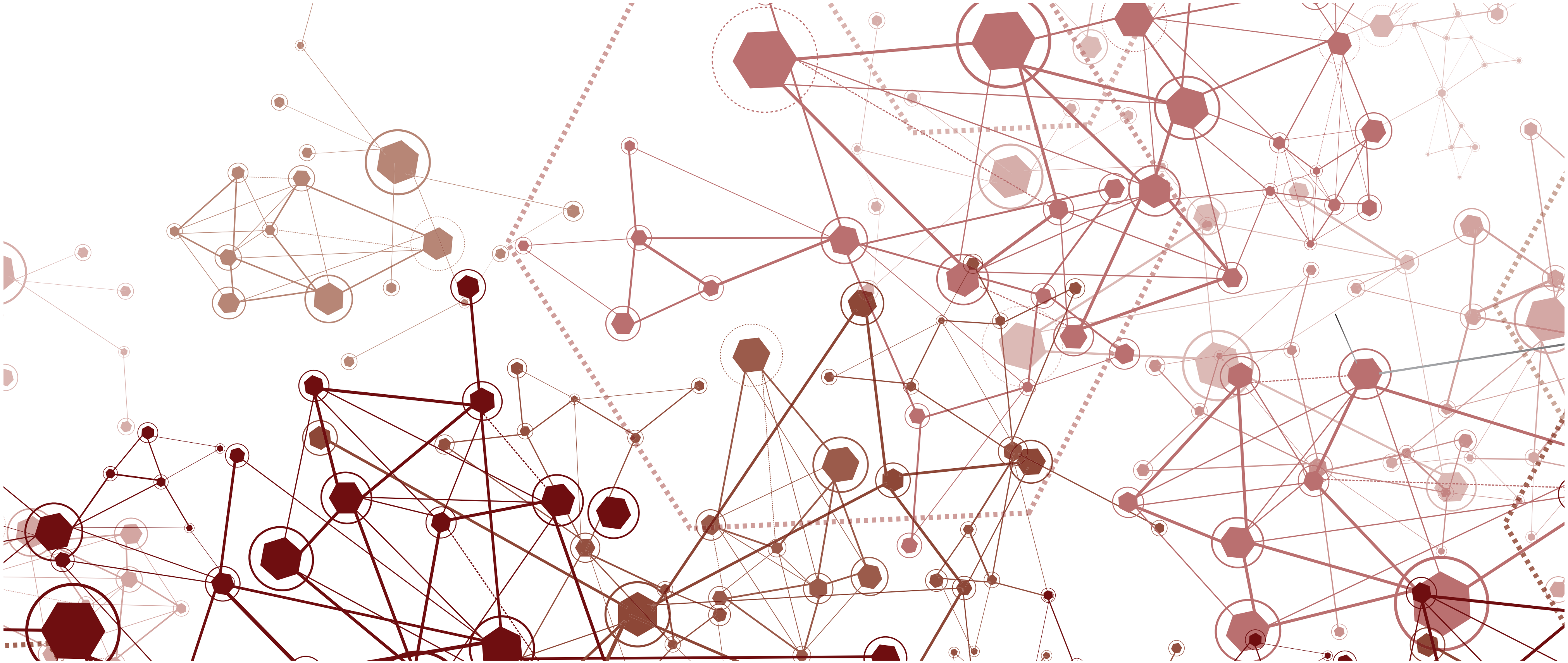
HM Government

FTSE 350 Cyber Governance Health Check

Tracker Report

November 2013



Contents

Foreword

The internet powers economic growth, fosters innovation and creates jobs. Alongside the many benefits that companies gain from operating in cyberspace, the security threats continue to grow; threats from those looking to seize commercial advantage and intellectual property, to those looking to destroy critical data and undermine the integrity of systems.

Now is the time for UK businesses to embrace the challenges and opportunities presented by cyberspace. Whilst the challenges should be taken seriously, they can also be viewed as an opportunity to realise considerable strategic, financial and reputational benefits.

I am glad to see so many FTSE 350 companies placing significant importance on the cyber risk and that it is now on many strategic risk registers. But the Tracker report shows us there is more to do. There is still a great deal of concern and uncertainty about cyber security within board rooms. Many admit that they do not actively manage the risk at board level. Nearly half state clearly that there is more they need to do to protect themselves.

I am very grateful to all of the FTSE 350 Chairs and Audit Committee Chairs who contributed to the content of this report, and would also like to thank the audit community for their crucial support in helping to deliver the Cyber Governance Healthcheck. I believe the results of this report will be of use to the wider economy in showing the way forward in managing the cyber risk, and supporting Government's objective of making the UK one of the safest places to do business in cyberspace.

David Willetts

Executive summary

A SERIOUS ISSUE

64% of Chairs think their Board colleagues take cyber risk very seriously.

WHO OWNS THE RISK?

When asked who owns the cyber risk for their company, Audit Committee Chairs responded with a wide variety of roles.

CYBER IS A BUSINESS RISK

56% of respondents said their strategic risk register includes a cyber risk category.

CYBER SAVVY BOARDS

Most Chairs think their Boards are qualified, to some extent, to manage innovation and risk in a digital age.

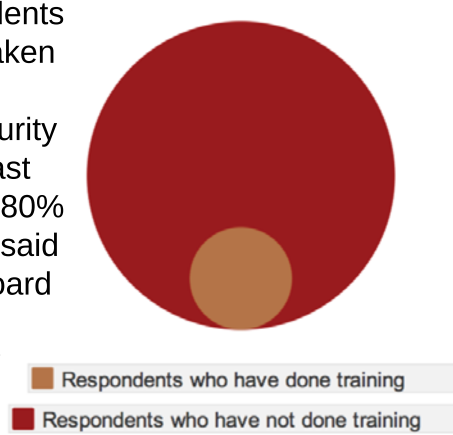
2% indicated their colleagues were 'barely qualified'

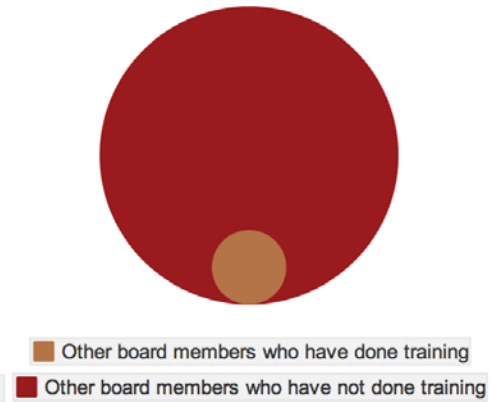
36% think they have 'good skills'

11% think they are well positioned for the digital age

TRAIN YOUR BOARD

75% of respondents had not undertaken any cyber or information security training in the last 12 months and 80% of respondents said none of their Board colleagues had undertaken any either.

