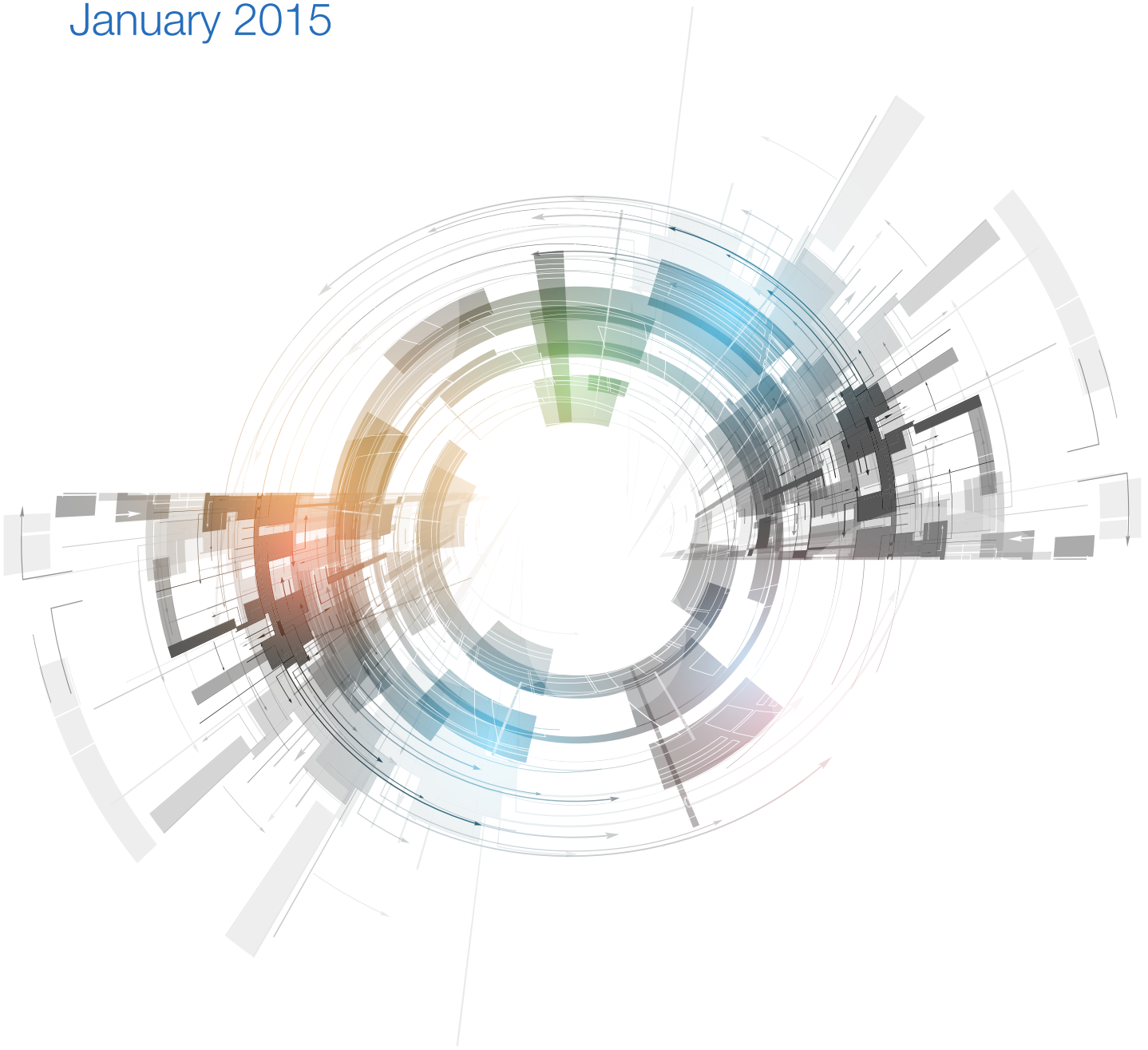
HM Government

FTSE 350 Cyber Governance Health Check Tracker Report

January 2015



Contents

Foreword

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

The world is becoming increasingly interconnected, with the digital revolution helping to deliver huge advances in freedom, knowledge, health and wellbeing. It is also powering economic growth, innovation and is creating opportunities and jobs. In the face of fierce global competition, the United Kingdom has demonstrated its credentials as an economy and a society capable of realising the opportunities.

As we continue to rely ever more heavily on networked information systems, the security of those systems becomes increasingly important for citizens, businesses and governments. In seizing the opportunities it is essential that all of us consider the growing security threats.

In 2013 the Government and the audit community worked in partnership to launch the first ever FTSE 350 Cyber Governance Health Check. Recognising the benefits, the FTSE embraced the initiative and paved the way for a second year. A second year has enabled us to benchmark progress on last year, highlighting some interesting and very positive results.

It is good to see so many FTSE 350 companies taking the cyber risk seriously, and that cyber security is now on most strategic risk registers. However the report also shows us that there is still work to do. For instance, the majority of boards still do not have a clear understanding of the impact a cyber attack could have on their business nor do they feel they are doing enough to protect themselves.

I am very grateful to all of the FTSE 350 board members who contributed significantly to the content of this report, and also wish to thank the audit community for their crucial support in helping to deliver the Cyber Governance Health Check. I urge all businesses to consider the findings, and together with your trusted advisors, act on them.

Executive Summary

More firms are
GETTING THE BASICS RIGHT

58%
of companies
had assessed themselves against the government's "10 Steps" cyber security guidance

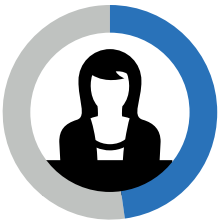
CYBER SECURITY
is seen as a business risk

88%
of companies
now include cyber-risk in their risk register

UP
from
58%
in 2013

BOARD KNOWLEDGE
of cyber security is
IMPROVING

Training
for board members has risen in the last
12 months



In 2014 this was
48%
for audit chairs

30%
of boards

received regular high level cyber security intelligence from their CIO or Head of Security

UP
from
18%
in 2013

INFORMATION SHARING
is improving

49%
of companies
encourage employees to share information with other companies in order to combat the cyber threat

Companies are getting better at UNDERSTANDING SUPPLY CHAIN RISK

UP from **52%** in 2013

59%
of boards
have a basic or clear understanding of where their critical information and data assets are shared with third parties (e.g. suppliers)

Companies know their KEY DATA ASSETS

92%
of boards
have a clear or acceptable understanding of the value of their companies' critical information and data assets

However...

65% **of boards**
rarely or never review their key information, data assets and personal data to confirm the legal, ethical and security implications of retaining them

Companies can improve their UNDERSTANDING OF THE THREAT

ONLY
24%
of companies
based their cyber risk discussion on comprehensive or robust management information

Introduction

The UK Cyber Security Strategy was published in November 2011. The strategy sets out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment.

A key objective within the strategy is to make the UK one of the most secure places in the world to do business in cyberspace. 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 ("the Tracker") is a process 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.

The Tracker is a non-technical governance questionnaire comprised of 37 questions. Completion of the Tracker 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 six firms which currently audit the full spectrum of the FTSE 350: BDO, Deloitte, EY, Grant Thornton, KPMG and PwC. The Government will seek to repeat the Tracker in 2015 in order to chart governance behaviours across the FTSE 350, enabling further benchmarking as both threats and mitigation best practice develops.

The governance behaviours, findings and guidance contained within this report should enable many large and small companies to better understand and manage 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 as in the previous year (88%).

Of those that were executive directors, 60% were Chief Financial Officers and 25% were the Chair of the Main Board. In 2013 85% of executive respondents were the Chair of the Main Board.

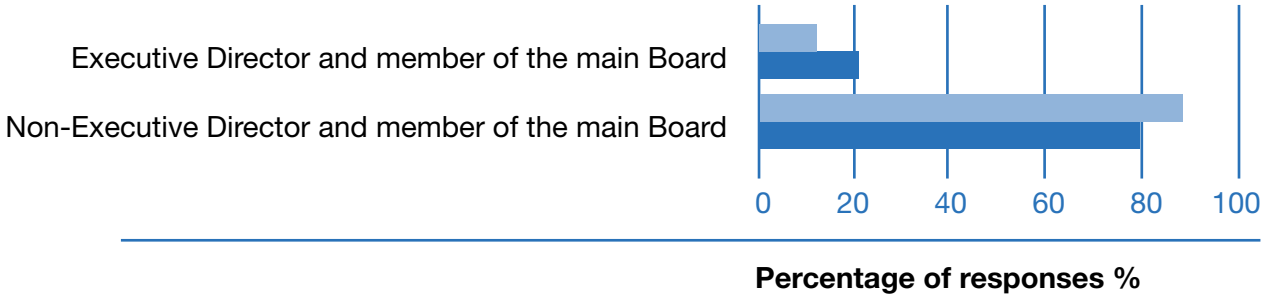
Of the non-executive respondents almost all were the Chair of the Audit Committee in both years (84% in 2014 and 80% in 2013).

Overall, 108 companies responded to the survey in 2014 compared to 218 in 2013, a reduction of almost exactly 50%. Response rates in all the sectors described in our results fell by 50% or more except Consumer Goods which only fell by 12%. The greatest falls were seen in “Technology Communications and Healthcare” (-63%) and “Financial Services” (-61%). Last year these sectors appeared to be the most cyber security aware which may have some implications for our results. This is discussed more fully in the Methodology section at the end of this report.

Respondents were asked to identify what cyber related risks applied to their companies. Two thirds (66%) of respondent companies said shareholder value was significantly dependent on securing critical information assets, up from 54% in 2013, while 39% handled high value financial transactions or other assets at high risk from theft or fraud. Only 14% of companies stated that more than half of their revenues came through online interactions which is slightly less than in 2013 (19%).

Respondent Profile

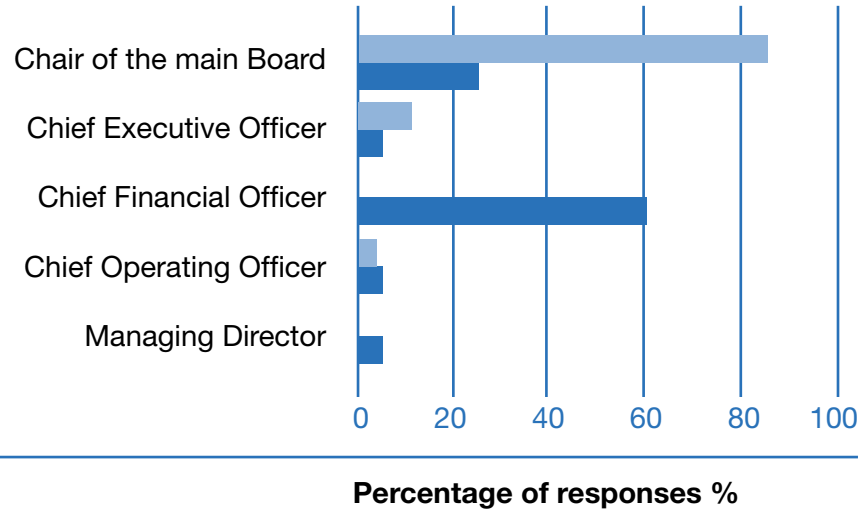
Which of the following describes you?



The majority of respondents were non-executives.

2013 response
2014 response

Which of these titles best describes your role?

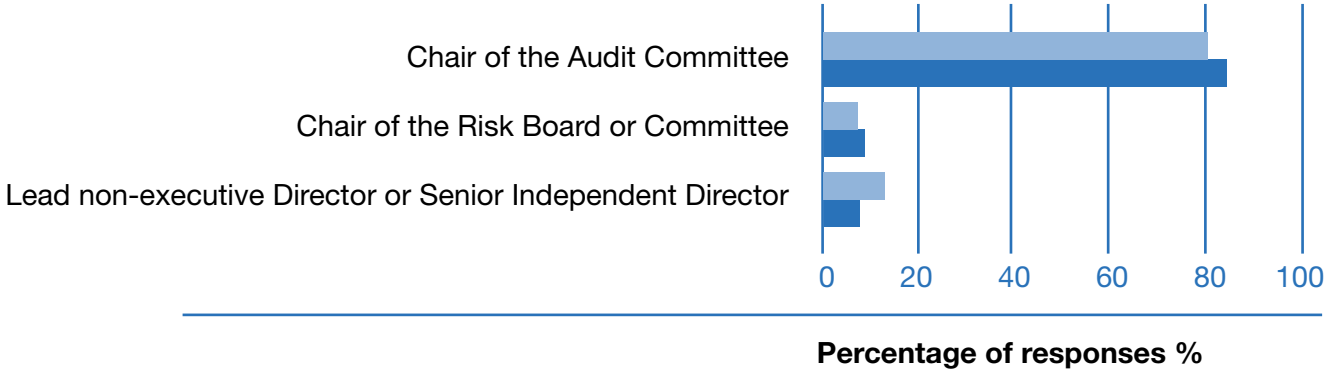


Executive Director respondents were most likely to be Chief Financial Officers rather than the Chair of the Main Board as in 2013.

