer Data

Do you and your suppliers have budget allocated specifically to ensure the adequacy of protection for consumer data?

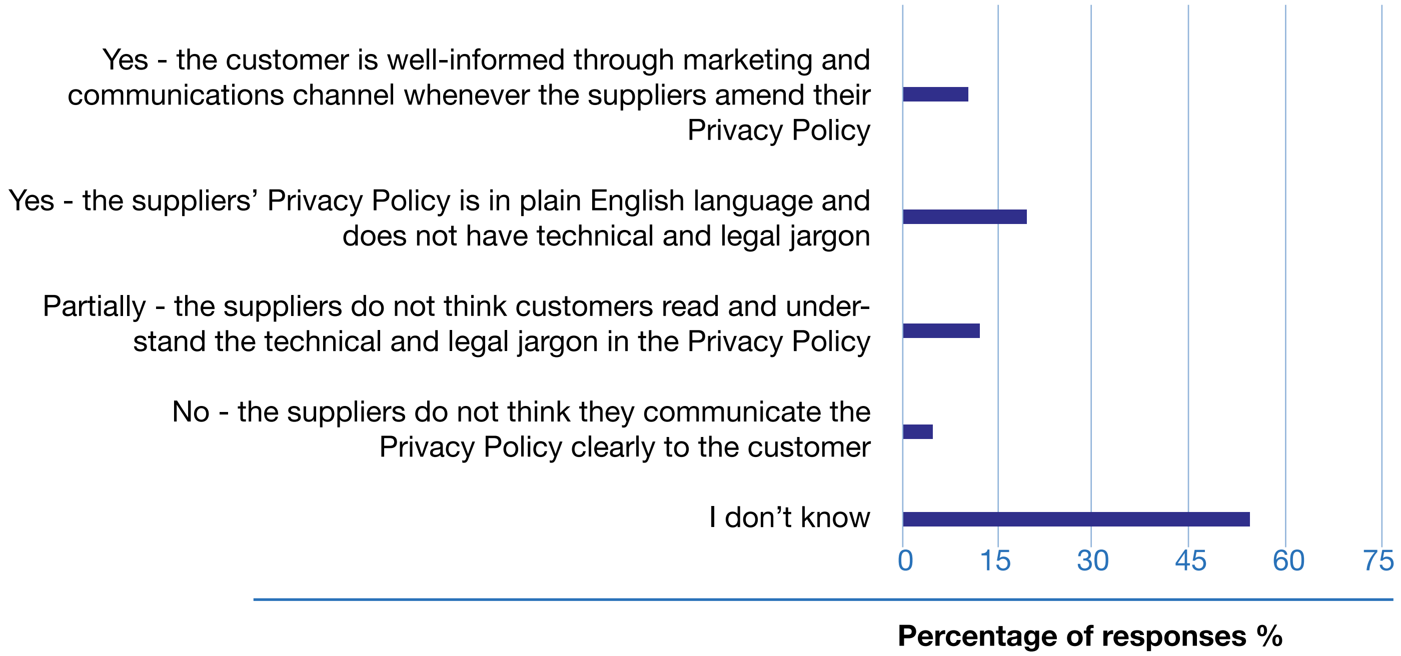


■ **2015 response**

A large proportion of companies had a budget determined as a sub-set of IT budget, or had a yearly budget determined by the board.

Investment and Customer Data

Do you think your customers read and understand your/your supplier's Privacy Policy?

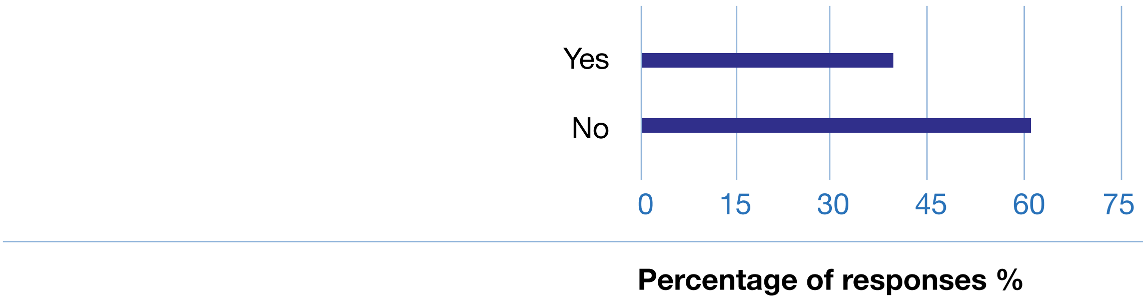


A small proportion of respondents did not believe that they communicate the Privacy Policy clearly to the customer.

■ **2015 response**

Investment and Customer Data

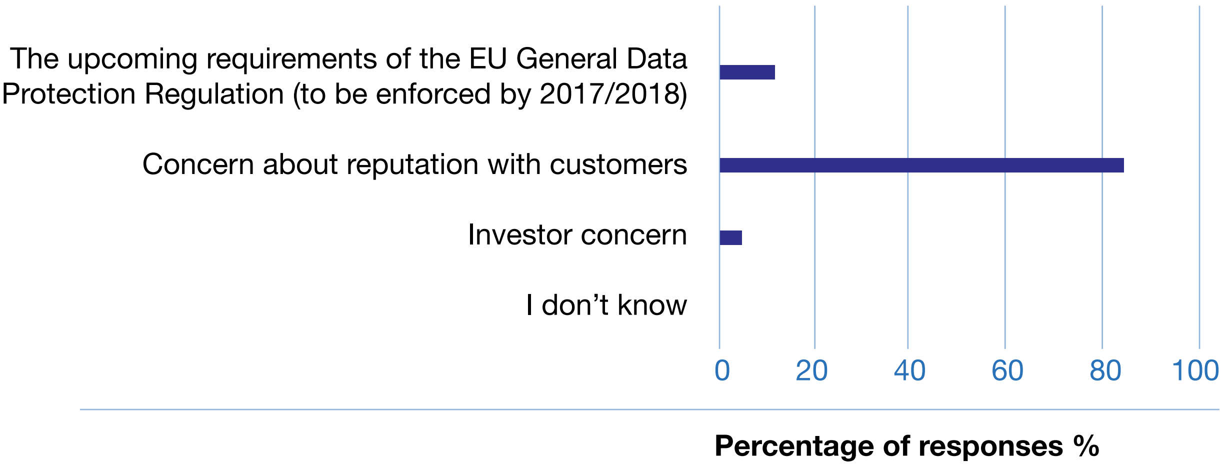
Does the board review and challenge reports on the security of your customer's data?