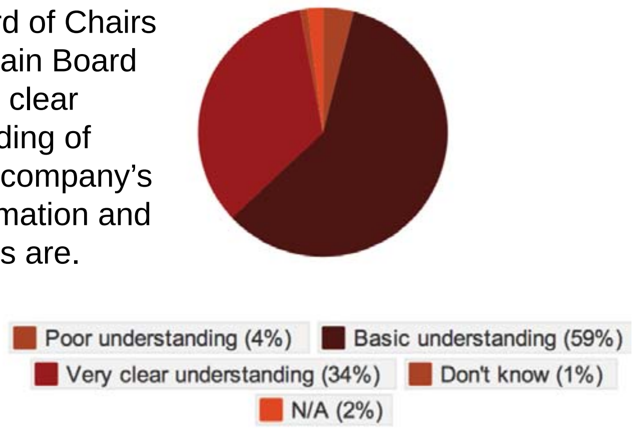




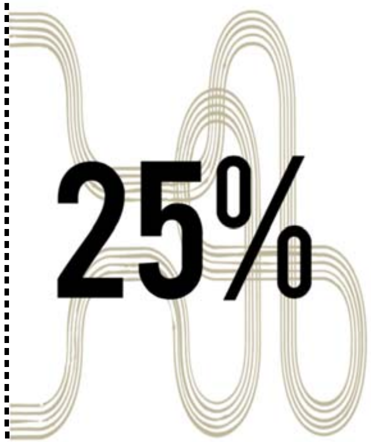
Executive summary

KNOW YOUR KEY DATA ASSETS

Over a third of Chairs said the main Board has a very clear understanding of what their company's main information and data assets are.



WHO HAS YOUR KEY DATA ASSETS?



A quarter of respondents said the main Board has a poor understanding of where the company's key information or data assets are shared with third parties (e.g. suppliers, advisors, customers and outsourcing partners).

UNDERSTAND THE THREAT

40% of Chairs said the main Board does not receive regular threat intelligence from their CIO or Head of Security.

THE IMPACT OF A CYBER ATTACK

Less than half of FTSE 350 Chairs think their main Board has a clear understanding of the potential impact of information and data asset losses.

INFORMATION SHARING

Nearly half of the respondents said their employees are encouraged to share information with other companies in order to combat cyber threats.

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 the FTSE 350, it offers significant insight into the cyber governance of the UK's highest-performing businesses.

What is the Cyber Governance Health Check?

This is an initiative that has been designed to understand and improve the cyber security governance behaviours of the FTSE 350. It is formed of two discrete elements:

i) The first stage is the 'Tracker', a web-based tool to assess and report levels of cyber security awareness and preparedness across the FTSE 350, from a governance perspective. Completion of the Tracker has resulted in this aggregated report, as well as confidential individual benchmarking reports for each participating company.

ii) The second stage is the 'Diagnostic', an audit-based tool which builds on the results of the Tracker. The Diagnostic will assess and report areas of cyber security vulnerability and good practice, and suggest what actions management can take to address vulnerabilities and build on good practice. This stage will be rolled out over the next six months.

The UK Government is delivering both stages of 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 the future in order to chart governance behaviours across the economy, enabling further benchmarking as both threats and mitigation best practice develops.

The 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 A sets out the aggregated sectors used for the purposes of this report.

Annex B contains important links to key Government cyber security guidance and support.

Respondent profile | Summary of findings

The Financial Services sector provided the largest number of respondents with 80 while the lowest number came from the Pharmaceuticals, Biotechnology and Healthcare sector. The sectoral make-up of respondents is heavily weighted by the fact that there a large number of financial institutions in the FTSE 350.

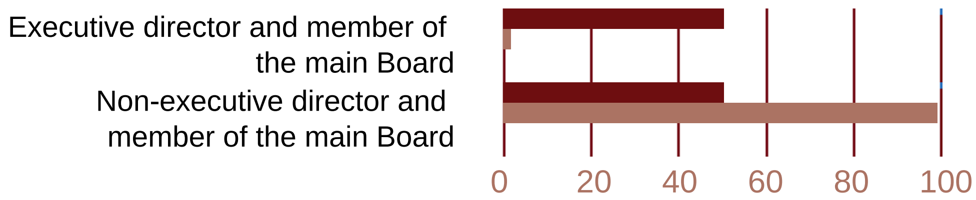
Of the companies that responded the majority generated over half of their sales outside the UK. The proportion of companies' employees being based outside the UK was very varied. This could be advantageous to the survey as a company's attitude to cyber security risk could well be influenced by the level of internationalisation of that company.

Respondents recognised cyber security risks as a very relevant issue. The following risk factors are listed in order of the number of respondents identifying with them:

- Shareholder value is significantly dependent on secrecy and security of our intellectual property
- We deliver services vital to the Critical National Infrastructure
- We run safety-critical automated systems
- We handle high value financial transactions or other assets at high risk from theft or fraud
- More than 50% of our revenue comes through online interactions

Respondent profile

Which of the following describes you?