2013 response
2014 response

Respondent Profile

As a non-executive Director, are you also:

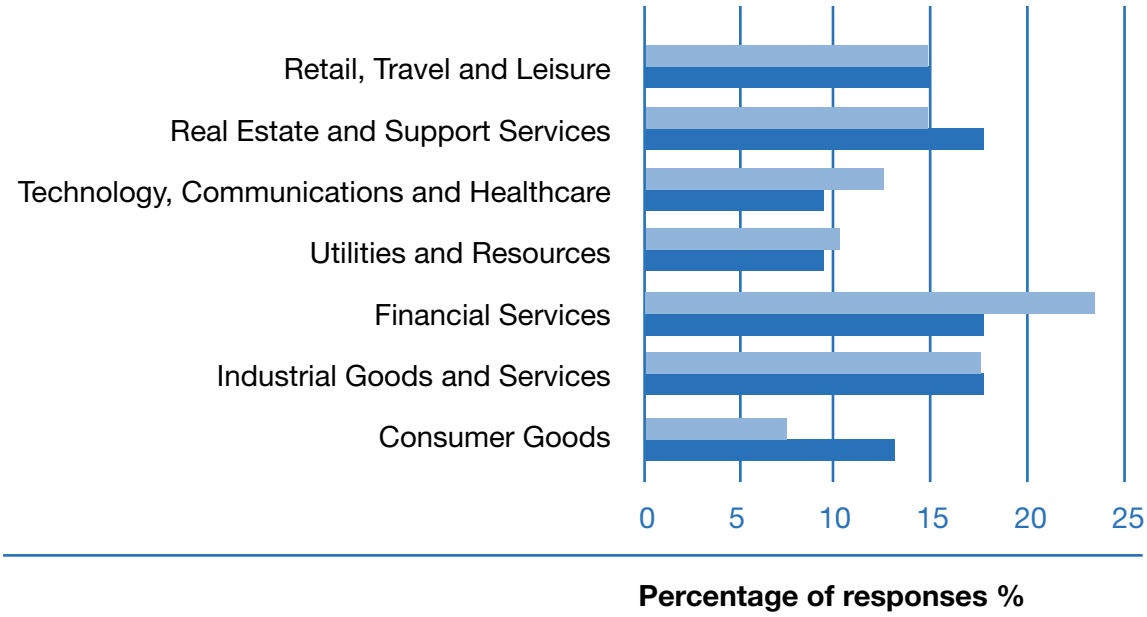


Non-executive Directors were almost all Audit Committee Chairs.

2013 response
2014 response

Respondent Profile

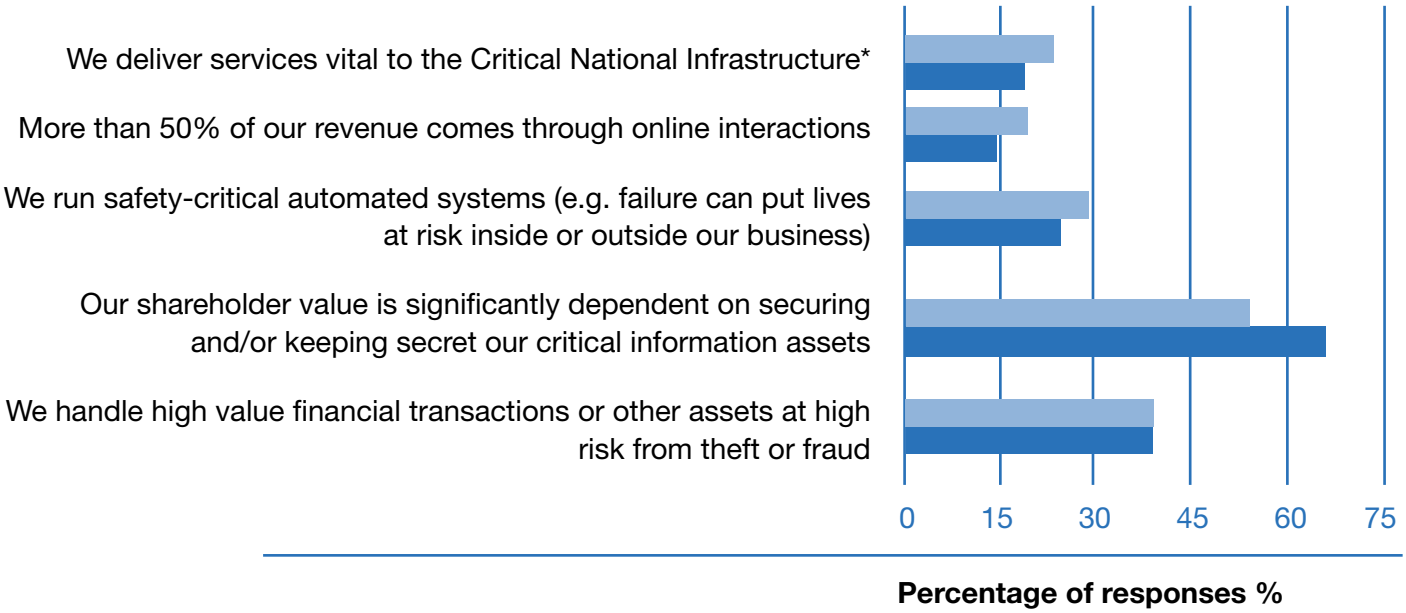
Which sector classification best applies to the company's main business?



While the spread of industries was not drastically different from the previous year there was proportionately weaker representation in "Financial Services" and "Technology, Healthcare and Communications".

Respondent Profile

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



In both years a large proportion of respondents had shareholder value that was significantly dependent on securing critical information assets or were involved in handling high value financial transactions 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

Audit committee chairs reported that the main boards they served either had an acceptable understanding (61%) or a clear understanding (33%) of what their key information and data assets were. This result is almost exactly the same as in 2013. Financial service industry audit chairs had the most positive view of their boards in this respect.

Related to this 57% of main boards were reported to have an acceptable understanding of the value of their key information and data assets with 34% having a clear understanding. Again responses to this question varied very little from 2013.

When asked about their main boards' understanding of the impact of loss or disruption of their key information and data assets, 55% of audit chairs thought they had an acceptable understanding, 36% a clear understanding and 8% a poor understanding. Audit chairs were more likely to rate their boards understanding of this as being "acceptable" rather than "clear" than they were in 2013 (47% "acceptable" and 44% "clear" in 2013). The main boards of financial services businesses were the most likely to be credited with having a clear understanding (55%).

Very few (5%) of main boards regularly and thoroughly review their key information and data assets. A quarter (24%) do claim to do so regularly and somewhat thoroughly while the majority rarely (35%) or never (30%) do so. This is true across the different sectors with this generally not seen as being main board business. These results are slightly more negative than in 2013 with more boards rarely or never reviewing this information (65% in 2014 vs. 58% in 2013).

Over half (55%) of boards discussion of cyber risk is underpinned by "some" up-to-date management information. Of the rest 18% received very little insight while 21% received comprehensive, generally informative management information and 3% had robust management information driving business choices. Financial services businesses tended to base their discussions on more complete information. The level of management information presented to boards has improved since 2013 with almost twice as many boards receiving comprehensive information

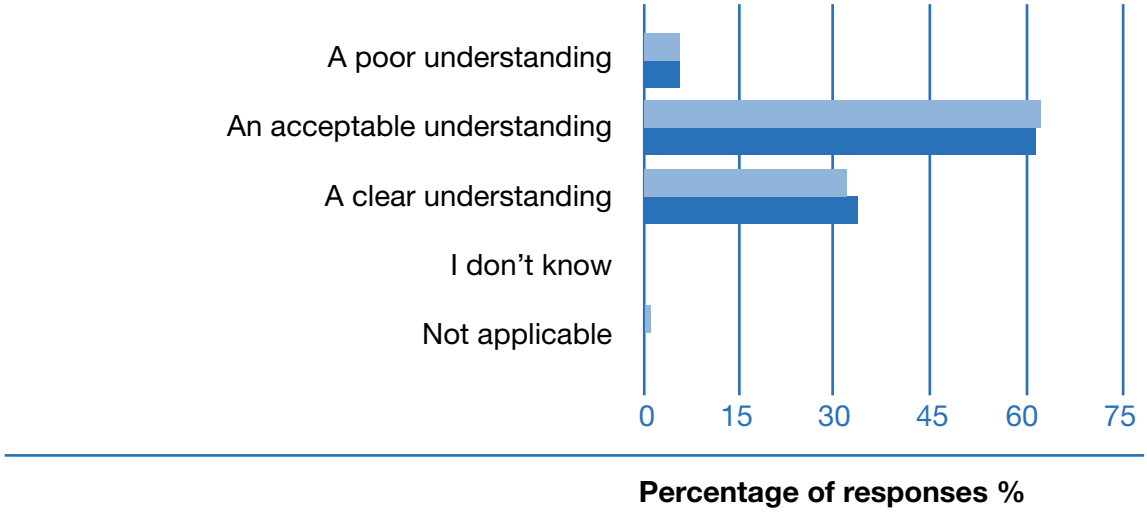
Nearly a third (30%) of boards received regular high level intelligence from their CIO or Head of security on who may be targeting their companies from a cyber-perspective (up from 18% in 2013). A further 37% received this information although rarely, while 25% of respondents' board never received such information (down from 43% in 2013). Companies in utilities and resources appeared to be the best informed from this perspective.

Three quarters (75%) of audit chairs believe that their board members have a limited understanding of their own personal cyber risk profile, with more said to have a full understanding (17%) than poor understanding (5%). This is an improvement on 2013 when 15% of boards were said to have a poor understanding. Financial services were the most positive sector on this measure.

Almost half (49%) of boards encouraged their technical staff to enter formal information sharing exchanges with other companies with a view to prevent and identify emerging cyber threats. This was up from 45% in 2013. However in both years there were a large proportion (over 20%) of "don't know" and "not applicable" answers to this question.

Understanding the Threat

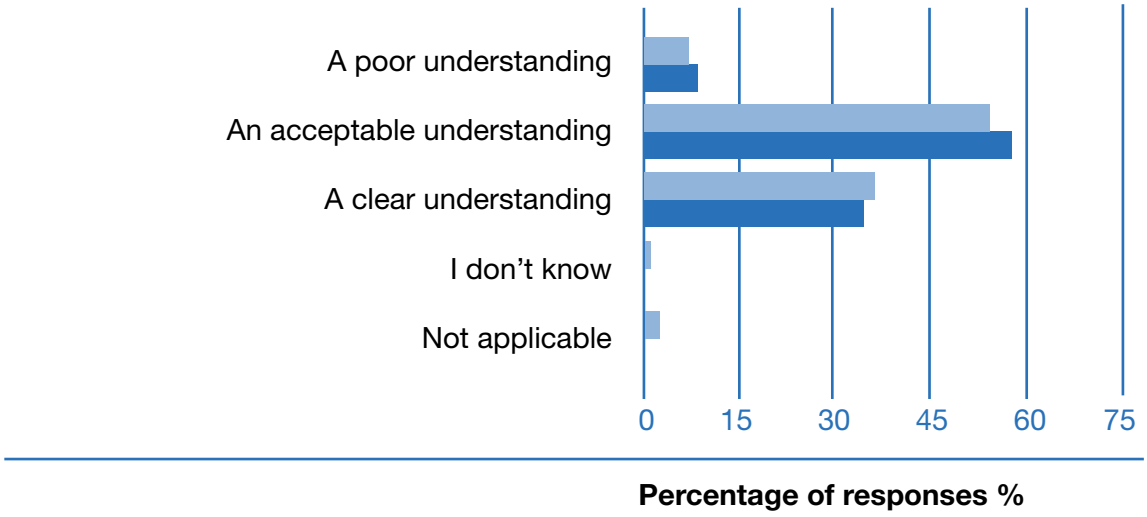
Does the main Board have a good understanding of what the company's key information and data assets are (e.g. IP, financial, corporate/strategic information, customer/personal data, etc)?



As in 2013 most respondents believe their mains boards only have a basic or acceptable understanding of what their companies' key information and data assets were.

Understanding the Threat

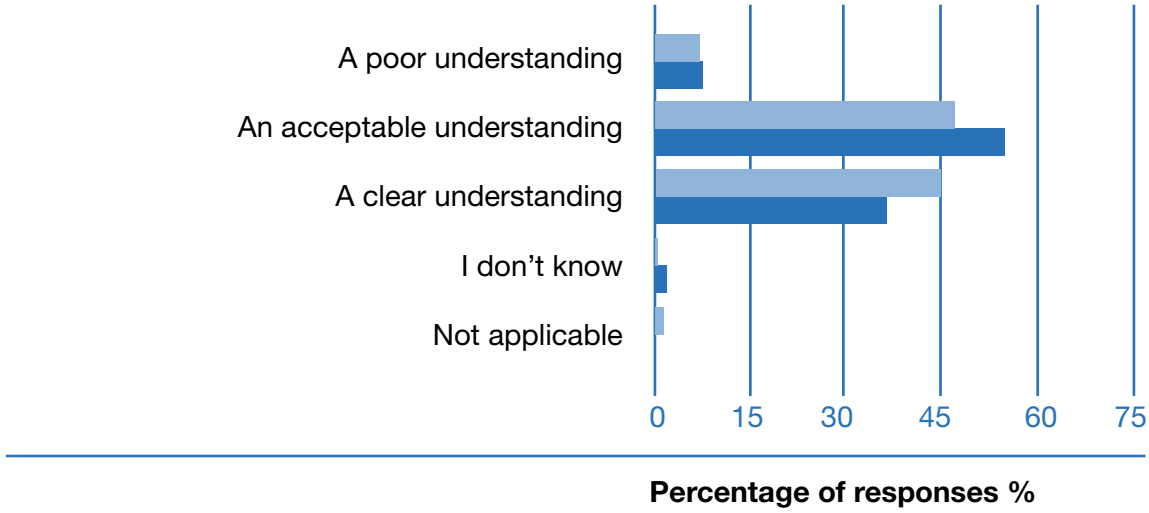
Does the main Board have a clear understanding of the value of those key information and data assets (e.g. financial, reputational, etc.)?