A large proportion of boards do not review and challenge reports on their security of their customer's data.

■ 2015 response

What are the drivers for the priority?



The majority of respondents reviewed and challenged reports on their customers' data due to concern about their reputation.

■ 2015 response

Methodology

The Health Check ran from 14th December 2015 to 12th February 2016 and this report is a collation of the combined anonymous responses of the boards of those companies. The report provides us with a rich picture of the respondents' attitudes to cyber security governance and should be indicative of large companies' view of these issues.

In 2013, both the Chairs and Audit Committee Chairs of the FTSE 350 were questioned. In the 2014 and 2015 survey the primary focus was with the Audit Committee Chair, with a recommendation that the questions were discussed with the Chair and board colleagues prior to submission.

Note on response rates and its effect on relevance of the findings.

In 2015, a third of FTSE 350 companies (113) responded to the survey, a similar proportion to in 2014 (108). This is half as many as responded in 2013, the first year of the survey (217). Such a change in response rate between years does raise concerns of non-response and self-selection bias – with companies responding being more likely to have higher levels of cyber security engagement or more likely to have adapted their behaviour in a positive way between the two years and vice-versa.

To account for this, it was considered in the 2014 tracker that restricting analysis to only those companies who had responded in both years of survey was considered. This was in order to present a very robust view of how these companies have progressed between years, accepting that they might not be representative of the FTSE 350 as a whole.

However, there was only a slight difference in the overall results of those answering in both years against the overall results using all respondents in both years. Using all the responses produced a marginally less positive year on year trend than when restricting analysis to those replying in both years.

Given that the trend in cyber security awareness displayed in the survey in these results is largely positive, the benefits of maximising the representativeness of the survey data by utilising all the results outweigh the benefits of having a stricter robust tracker representative just of the 80 or businesses that replied in both years.

In addition, the greatest decline in response rate was seen in Financial Services, a sector that showed the highest levels of cyber security "maturity" in 2013. The decline in responses in key sectors may be as a result of more prioritised and specific cyber security activity following the 2013 Health Check and wider sectoral cyber security initiatives.

Again, with only a third of FTSE 350 companies responding to the survey in 2015, this approach was used again. Whilst issues around non-response are still relevant, the year -on-year change in cyber security behaviours from the results are more likely to understate the development of cyber security maturity rather than exaggerate it.

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

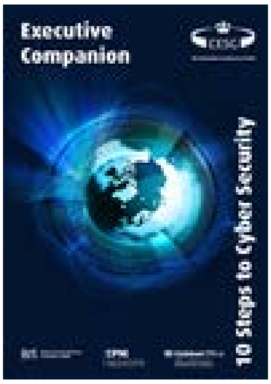
Utilities and Resources
Mining
Oil and Gas
Basic Resources (excl mining)
Utilities

Annex B

HMG Cyber Security Initiatives

Ten Steps to Cyber Security

The Government's primary cyber security guidance, which is designed to offer board rooms practical steps to improve the protection of their networks and the information carried upon them.



www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

CYBER ESSENTIALS

Cyber Essentials Scheme

Cyber Essentials is a Government-backed and industry supported technical 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, your company will be better protected from 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.

From 1st October 2014, 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 technical products and services.
www.cyberstreetwise.com/cyberessentials/

Cyber Incident Response

Companies can access help through a twin track approach encompassing a broadly based CREST (Council of Registered Ethical Security Testers) scheme endorsed by GCHQ and CPNI, and a small, focused GCHQ and CPNI scheme designed to respond to sophisticated, targeted attacks against networks of national significance.

www.cesg.gov.uk/servicecatalogue/service_assurance/CIR/Pages/Cyber-Incident-Response.aspx

CERT UK

CERT UK is the UK National Computer Emergency Response Team. CERT UK works closely with industry, government and academia to enhance UK cyber resilience.
www.cert.gov.uk

Cyber-Security Information Sharing Partnership (CISP)

The CISP facilitates the sharing of information and intelligence on cyber security threats in order to make UK businesses more secure in cyberspace. The CISP includes a secure online collaboration environment where government and industry (large and SME) partners can exchange information on threats and vulnerabilities in real time.
www.cert.gov.uk/cisp/

HMG Cyber Security Initiatives

The 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 cyber crime. The NCCU will support domestic and international law enforcement, and the wider NCA, to take responsibility for tackling cyber and cyber-enabled crime affecting the UK.

The NCCU will be 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 below).
www.nationalcrimeagency.gov.uk

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

Centre for the Protection of National Infrastructure (CPNI)
CPNI protects national security by providing protective security advice, covering physical, personnel and cyber security, to the UK's Critical National Infrastructure (CNI). CPNI works to raise awareness at board level as well as at a technical level across the CNI. Cyber security advice and guidance is available on the CPNI website.
www.cpni.gov.uk

FTSE 350 Cyber Governance Health Check Report 2015

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

Any enquiries regarding this publication should be sent to:

Department for 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.