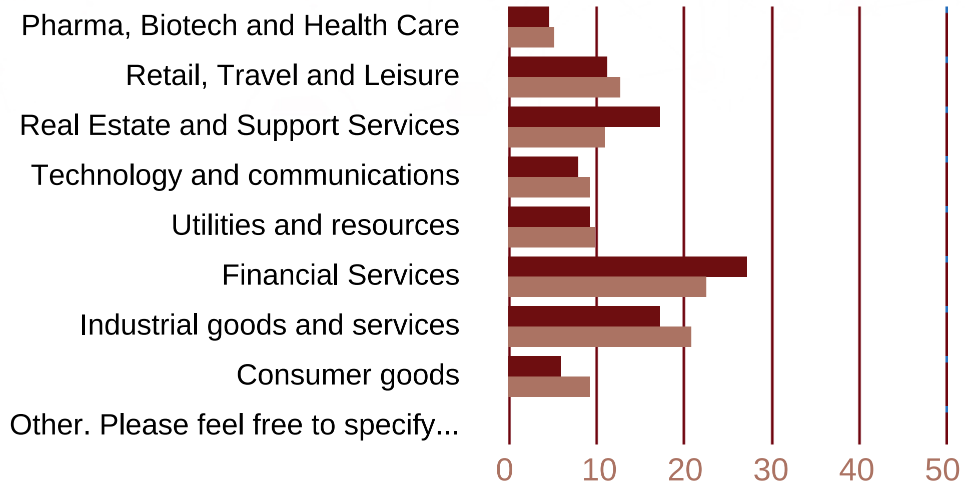


Percentage of responses
(Total number of responses: 326)

- **Chairs**
- **Audit Committee Chairs**

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

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



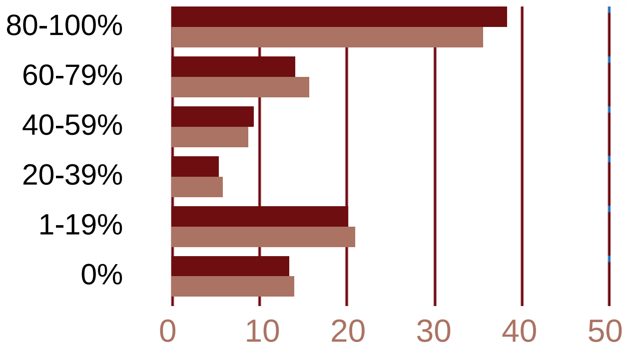
Percentage of responses
(Total number of responses: 326)

- **Chairs**
- **Audit Committee Chairs**

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

Respondent profile

What proportion of company revenue/sales are generated outside the UK?



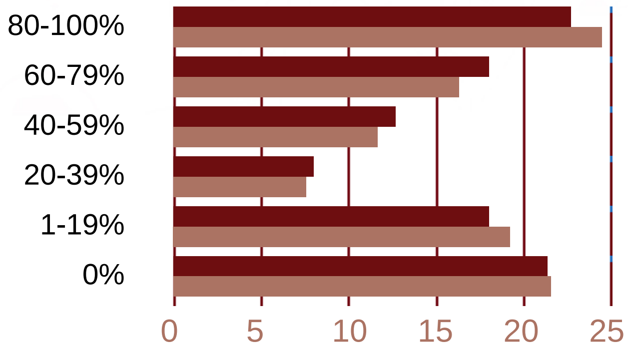
Percentage of responses
(Total number of responses: 323)

Chairs

Audit Committee Chairs

Total number of companies which provided at least one response: 215
Total number of Chair responses: 150
Total number of Audit Committee Chair responses: 173

How many employees are based outside the UK?



Percentage of responses
(Total number of responses: 324)

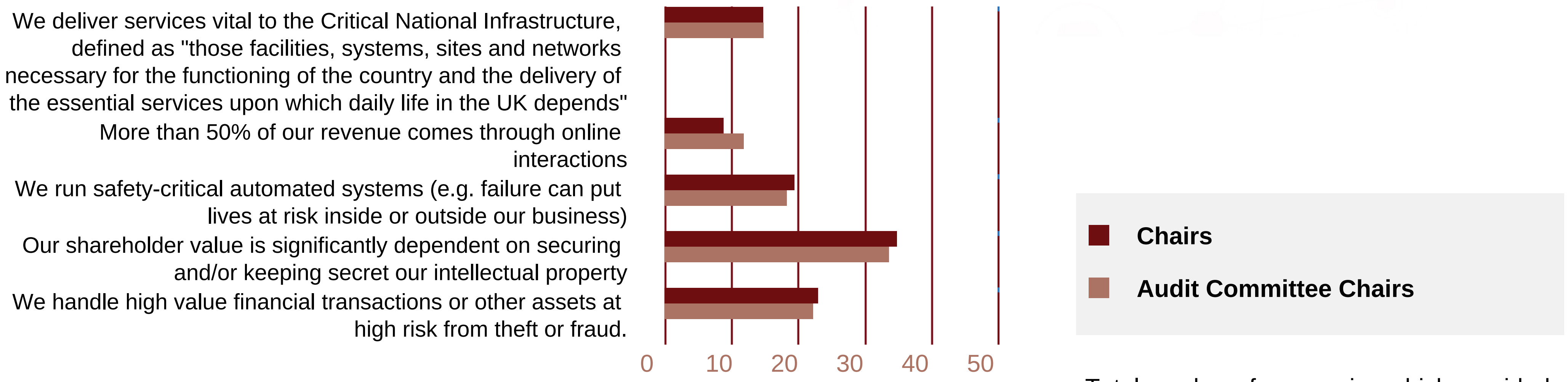
Chairs

Audit Committee Chairs

Total number of companies which provided at least one response: 215
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 173

Respondent profile

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



Percentage of responses
(Total number of responses: 375)

Total number of companies which provided at least one response: 157
Total number of Chair responses: 171
Total number of Audit Committee Chair responses: 204

Encouragingly, the majority of respondents (60%) stated that their Boards have a basic or acceptable understanding of the company's **key information and data assets**, with a third (33%) reporting "a very clear understanding". Respondents from the more cyber mature Technology and Communications and Financial Services sectors were the most likely to say there was "a very clear understanding" (56%) while only 14% in the Industrial Goods and Services sector said this.

A higher proportion of respondents (40%) said their Board had "a very clear understanding" of the **value** of their companies' key information and data assets. This was highest in the Pharmaceuticals, Biotech and Healthcare sector (79%) and lowest in the Utilities and Resources sector at 14%.