When asked about the "value" of these assets the distribution of answers was very similar to the previous question and the answers given to this one in 2013.

Understanding the Threat

What is the Board's understanding of the potential resulting impact (for example, on customers, share price or reputation) from the loss of/disruption to, those key information and data assets?

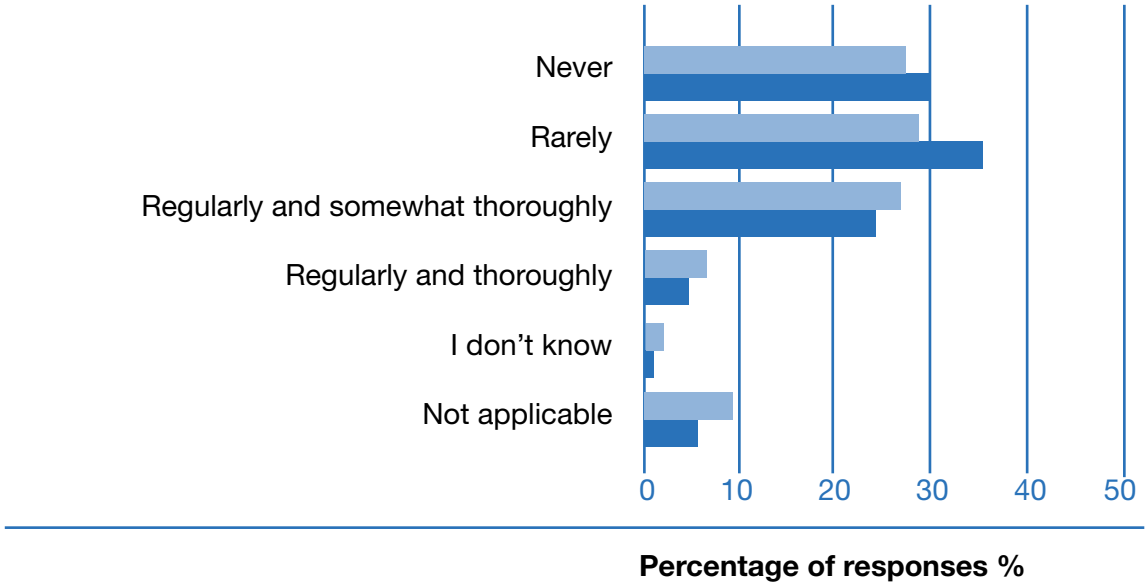


Respondents were perhaps slightly less confident of their main boards understanding of the consequences of loss or disruption to their key information or data assets than in 2013.

2013 response
2014 response

Understanding the Threat

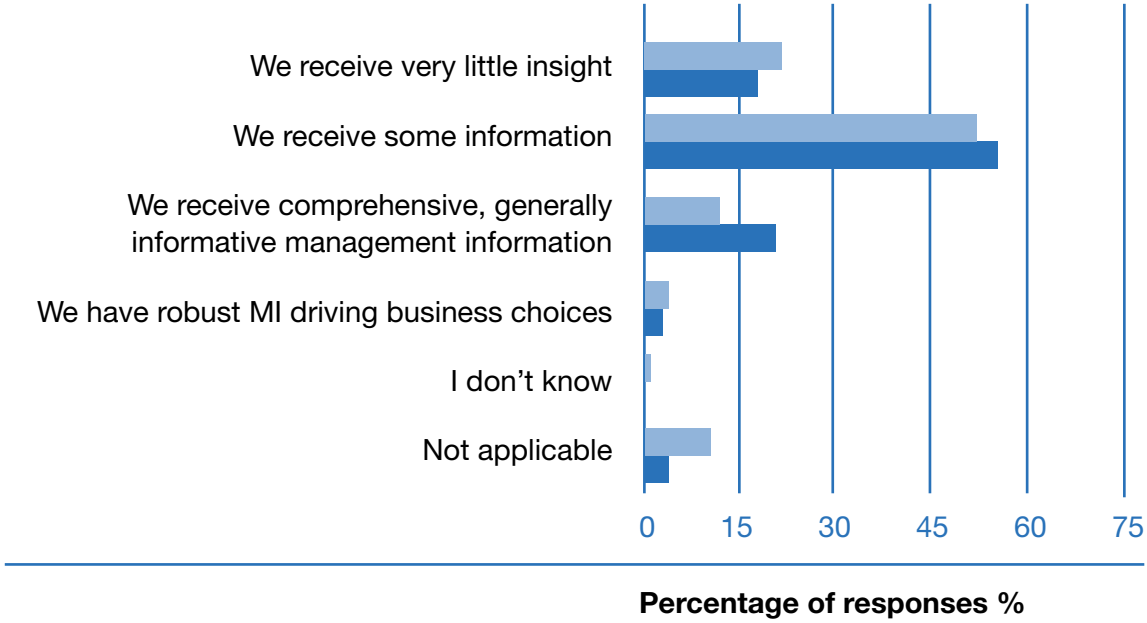
Does the main Board periodically review key information and data assets (especially personal data) to confirm the risk management, legal, ethical and security implications of retaining them?



In 2014 audit chairs reported that main boards were slightly less likely to review their key information and data assets on a regular basis than in 2013.

Understanding the Threat

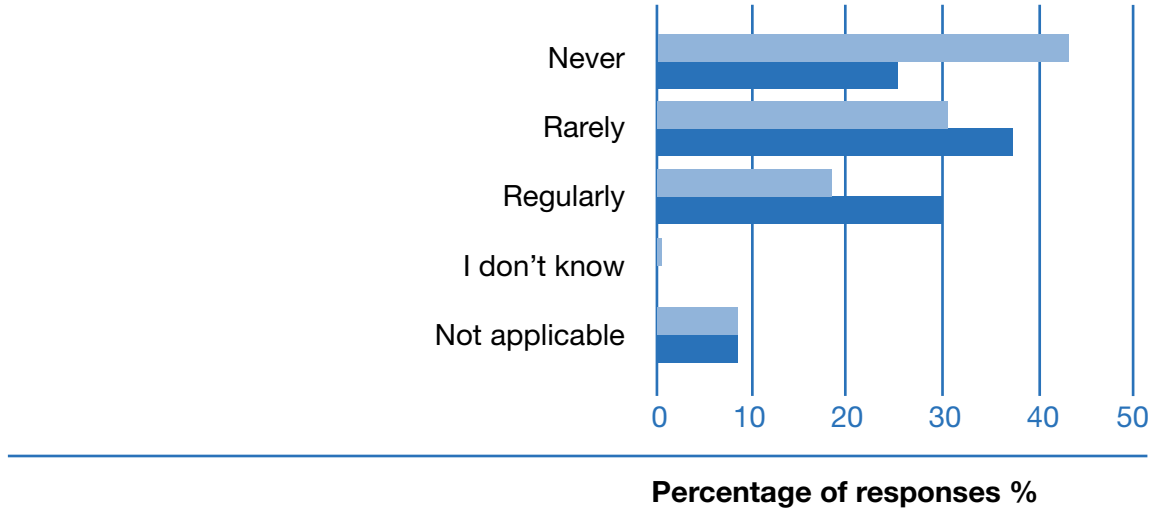
To what extent is your Board's discussion of cyber risk underpinned with up-to-date management information?



Provision of management information to underpin discussion of cyber risk has slightly improved compared to 2013.

Understanding the Threat

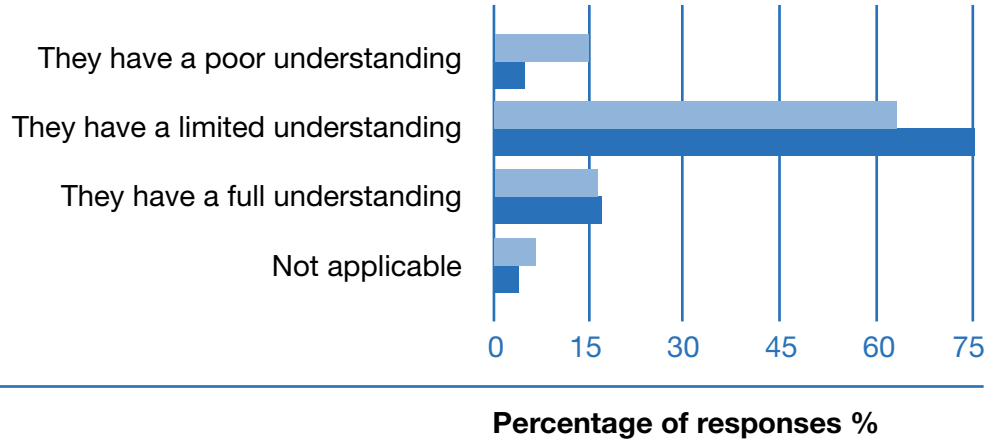
Does the Board receive regular high level intelligence from the CIO/Head of Security on who may be targeting your company, from a cyber-perspective, and their methods and motivations?



There appears to be an improvement in the provision of intelligence given to company main boards on who may be targeting them for cyber related attacks with more board regularly receiving such information and fewer never doing so.

Understanding the Threat

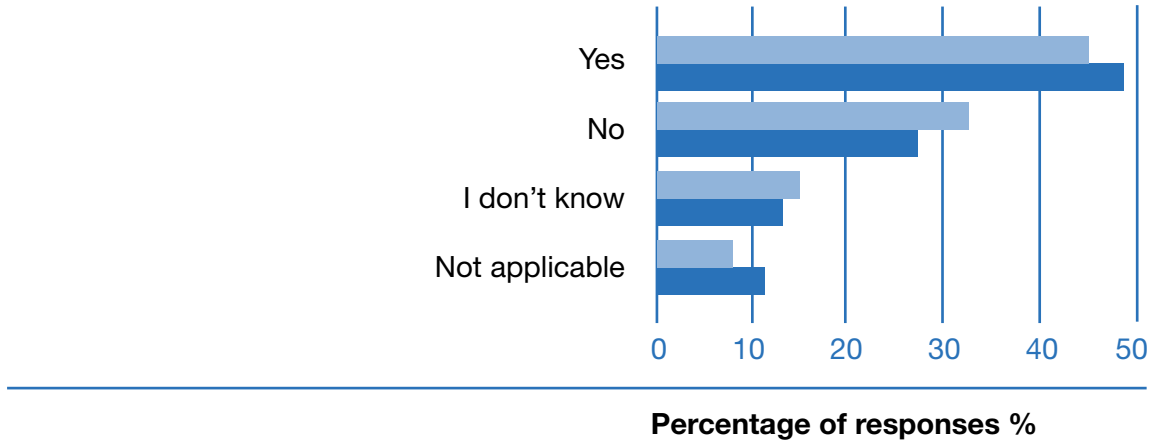
In your view how good is the board members' understanding of their own personal cyber risk profile (e.g. how to prevent being a target of an electronic attack?)



Audit chairs were more positive about their main board's understanding of their own personal cyber risk profile than in 2013, with a greater proportion said to have a limited understand and fewer said to have a poor understanding.

Understanding the Threat

Does the Board encourage its technical staff to enter in to formal information sharing exchanges (e.g. CISP*) with other companies in your sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats?



Around half of main boards are said to encourage staff to enter formal information sharing exchanges , a greater proportion than the previous year.

**Cyber Security Information Sharing Partnership (CISP)*
https://www.cisp.org.uk/

Leadership

Summary of findings

Respondents to the survey expected cyber net risk to increase slightly (46%) or stay the same (33%) with only 12% foreseeing a significant increase. This is more optimistic than in 2013 when 66% expected a slight or significant increase compared to 58% in 2014.

When asked about the importance of cyber risk to the business, just over half of respondents (53%) ranked cyber risks as being of moderate importance. Of the rest 36% stated it as being extremely important and 10% of limited importance. Those in the retail, travel and leisure industries and financial services attached the greatest importance to cyber risks. Responses to this question should not be compared with the previous year's results as audit chairs were not given the option to answer "moderately important" in 2013.

With regards to employees in their companies, half (49%) of respondents said that their employees were comfortable reporting compromises or losses of information or data assets while a further 44% "thought" that this was the case. This is slightly up on the previous year with only 2% thinking employees were not comfortable reporting such things.

For the majority of boards (56%) cyber risk is a subject they hear about occasionally - biannually or when something has gone wrong - but 24% said they rarely did so or did not consider it board level business. However, 16% of boards were reported to regularly consider cyber security issues or actively manage their cyber risk profile. Cyber risk is more commonly handled at main board level than it was in 2013 with a 19 percentage point increase in the proportion of boards occasionally hearing about it and a 20 percentage point decrease in those rarely or never dealing with it.

When it comes to risk ownership for cyber security the responses were more fragmented than in 2013 with a wide range of roles being identified. It is now much less likely to be the Head of IT (14% in 2014 vs. 23% in 2013) and much more likely to be the Chief Information Officer (15% in 2014 vs. 0% in 2013). The Chief Executive Officer and Chief Financial Officer were also common choices.

Whoever the "cyber risk owner" is, the main board was the most common area for this role to be held to account in both years (41% in 2014, 39% in 2013). The Operating Board/Executive Committee (20% in 2014 vs 22% in 2013) and the Audit Committee (28% in 2014 vs 19% in 2013) were also common fora for this to be discussed in respondents companies.

When asked whether their boards had the right skills and knowledge to manage innovation and risk in the digital world 55% of audit chairs stated that their boards had the right skills "to a limited degree" compared to 47% saying this in 2013. 38% said their boards had the right skills to a significant degree down from 39% in 2013 and only 1% labelled their board fully informed and skilled (compared to 7% the previous year). Companies in "Technology, Health and Communications" and "Real Estate and Support Services" had the most positive outlook here.

When asked whether their companies were doing enough to protect themselves against cyber threats the most notable result was that more audit chairs had an opinion on this than last year with fewer responding "I don't know" (2% down from 8%). A greater proportion of companies admitted that there was more that they needed to do (49% up from 44%) with the same proportion believing they were currently doing enough (44% in both years). Again companies in "Real Estate and Support Services" were proportionally more positive as were those in the "Utilities and Resources" sector.

Leadership

Summary of findings

On whether their boards took cyber risk sufficiently seriously more audit chairs felt able to express an opinion than last year with only 6% answering "I don't know" or "Not applicable" compared to 17% in 2013. The majority of these felt that their boards took cyber risk very seriously (75% up from 61% in 2013) with fewer feeling their boards did not take it seriously enough. Companies within the "Industrial Goods and Services" sector were the least positive about their boards on this measure in 2014.

The incidence of training in this area for board members has increased. In 2014 48% of audit chairs had undertaken some form of cyber security/information security training in the 12 months prior to answering the survey, this is up from 29% in 2013. This measure varied from 60% in the Financial Services sector to 19% in "Retail Travel and Leisure".

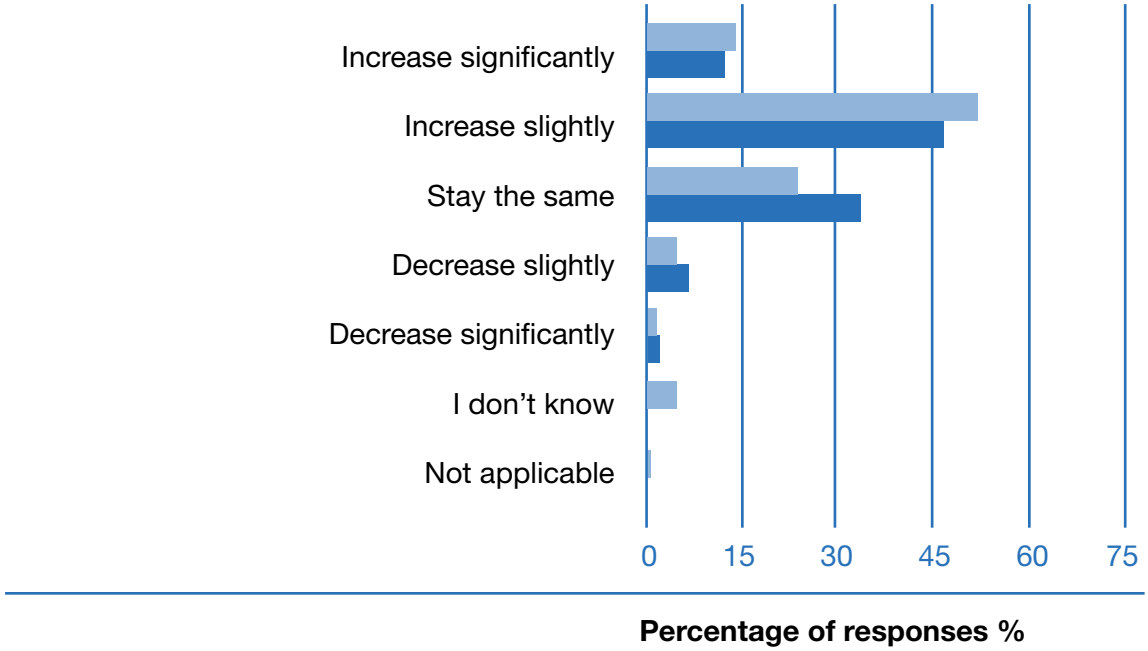
With regards to the rest of the board 40% of respondents in 2014 said board members other than the audit chair had undertaken cyber security or information security training in the previous 12 months up from 22% in 2013. As in the previous question the Financial Services sector were the most active in undertaking training.

In neither year of the survey did any audit chair state that their company invested "too much" in cyber defences. Positively the proportion claiming a "reasonable sum" was invested rose to 84% in 2014 from 67% in 2013. Those who thought their companies invested "not a great deal" fell to 6% from being as high as 32% in 2013.

Near half (45%) of respondent boards have outlined their approach to cyber security clearly in their annual reports and on their websites, with a view to reassuring investors and customers. Of the rest 25% have not actively sought to reassure investors and customers but maintain that they have a robust approach nonetheless while 11% admit they currently lack a robust approach. Outlining the cyber risk approach in the annual report and website was most common in the "Retail Travel and Leisure" sector (75% of these respondents) while 50% of companies in both the "Utilities and Resources" and "Technology, Healthcare and Communications" sectors did not seek to reassure despite having a robust approach to cyber security.

Leadership

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

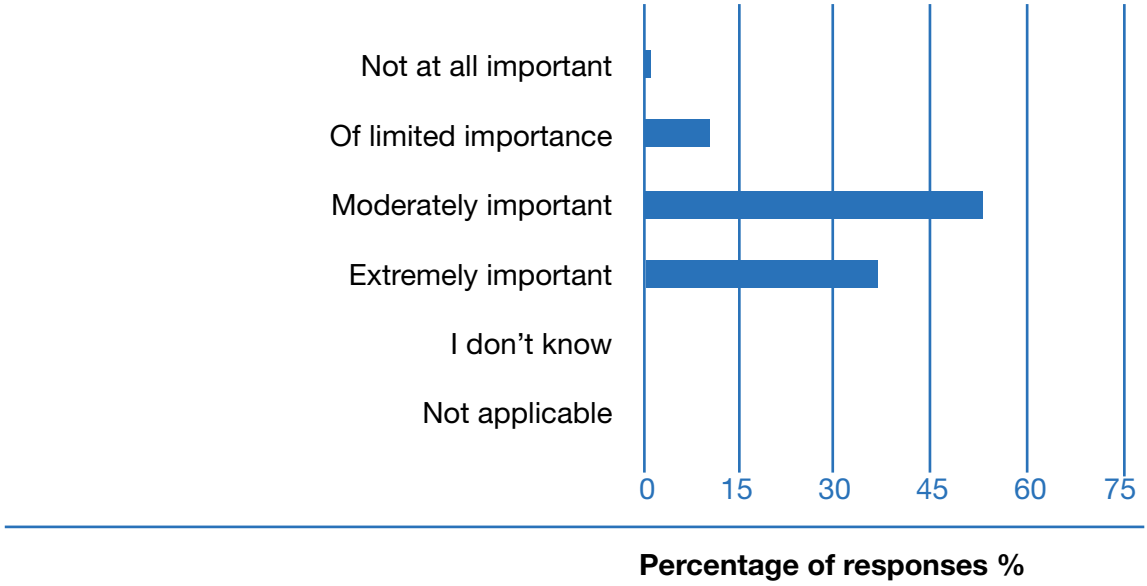


Audit chairs expect net cyber risk to increase rather than decrease, though are more optimistic about this than in 2013.

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

Leadership

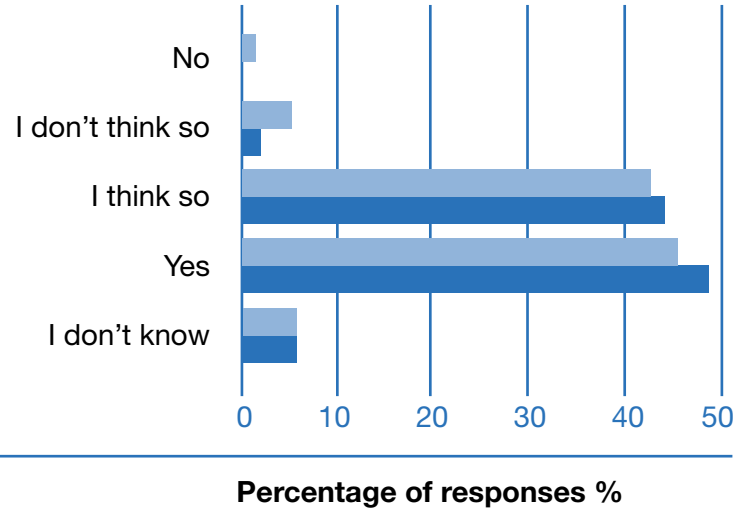
In your personal view, how important are cyber risks to the business?



The vast majority of respondents view cyber risks to be of moderate (53%) or extreme (36%) importance to the business.

Leadership

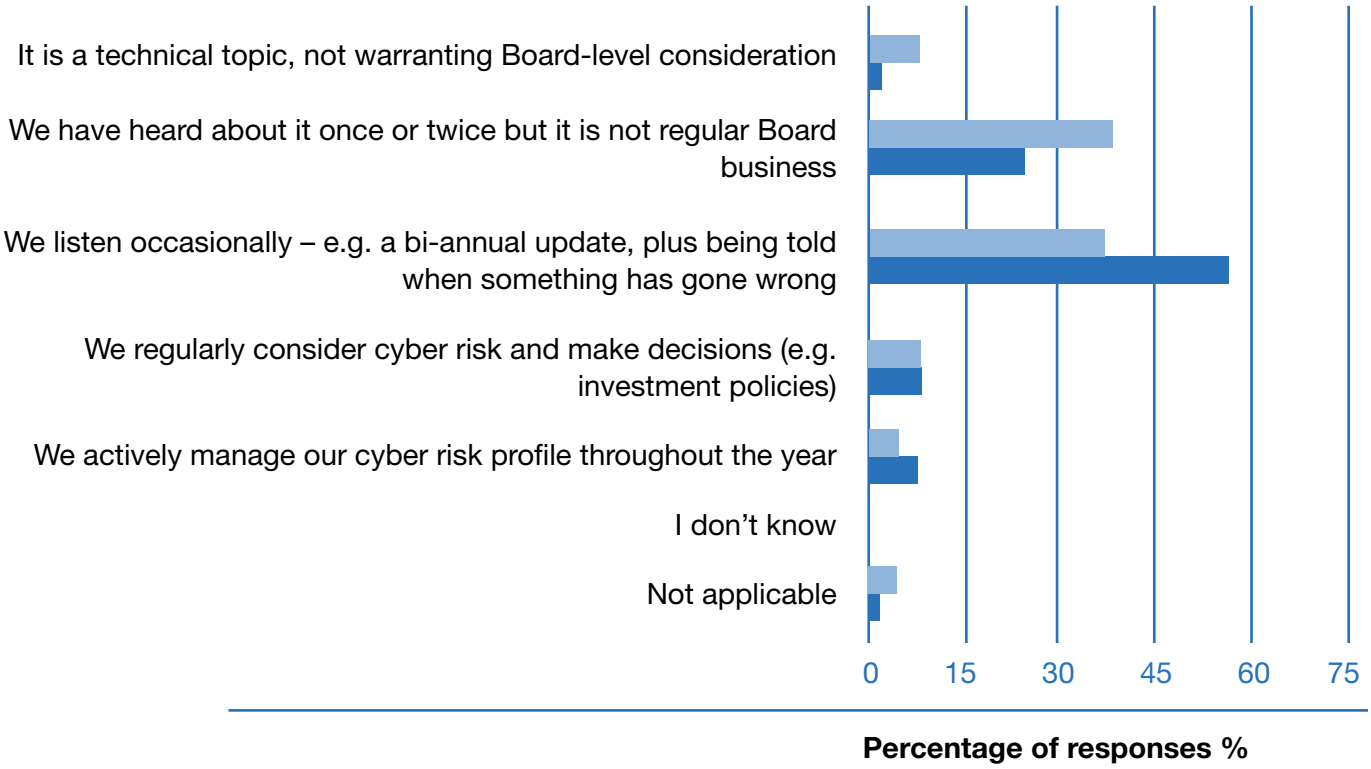
Do you think that employees are comfortable reporting compromises or losses of information and data assets?



Over 90% of respondents thought that employees in their company were comfortable reporting compromises or losses of information and data assets.