Boards are evenly split between having a basic/acceptable understanding (45%) and a very clear understanding (46%) of the potential **impacts** of losing their key information and data assets assets. Financial Services demonstrated the highest proportion of very clear responses (62%), but the Utilities and Resources (28%) and Industrial Goods and Services sectors (31%) showed the least understanding.

The majority (56%) of respondents said their Boards "never" or "rarely", **reviewed** key information and data assets to confirm the legal, ethical and security implications of retaining them.

This figure was only 30% for the Financial Services sector, but 78% for the Consumer Goods and Industrial Goods and Services sectors

Some 19% said that their Boards **regularly received intelligence on cyber threats** from their CIO or Head of Security, with 43% stating that this never happened. Boards in the Technology and Communications sector were the most likely to seek regular intelligence (33%), whilst the Pharmaceutical, Biotech and Healthcare sector was the most likely never to receive such information (60%)

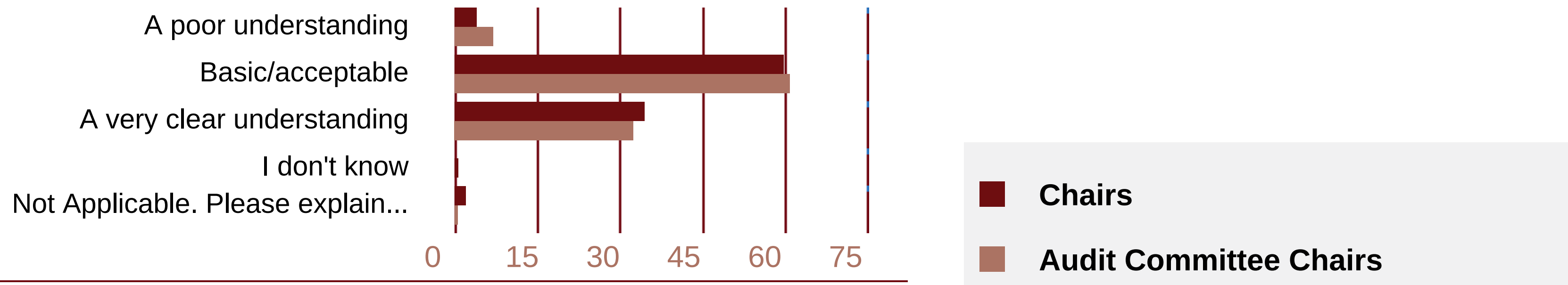
The majority of respondents (63%) thought their Board members possessed only a marginal **understanding of their own cyber risk profile** with the most of the remaining responses evenly distributed between "fully understanding" (17%) and "poor" understanding (16%). Utilities and Resources sector Boards were said to be the most aware, with 41% of respondents reporting a "full understanding".

The Boards of 44% of respondents to the survey encouraged their technical staff to **enter into formal information sharing exchanges** (e.g.www.cisp.org.uk) with other companies in order to improve their situational awareness, see emerging threats and learn from others. Some 33% said they did not participate in information exchanges. The more cyber mature Technology and Communications sector was the most likely (64%) to enter into

Understanding the threat

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, customer/personal data, etc)

The majority of respondents admit that the main Board only has a basic or acceptable understanding of their companies' key information and data assets, with around a third claiming a "very clear understanding".

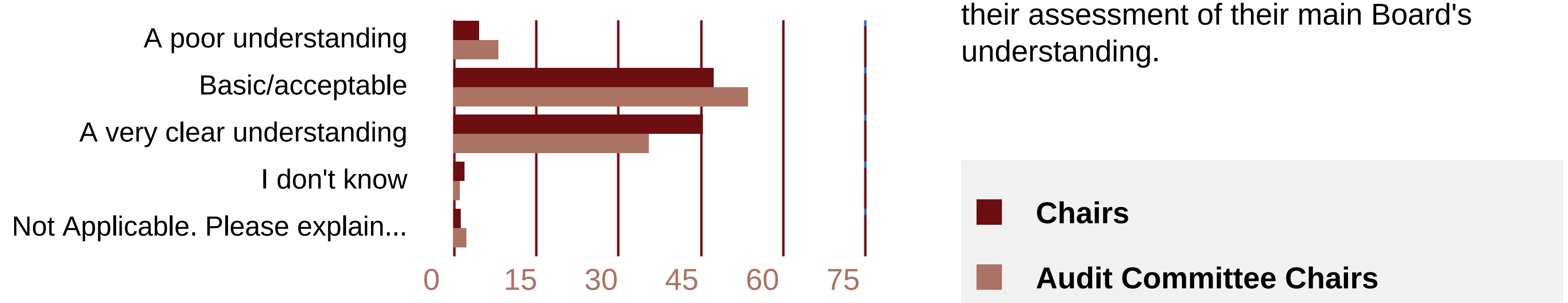


Percentage of responses
(Total number of responses: 326)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

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)?



Percentage of responses
(Total number of responses: 324)

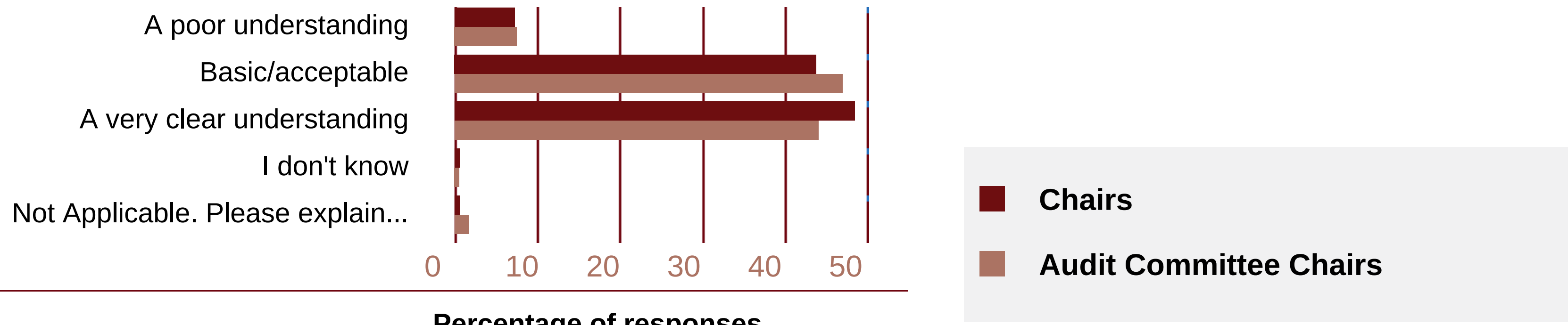
A slight majority of respondents admit that the main Board has only a basic or acceptable (or in a few cases, poor) understanding of the value of their company's information and data assets. Audit Chairs tend to be more pessimistic in their assessment of their main Board's understanding.