Leadership

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

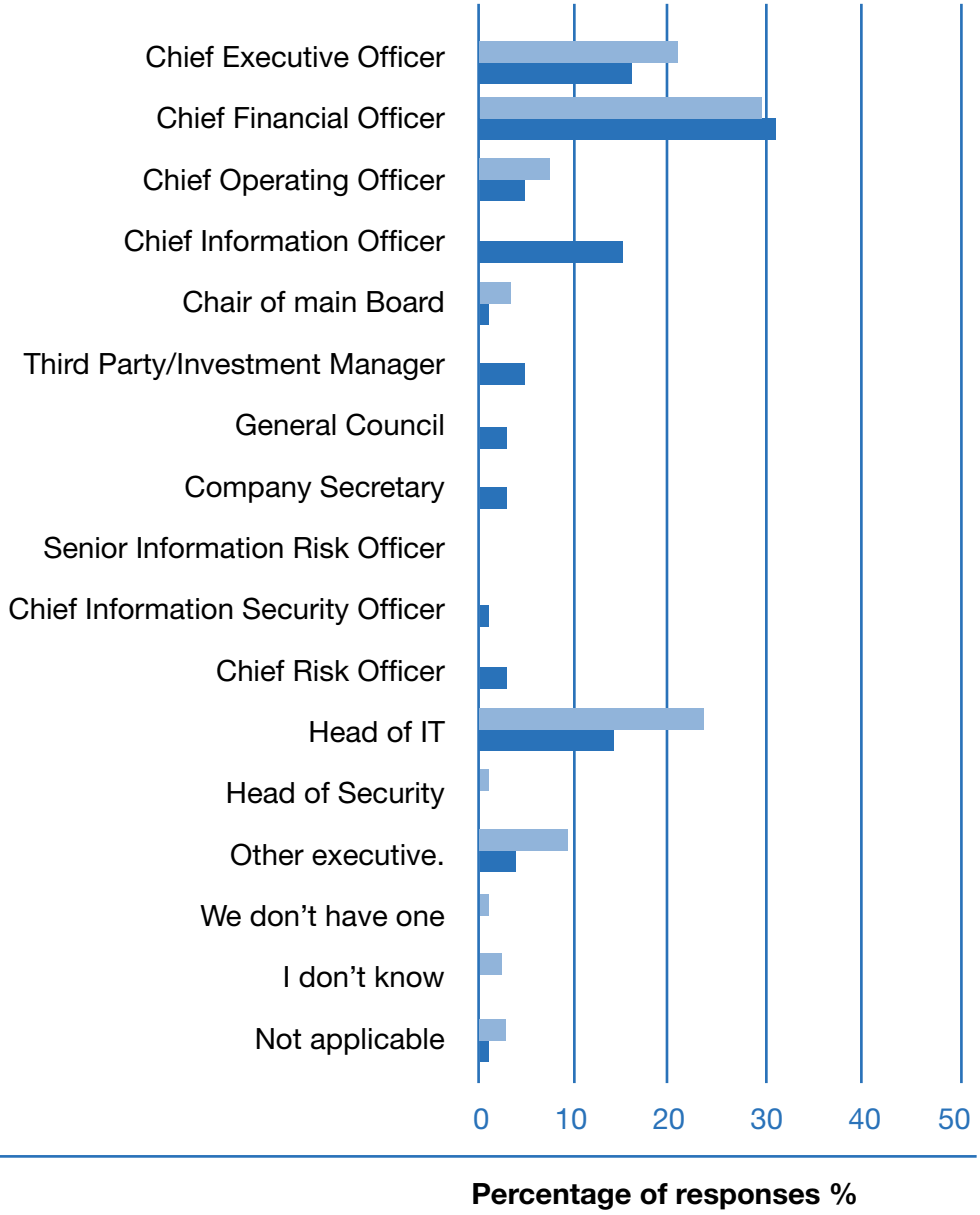


Cyber risk is more commonly handled at main board level than in 2013.

2013 response
2014 response

Leadership

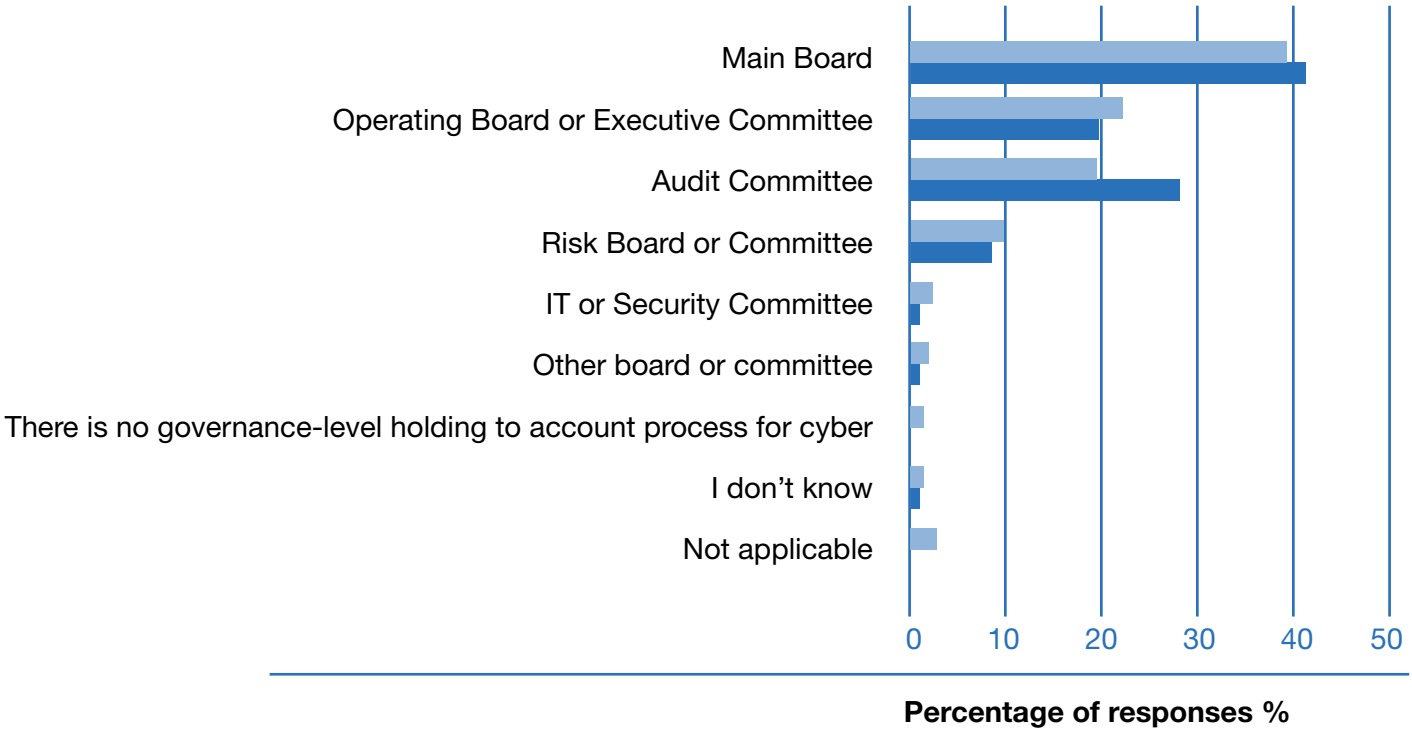
Who is the company's most senior "risk owner" for cyber?



There is no commonly agreed role for ownership for cyber risk issues across FTSE350 companies with a wider range of positions being identified for this than in the previous year.

Leadership

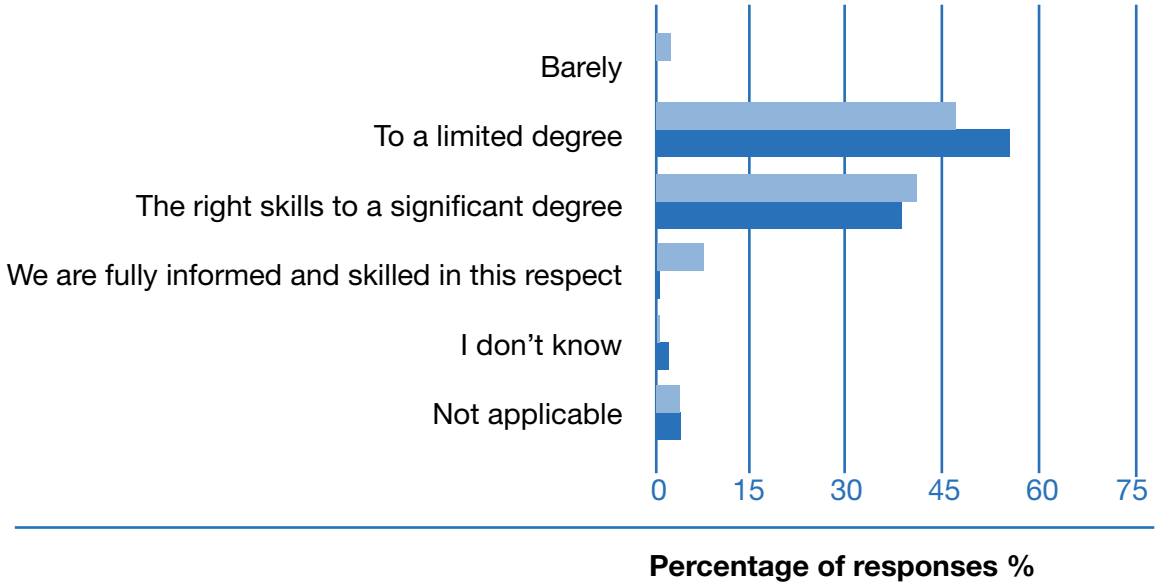
Where, in governance terms, is the "risk owner" for cyber held to account?



The main board is the most likely group to hold the company's cyber risk owner to account, with the audit committee and operating board also commonly taking up this role.

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?

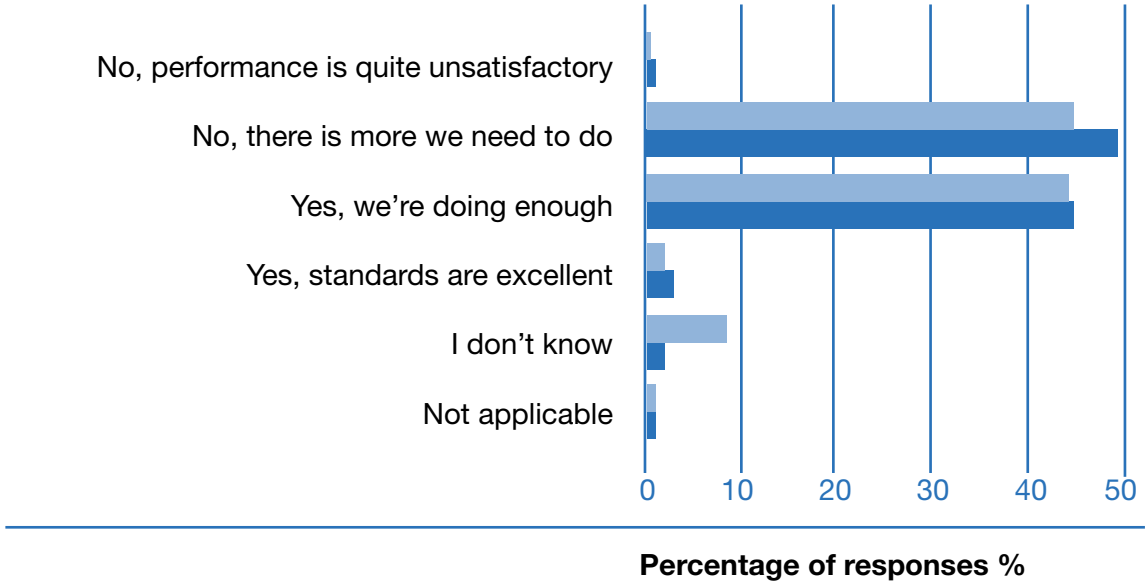


In 2014 a greater proportion of boards were thought to have the right skills "to a limited degree" and fewer were thought to be "fully informed and skilled" than in 2013.

2013 response
2014 response

Leadership

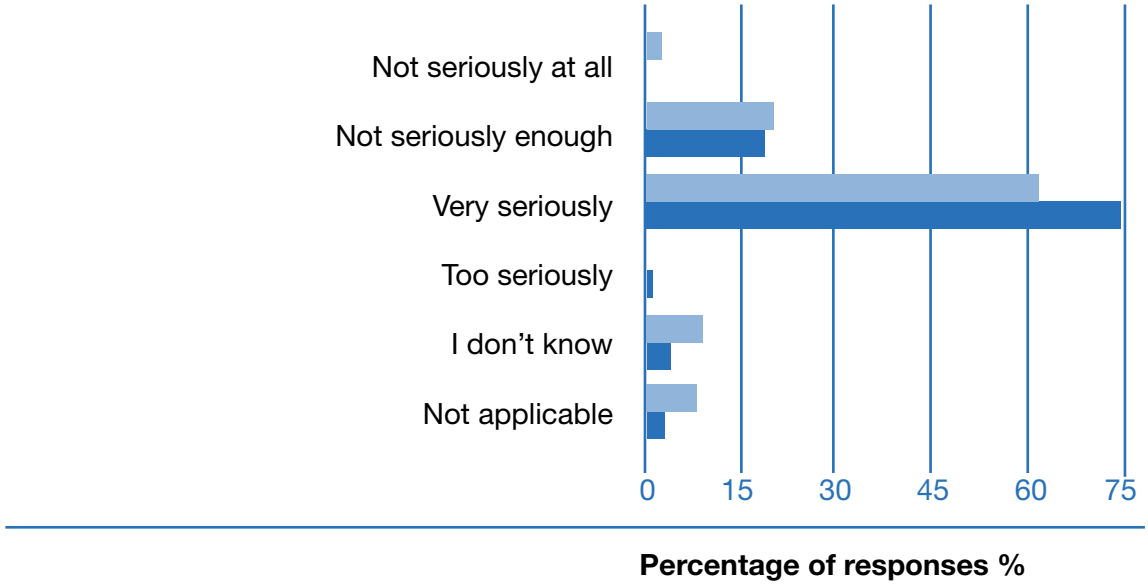
Do you feel the company is doing enough to protect itself against cyber threats?



Almost half (49%) or respondents believe that there is more to be done to protect their company from cyber threats.

Leadership

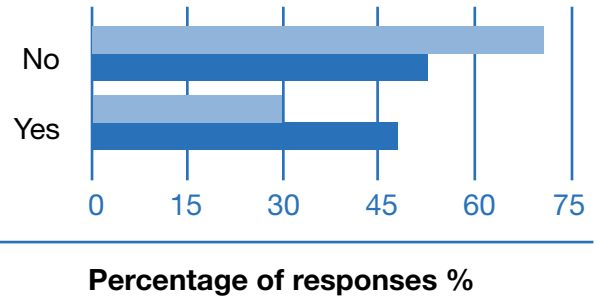
Are Board colleagues taking the cyber risk sufficiently seriously?



A greater proportion of audit chairs believe their boards take cyber security seriously than in 2013.

Leadership

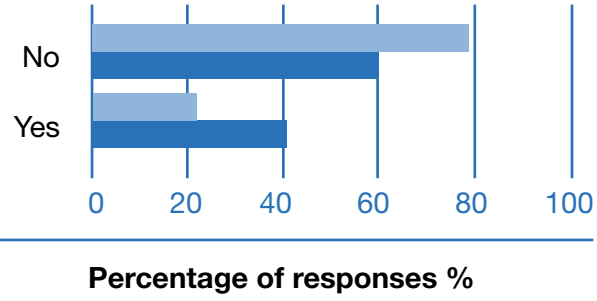
Have you personally undertaken any form of cyber security/information security training in the last 12 months?



A greater proportion of the audit chairs responding had undertaken some form of cyber security or information security training than in 2013.

2013 response
2014 response

Have other Board members undertaken any form of cyber security/information security training in the last 12 months?

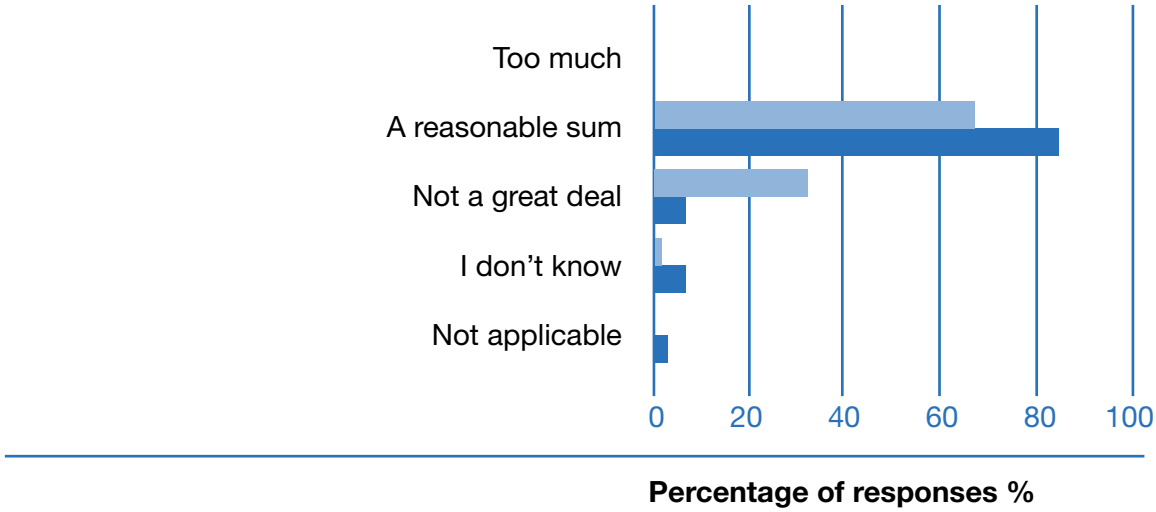


In 2014 boards were more likely to contain members other than the audit chair who had undertaken such training in the last 12 months.

2013 response
2014 response

Leadership

Given the risks you face, how appropriate is the investment you are making around cyber defences?

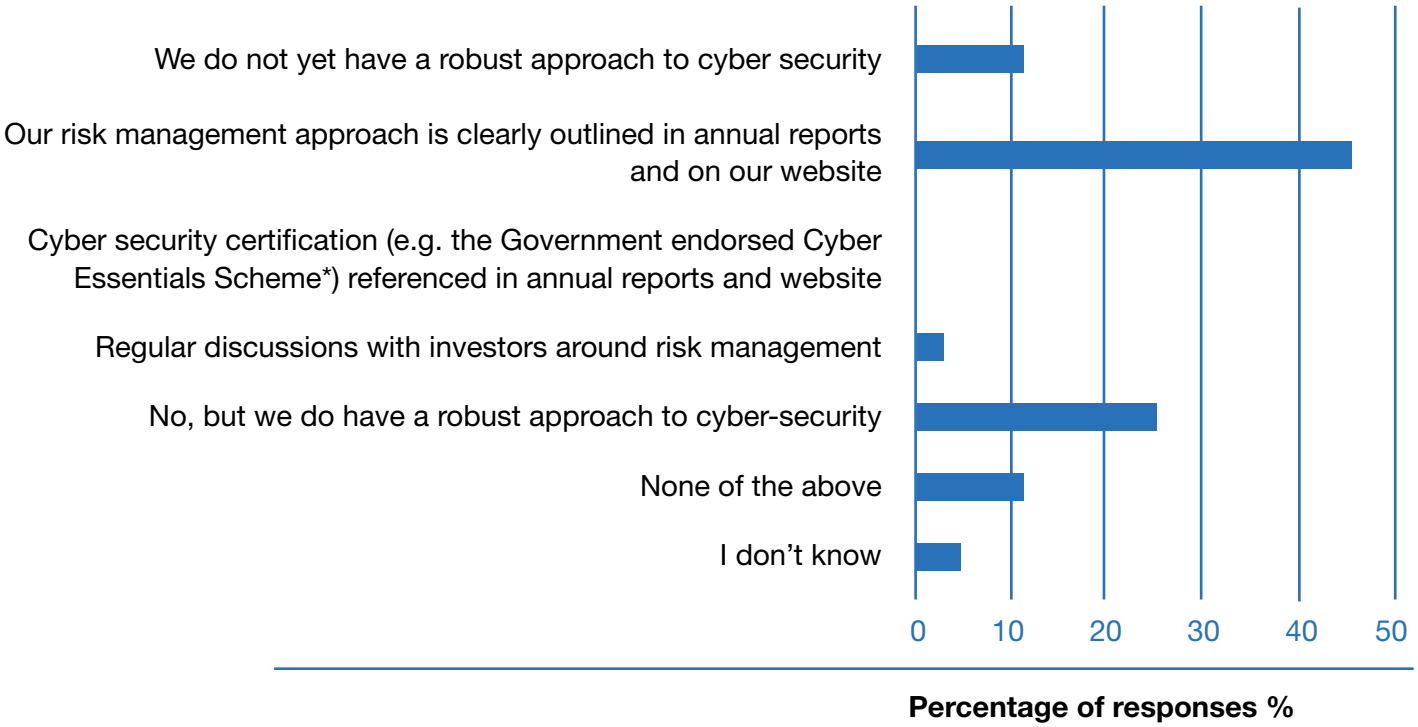


More respondents believe that their companies invest a reasonable sum in their cyber defences than was the case in the previous year.

2013 response
2014 response

Leadership

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



Many companies publicise their cyber security policy in their annual reports or on their website. One quarter of respondents have not done so despite claiming to have a robust approach to cyber security.

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

Risk Management

Summary of findings

One of the most clearly positive movements in the survey is that now nearly nine in ten (88%) of companies included a cyber-risk category in their risk registers up from 58% in 2013. While this percentage varies slightly between sectors the overall pattern is the same.

Around nine in ten (89%) respondents felt that cyber risks were either reasonably or clearly described in their company's risk register up from 70% in 2013. Those in Financial Services were slightly more likely to believe that cyber risks in their risk registers were clearly described (30%)

Main Boards were more likely to explicitly set their appetite for cyber risk, both for existing business and for new digital innovations, in 2014 than they were in 2013. Roughly the same proportions (18% vs 17%) had this "clearly set and understood" while more had a loosely set appetite (44%) in 2014 than in 2013 (35%). Only 31% thought their boards did "not really" set this compared to 41% in 2013. Boards in the "Retail, Travel and Leisure" industry were the most likely to explicitly set this for their businesses

Similarly to the previous year, when balanced against all types of risk, companies were more likely to rate cyber risk as being of low/operational level risk, then medium /segment risk and, least likely, as being of top/group risk. However the balance has shifted slightly with 29% rating cyber risk as top in 2014 compared to 25% in 2013. The sectoral pattern was very varied here with those in "Retail Travel and Leisure" giving cyber risk the highest priority and those in "Consumer Goods" the lowest. Financial services was an interesting case in that only 15% rated cyber as being of medium risk with the rest being split between low (45%) and high (40%).

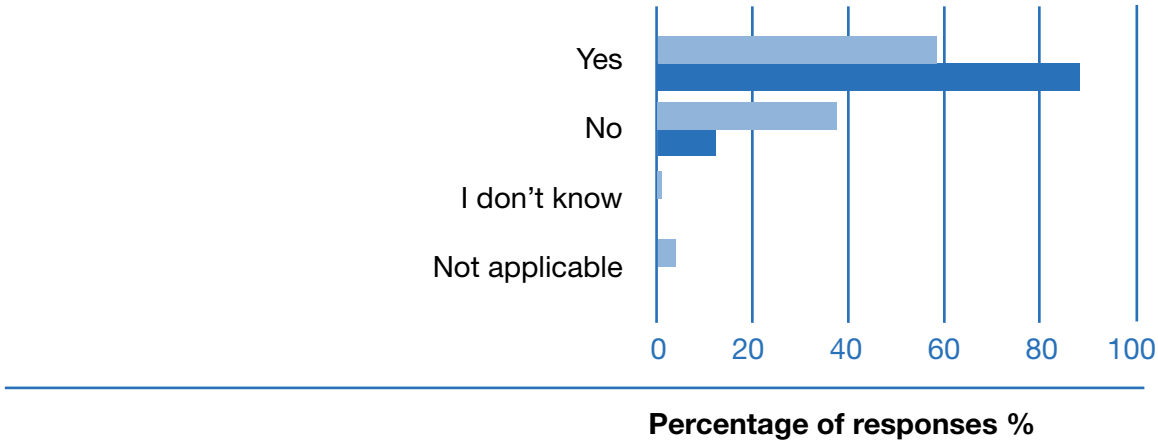
Management of the sharing of key data and information asset is clearly important. More audit

Management of the sharing of key data and information assets is clearly important. More audit chairs (48%) credited their boards with a basic understanding of key information/data sharing arrangements with third parties than in 2013 (40%). The proportions stating a "very clear" (11%) or "marginally acceptable" (18%) understanding were barely changed from the previous year. Positively, fewer audit chairs said their boards had a poor understanding of this (19% in 2014 vs 24% in 2013). Financial Services boards followed by those in "Technology, Healthcare and Technology" were believed to have the best grasp of this.

Audit chairs were also asked to reveal how their companies addressed cyber risks with their suppliers and other third parties. In 2014 companies were asked to indicate all applicable options, while in 2013 only a single answer was requested, making this unsuitable for comparison over time. Nearly half (48%) of all respondents used contract clauses to address cyber risks with suppliers with (44%) utilising pre-contract due diligence. A third (33%) of companies practised third party audits while a quarter (25%) used third party self-assessments. However, 24% of respondents did not know what methods their companies used.

Risk Management

Does the company's Risk Register include a "cyber risk" category?

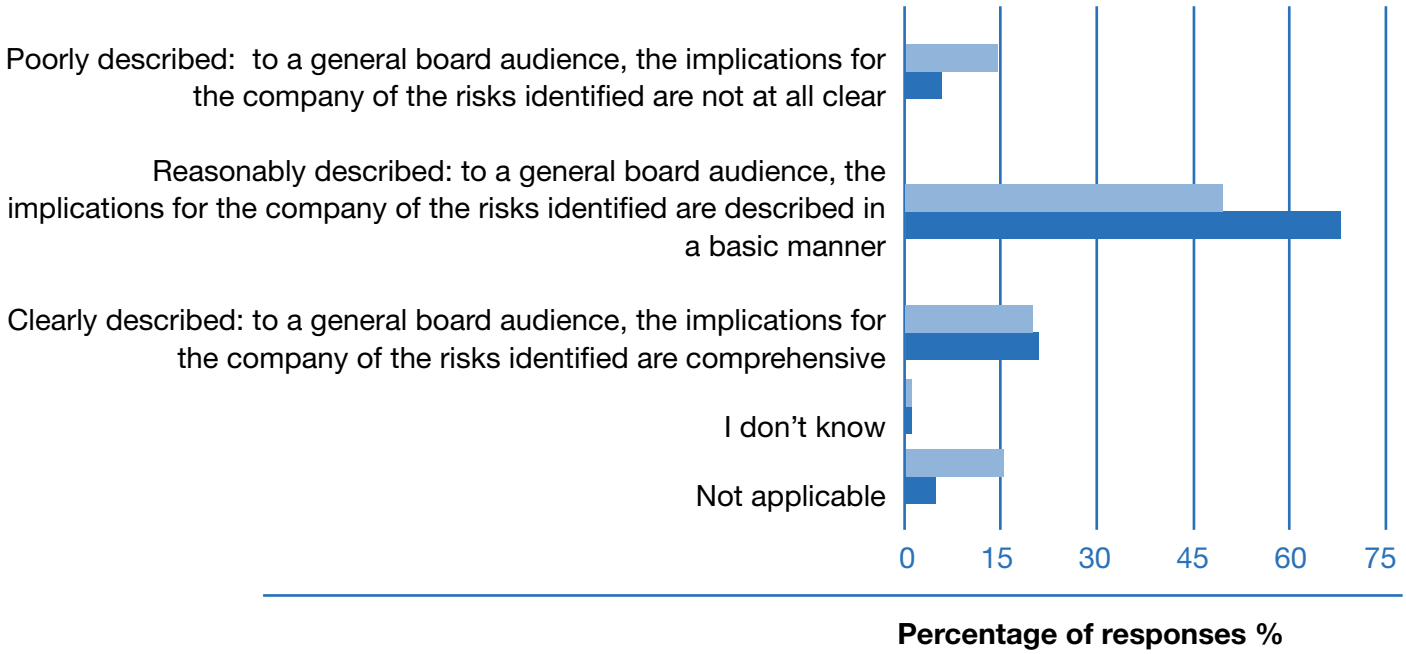


Companies were more likely to include a cyber-risk category in their risk registers than in the previous year.