Total number of companies which provided at least one response: 217
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 173

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?

Less than half of respondents believe their main Boards have a very clear understanding of the potential impacts of information and data asset losses, with 7% stating their Boards have a poor understanding

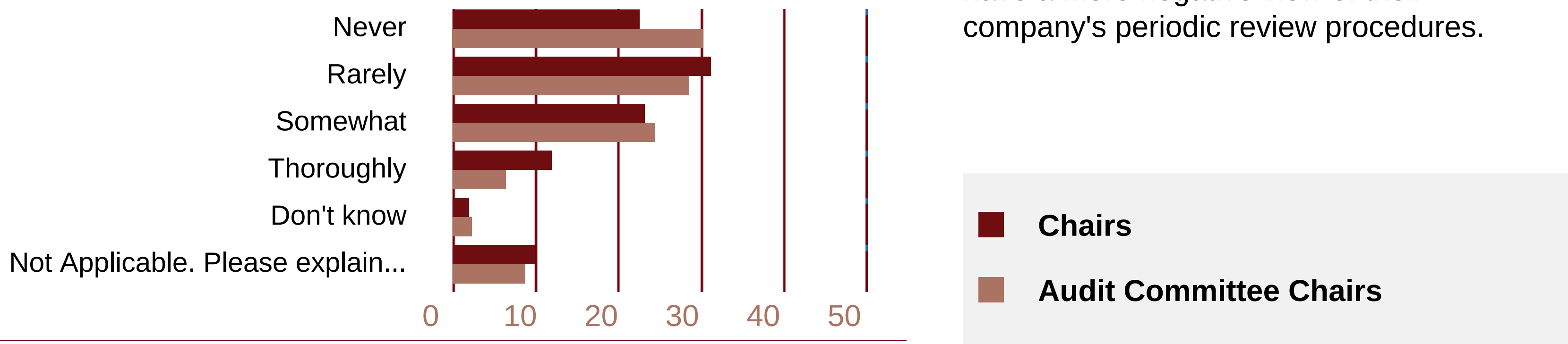


Percentage of responses
(Total number of responses: 326)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

Understanding the threat

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



Percentage of responses
(Total number of responses: 325)

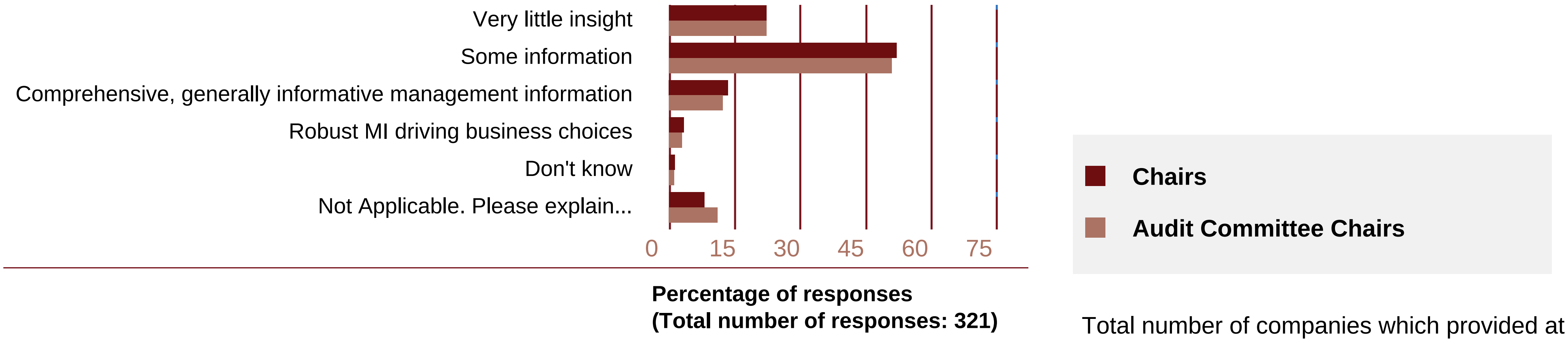
Over half of companies rarely or never review their key information and data assets. Only 12% of Chairs and 6% of Audit Chairs believe a thorough review takes place here. Overall, Audit Chairs tend to have a more negative view of their company's periodic review procedures.

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 173

Understanding the threat

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

22% of respondents state that their Board's discussion of cyber risk is based on "very little insight", with only around 16% believing it to be based on comprehensive or robust management information.

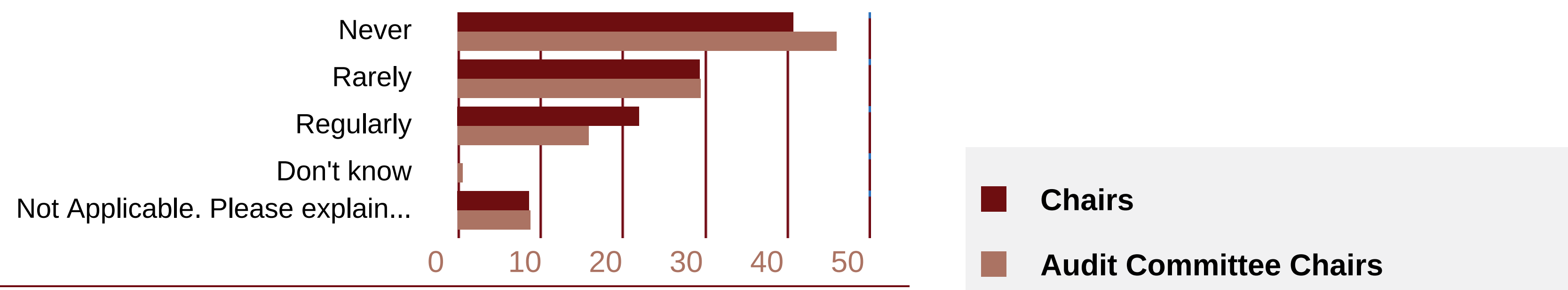


Total number of companies which provided at least one response: 214
Total number of Chair responses: 149
Total number of Audit Committee Chair responses: 172

Understanding the threat

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

Less than a fifth of all respondents said that their Boards received regular intelligence on cyber threats from their CIO or Head of Security. Over 40% of respondents stated that this never happens.