2013 response
2014 response

Risk Management

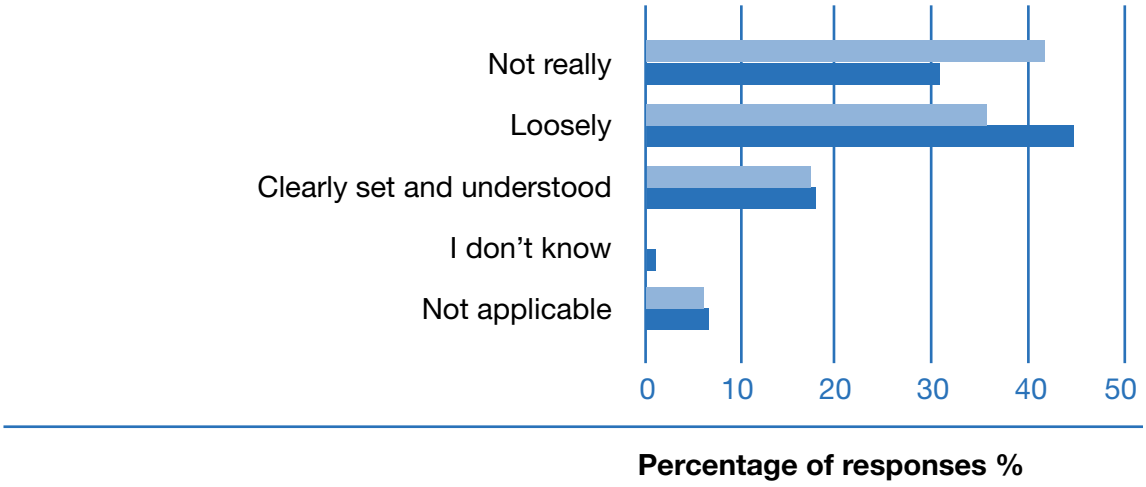
In the Risk Register, how well described (i.e. understandable to a general board audience) are cyber risks, and the potential consequences for the business?



Audit chairs were more positive about how clearly their companies' risk registers described cyber risks.

Risk Management

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

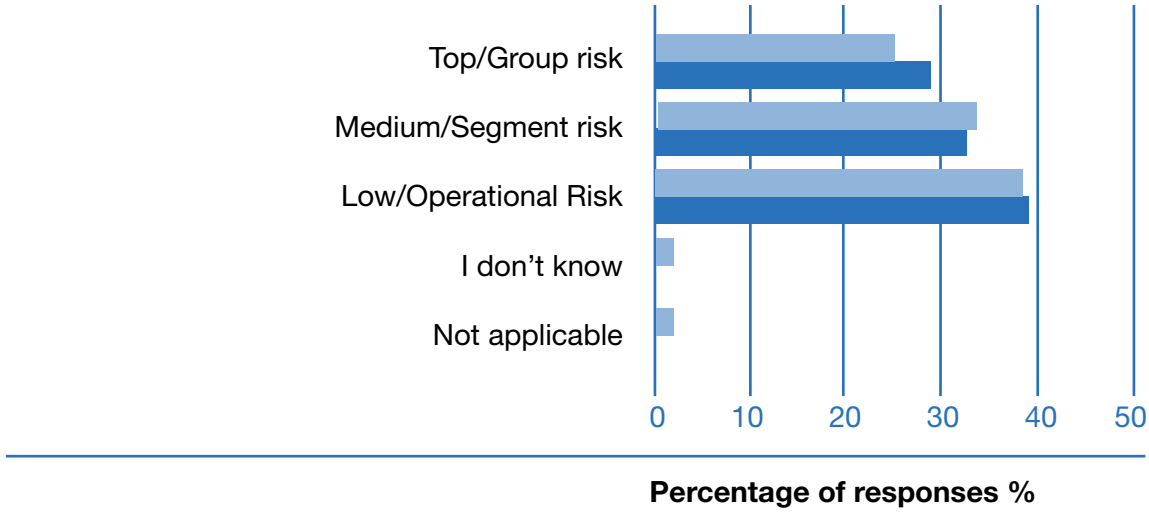


A slightly greater proportion of boards were said to explicitly set their company's appetite for cyber risk.

2013 response
2014 response

Risk Management

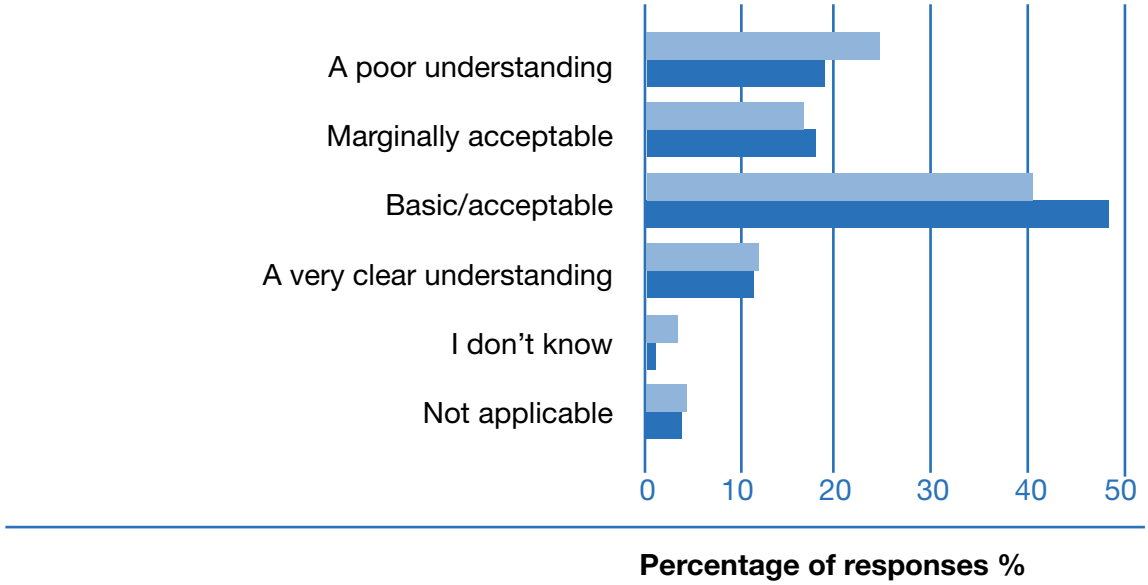
How significant or important is cyber risk, where risk is a product of likelihood and magnitude, when compared with all the risks the company faces?



Over the two year period companies tended to consider cyber risks as relatively less important, compared to other risks they faced. In 2014 there was an increase in the number of respondents that identified cyber risks as being of "top importance" (29%)

Risk Management

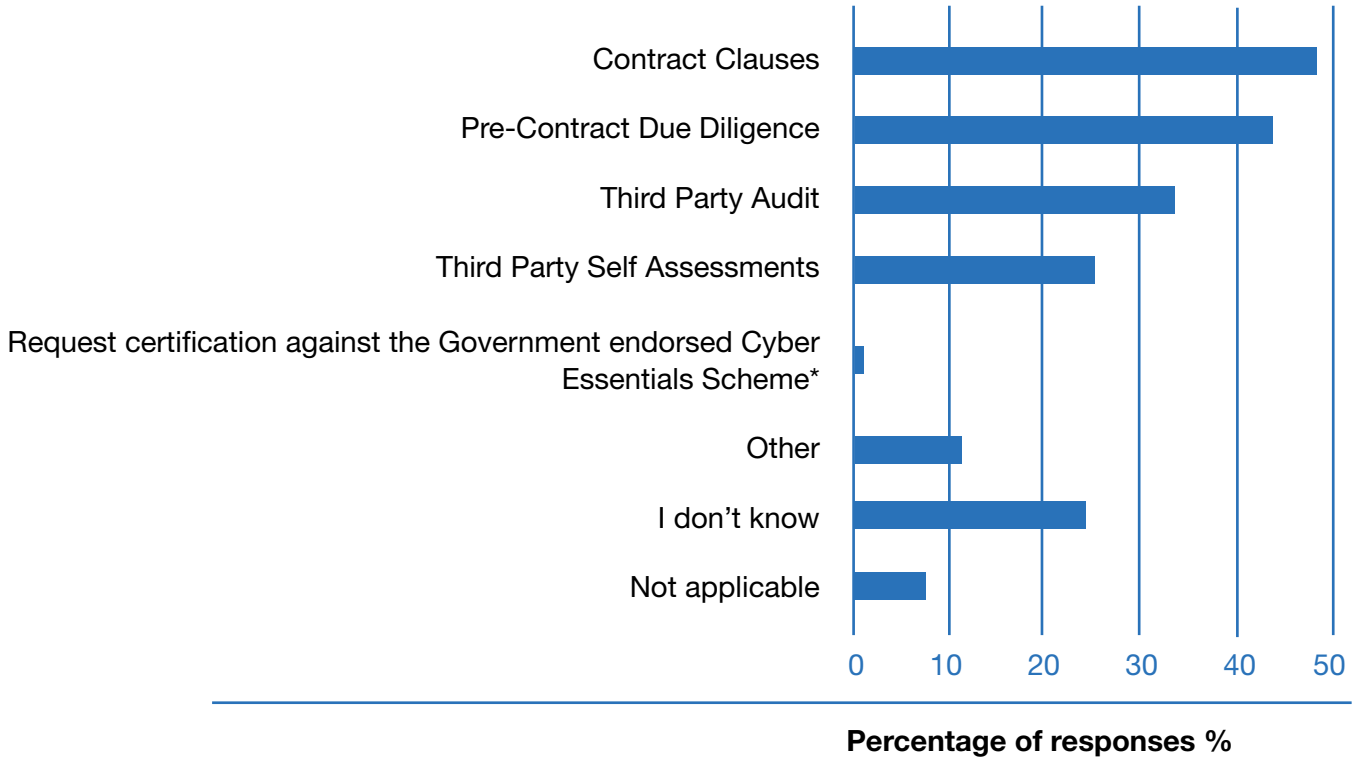
Does the main Board have an understanding of where the company's key information or data assets are shared with third parties (including suppliers, customers, advisors and outsourcing partners)?



Understanding of how the company shares key information and data assets with third parties is said to have improved since 2013.

Risk Management

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

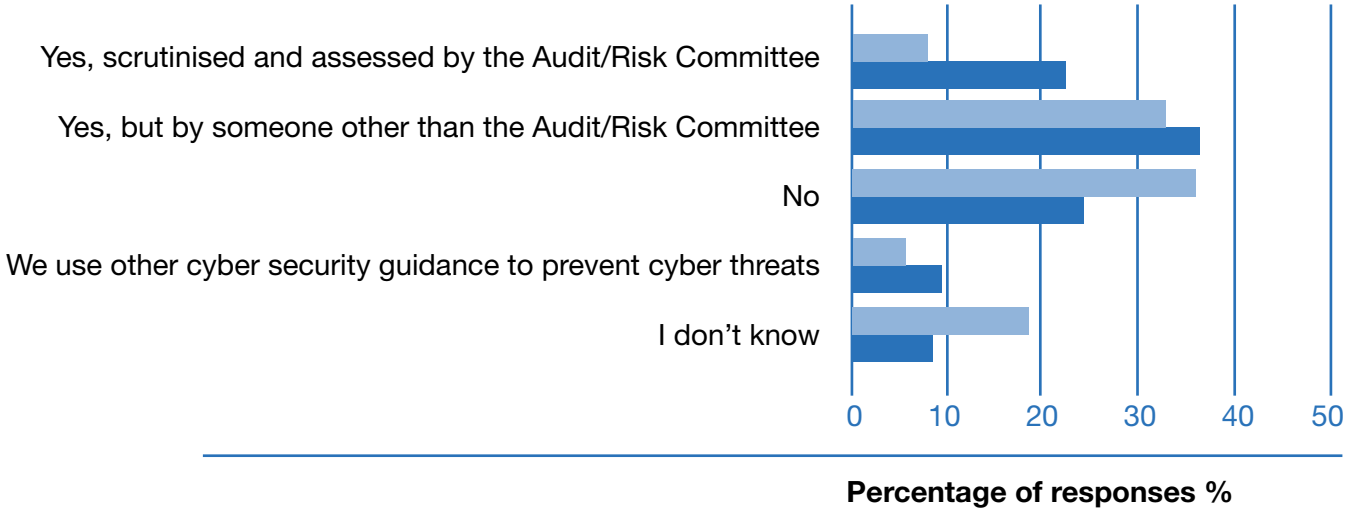


Nearly half of companies in the survey made use of contract clauses and pre contract due diligence in 2013. A large proportion made use of third party audits and third party self-assessments

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

Awareness of Help and Support

The Government estimates that 80% of the cyber threat could be thwarted by the basic security measures detailed in the Government's "10 Steps" Cyber Security Guidance* Has your company assessed itself against the Government's "10 Steps" Cyber Security Guidance?



In 2014 58% of companies had assessed themselves against the Government's "10 steps" Cyber Security Guidance, either through their audit committees or elsewhere compared to 40% in 2013. Assessments of 10 Steps through audit committee saw the largest increase (22% from 8%).

While not using the Government's 10 steps guidelines 9% of those in the survey had assessed themselves using some other guidelines (up from 6% in 2013). The proportion admitting to not using some form of cyber security guidance fell from 36% in 2013 to 24% in 2014.