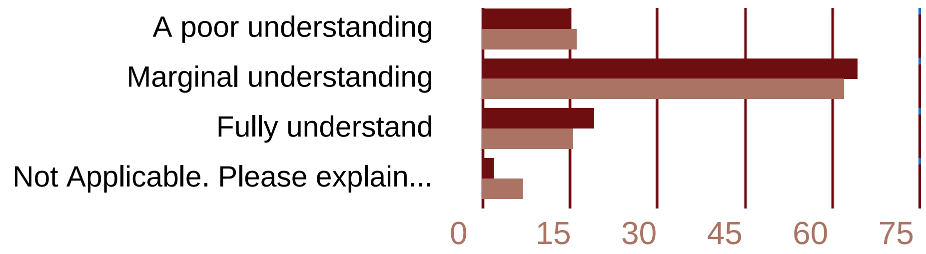


Percentage of responses (Total number of responses: 322)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 171

Understanding the threat

In your view do all Board members understand their own personal cyber risk profile (e.g. how to prevent being a target of an electronic attack)?



Percentage of responses
(Total number of responses: 326)

Almost two thirds of respondents stated that their Board members possessed a marginal understanding of their cyber risk profile, with other respondents evenly spread between "fully understanding" and "poor understanding". As with much of the rest of the results, Audit Chairs tended to be more negative but this difference cannot be said to be statistically significant.

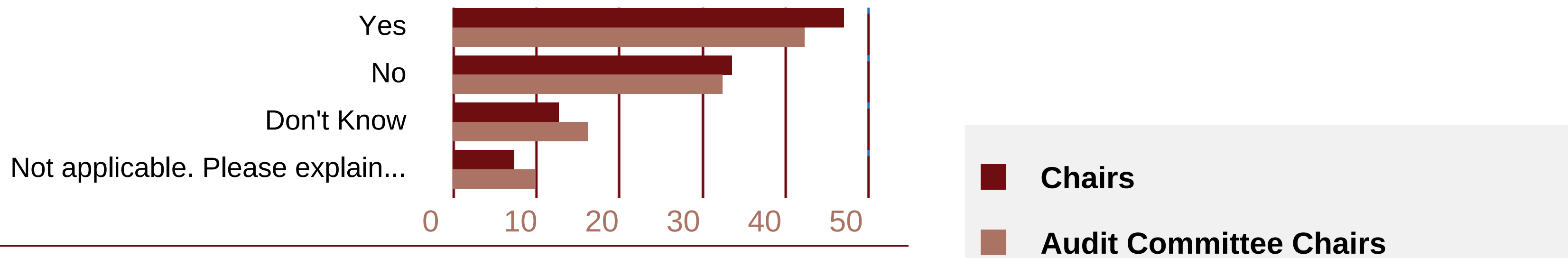
- **Chairs**
- **Audit Committee Chairs**

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

Understanding the threat

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

While nearly a quarter of respondents were unable to answer this question, around 44% of respondents confirmed that their staff were encouraged to share information with other companies in order to combat cyber security threats.



Percentage of responses
(Total number of responses: 324)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 150
Total number of Audit Committee Chair responses: 174

Leadership — Summary of findings

Only 10% of respondents stated that their Boards r**eviewed their strategic risk register** at every meeting, the majority covering this annually (40%) or bi-annually (31%). In the Technology and Communications sector, 22% of respondents said this was done at every meeting. In the Financial Services sector this was most likely to be quarterly business (31%).

Just over half (51%) **expect cyber risks to slightly increase** in the next year, with about a quarter (24%) expecting the same level to be maintained. Only 15% foresaw a significant rise in the cyber threat. Real Estate and Support Services sector respondents were least likely to predict a significant increase (2%) and the most likely to expect things to stay the same (35%). In the Pharmaceutical, Biotech and Healthcare sector 20% of respondents actually predicted a slight or significant decrease in the cyber risk.

On the **importance of cyber risks to their business**, 50% rated them extremely important, with 46% regarding them as being of “limited” importance. In the Technology and Communications sector 82% rated cyber risks as extremely important. Respondents in Real Estate and Support Services were the most likely to rate cyber risks as being of limited importance (67%)

The majority of respondents believe (47%) or think (41%) that their staff are comfortable reporting information and data asset losses.

Cyber risk is not **regular Board business** for 35% of respondents, with a further 37% reporting it as an occasional 6 monthly update or just a matter of being informed when things go wrong.

Only 4% said they actively managed their **cyber risk profile** throughout the year, with a further 10% regularly considering cyber risk in their decision making. The Board of 8% of respondents viewed cyber risk as a technical topic, not warranting Board level consideration. Not a single respondent from the Pharmaceutical, Biotech and Healthcare sector said their Boards actively managed their cyber risk profiles or regularly considered cyber risk, while 23% of those in the Retail Travel and Leisure sector said this was the case.

Some 39% of respondents reported being “anxious” or “very anxious” about their **company’s approach to cyber risks**, with 47% being not particularly concerned. A further 4% reported being relaxed or very relaxed about their company’s cyber security policy. Respondents in the Retail Travel and Leisure sector were the most concerned, with 59% being “anxious” or “very anxious” but strangely also the most likely to report being “relaxed” or “very relaxed” (10%).