** "10 Steps" Cyber Security Guidance:*
https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

Cyber Incidents

Summary of findings

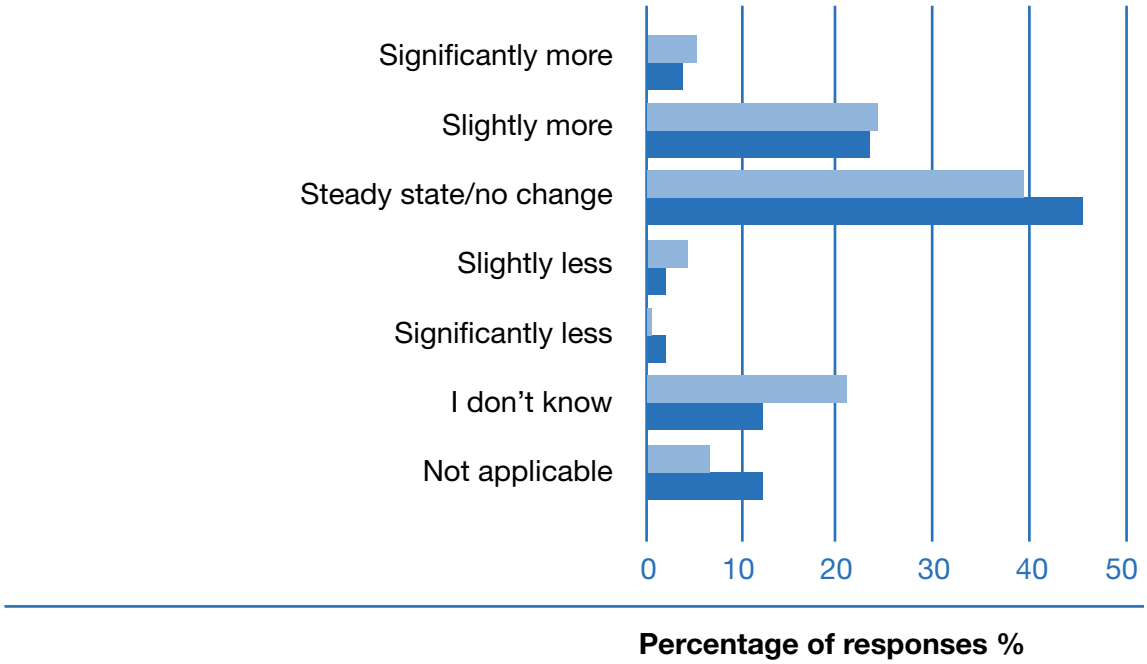
Respondents were most likely to report a "steady state/no change" in the level of cyber compromises over the last year (45% in 2014 vs. 39% in 2013). Of the rest, far more reported slightly (23%) or significantly more (4%) cyber occurrences than less (4%), however there is no conclusive difference here from the previous year. Fewer audit chairs reported that they "did not know" about the level of compromises (12% down from 21%); curiously more reported this as being "not applicable". "Technology, Healthcare and Communication" companies were the most likely to report an increase in cyber occurrences.

A greater proportion (48%) of audit chairs believed that their companies handled cyber occurrences and compromises quite well or very well in 2014 than did so in 2013 (43%). Reassuringly, in neither year did anyone state these cyber compromises were dealt with in an unacceptable manner. In both years this question attracted a lot of "don't know" or "not applicable" answers (35% in 2014 and 40% in 2013).

When asked where in governance terms these events were considered, respondents were equally likely (37%) to identify the Executive/Operational Board and the Audit Committee. The IT or Security Board were mentioned by 31% of respondents while 19% identified a separate Risk Committee. Companies were able to select more than one answer in 2014 and not in 2013 so for this reason comparisons across years have not been made.

Cyber Incidents

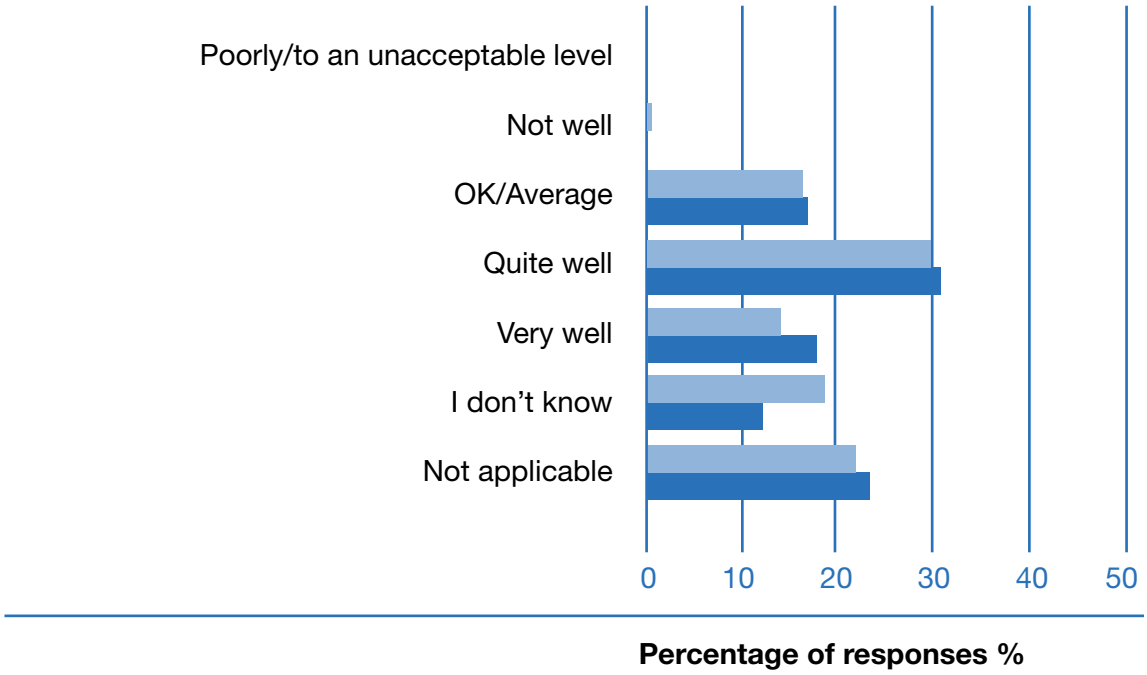
Based on your own recollection, has the company suffered more or fewer cyber compromises and occurrences over the last year?



While a greater proportion of respondents were able to offer an opinion on this the balance of answers was similar to the previous year with largest proportion reporting no change and over a quarter reporting an increase.

Cyber Incidents

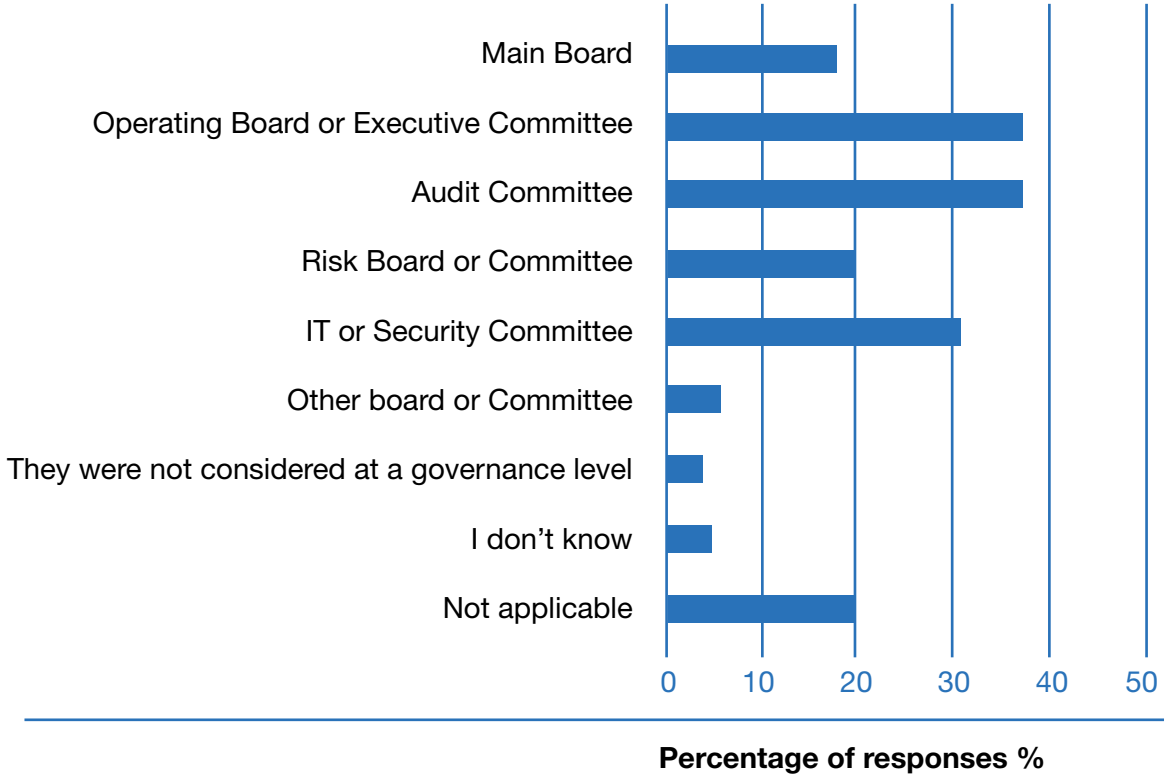
From your own recollection, how well did the company respond to those compromises and occurrences?



Respondents were slightly more positive about how well their companies handled cyber compromises and occurrences in 2014 than in the previous year.

Cyber Incidents

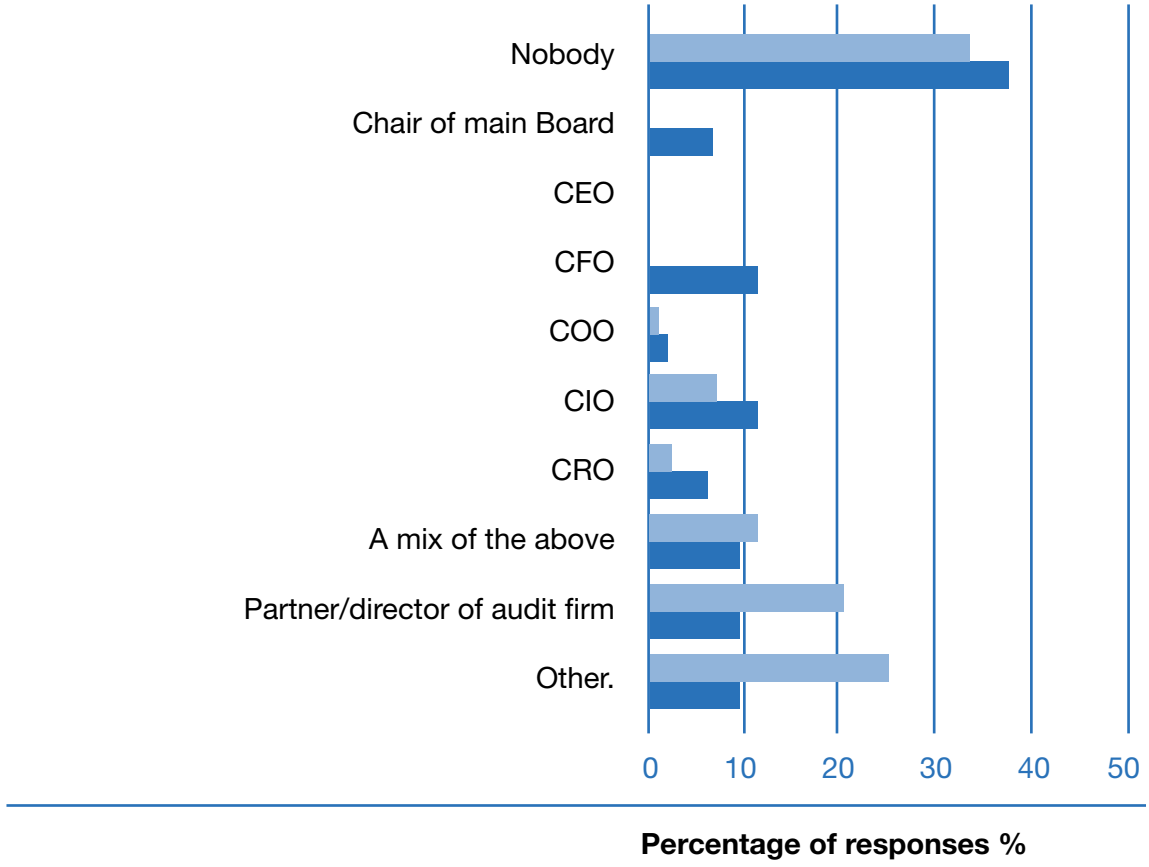
Where, in governance terms, were these compromises and occurrences considered?



The executive board, audit committee and the IT/Security board were the most commonly identified governance groups where cyber risk events were considered.

Completion of Tracker

In order to optimise results, we request that this questionnaire is not passed to the 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?



37% respondents answered this questionnaire on their own (compared to 33% in 2013) however those that did not identified a wide variety of different roles they consulted.

Methodology

The Tracker ran from 1 September to 24 October 2014. 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 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 2014 a third of FTSE 350 companies (108) responded to the survey. This is half as many as responded in the first year of the survey (217). Such a change in response rate 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, restricting analysis to only those companies who had responded in both years of survey was considered, in order to present a very robust view of how these companies have progressed between 2013 and 2014, accepting that they might not be representative of the FTSE 350 as a whole.

However there is 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, the sector which 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.

There are still issues around non-response, but 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 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

Tracker Report 2014

FTSE 350 Cyber Governance Health Check

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

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET

Tel: 020 7215 5000

biscybersecurity@bis.gsi.gov.uk

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/15/37