Principal Governance responsibility for assessing and monitoring cyber threats is quite varied between companies in the FTSE 350.

Leadership | Summary of findings

Most commonly the responsibility resides with the Operating Board/Executive Committee, the main Board or the Audit Committee, with between 19% and 20% of respondents naming these groups. In a very small number of cases respondents did not know, or said no-one had this responsibility. The Audit Committee was the most commonly nominated body in the Pharmaceutical, Biotech and Healthcare sector (33%) and the Retail,Travel and Leisure sector (46%); while the Executive Committee was highest for the Utilities and Resources sector (34%). The Consumer Goods sector was the most likely to name the head of IT (29%).

According to 30% of respondents, the main Board ***should*** have governance of cyber risk issues, with the Audit Committee and Executive Committee being named by 20% and 19% of respondents respectively. The Audit Committee was most nominated by the Pharmaceutical, Biotech and Healthcare sector (36%) and the Retail, Travel and Leisure sector (43%), while the Executive Committee was the first choice of those in the Utilities and Resources sector (41%).

The Chief Financial Officer was named as the **most senior "risk owner"** for cyber issues by 30% of respondents, while 23% named the Chief Executive Officer. However 22% of respondents identified the Head of IT. The Chief Financial Officer featured very strongly in the Consumer Goods (54%) and the Pharmaceutical, Biotech and Healthcare sectors (53%) while the Head of IT was named by 41% of those from the Retail, Travel and Leisure sector.

The Head of IT was most commonly named as the **most senior "risk manager"** for cyber risks with 47% of responses. This was the highest answer in all sectors and received 78% of responses in the Consumer Goods sector, but only 23% in the Technology and Communications sector.

Cyber risk owners are **held to account** at the main Board, according to 40% of respondents. The Executive Committee was named by 22%, and the Audit Committee by 19%. The main Board was the first choice across all sectors except for the Real Estate and Support sector where 35% of respondents named the Audit Committee.

While only 8% of respondents believe that their Boards are "positioned for the digital age" in terms of the c**ontributions of their executive and non-executive members**, a further 38% claimed their Boards had "good skills" in this area and 48% stated that Boards had the right skills "to some extent". Only 2% identified their Boards as being barely qualified. Technology and Communications sector respondents were the most positive with 29% believing that their Boards are positioned for the digital age and a further 46% crediting them with good skills. The Pharmaceutical, Biotech and Healthcare sector respondents were the most likely to say their Boards were “barely” prepared (13%).

Leadership

Summary of findings

When asked whether their company were **doing enough to protect themselves against cyber threats**, 46% said there was more that their companies needed to do while 44% believed that their firms were "doing good things". Only 2% claimed “standards were excellent”. The Utilities and Resources sector was the most positive on this question, with 65% giving a rating of good or excellent. Those in the Consumer Goods sector tended to report there was more they needed to do (58%) as did those in the Industrial Goods and Services (53%) and Retail Travel and Leisure sectors (54%).

The majority (62%) of respondents thought Board members took the cyber risk very seriously, with 20% saying their colleagues did not take it seriously enough, and 2% not taking cyber seriously at all. Technology and Communications sector Boards were deemed the most likely to take these risks very seriously (82%) whilst those reporting from the Pharmaceutical, Biotech and Healthcare sector tended to report that their Boards did not take cyber risks seriously enough (53%) .

Just 25% of respondents have undertaken any f**orm of cyber security or information security training** in the last 12 months (ranging from 11% in the Real Estate sector to 41% in the Utilities and Resources sector) and only 21% of respondents were aware that Board members others than themselves had undertaken cyber security or information security training in the last 12 months (32% in Utilities and Resources down to just 7% in Pharmaceutical, Biotech and Healthcare)

Only 2% of respondents said their companies had signed up to the **World Economic Forum’s "Partnering for Cyber Resilience" principles.**

The majority of respondents believed that their company **invested** sufficiently in cyber defences, with 65% calling spending here "a reasonable sum". One third thought "not a great deal" was spent on cyber defences, and 2% thought spending was too low. No respondents thought too much was spent on cyber security. Respondents from the Utilities and Resources sector were the most positive about their own company’s resourcing with 86% saying their company invested a reasonable sum. The Consumer Goods sector was the most negative with 41% reporting “not a great deal” and 9% “too low”.

Leadership

How often is your strategic risk register reviewed and discussed at your main Board?

Percentage of responses
(Total number of responses: 325)

There is little real difference between the Chair and Audit Chair response patterns. While the Audit Chair responses might suggest they believe strategic risk is considered less often than main Chairs, this difference is small and far from conclusive.

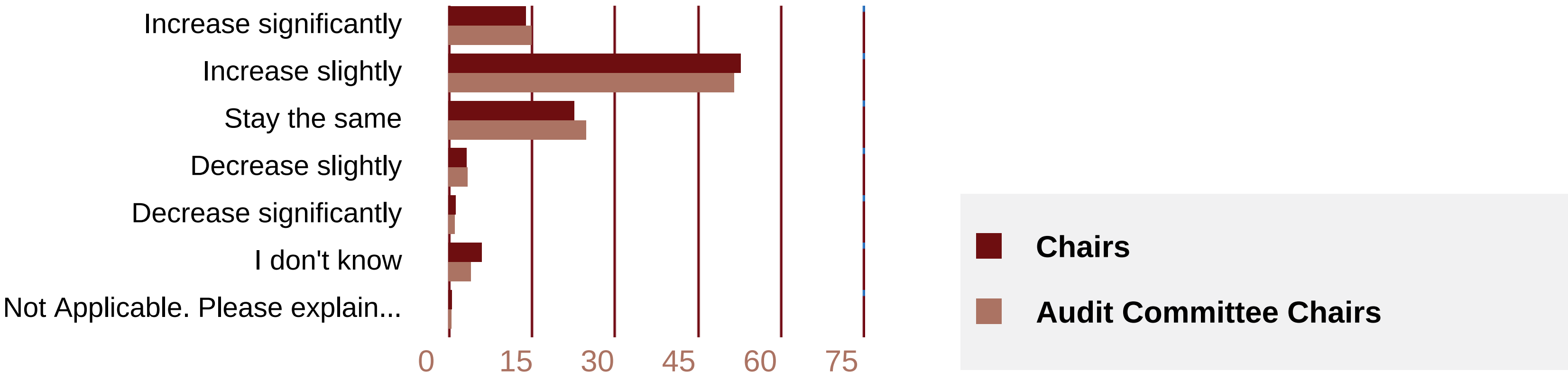
Total number of companies which provided at least one response: 217
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Leadership

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

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

The majority of companies expect the level of cyber risk to increase over the next year, although the increase predicted by over 50% of respondents is slight.



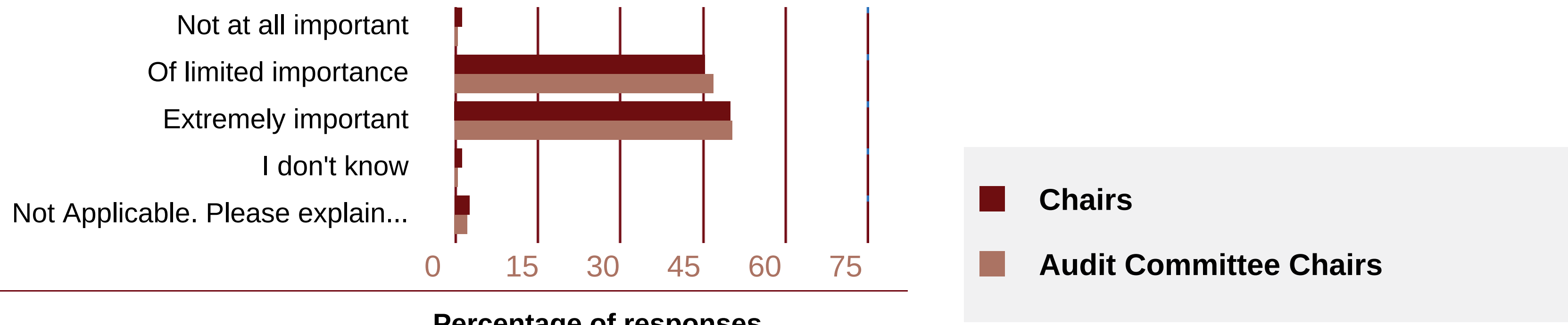
Percentage of responses
(Total number of responses: 325)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Leadership

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

Both Chairs and Audit Chairs regard cyber security risks as being of importance, with around half of each attaching extreme importance to them.

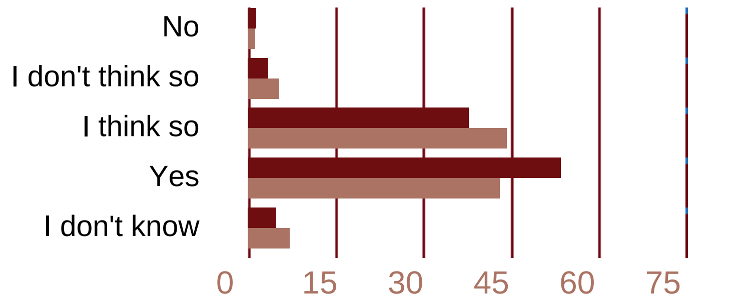


Percentage of responses
(Total number of responses: 325)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Leadership

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



Percentage of responses
(Total number of responses: 318)

Just over half of Chairs stated that their staff were comfortable reporting data or information compromises/losses, with the majority of the rest saying they thought this was the case. Audit Chairs were less certain about this, but still 87% of these said their staff were or "they thought their staff were" comfortable reporting these losses.

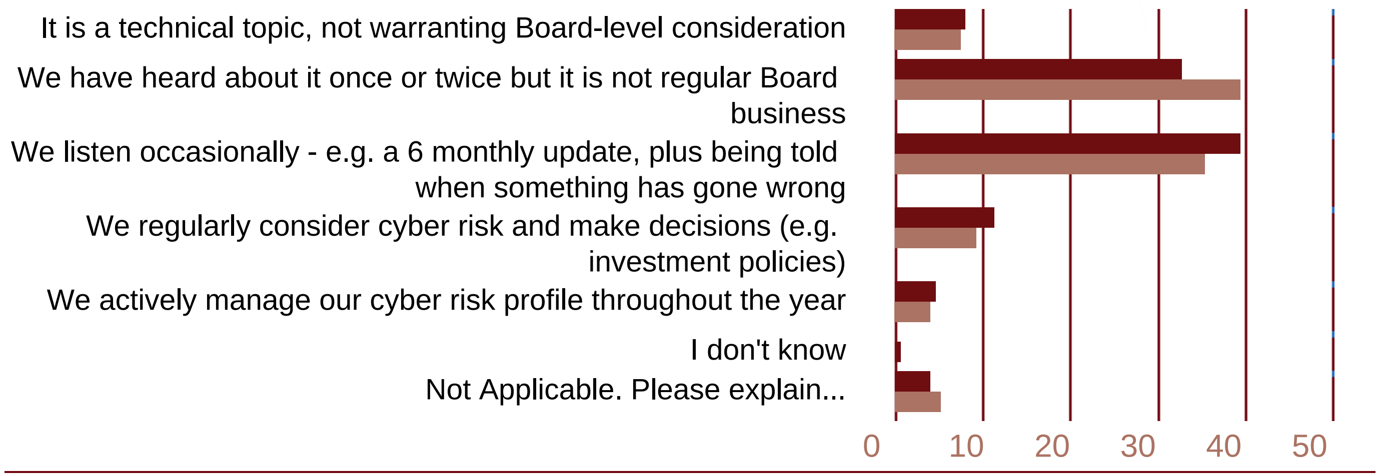
Chairs

Audit Committee Chairs

Total number of companies which provided at least one response: 214
Total number of Chair responses: 147
Total number of Audit Committee Chair responses: 171

Leadership

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



Percentage of responses
(Total number of responses: 325)

For the majority of companies, cyber risks are occasional rather than regular Board business. Only 16% of Chairs and 13% of Audit Chairs said that their Board regularly considered cyber risks or "actively managed" cyber risk profiles.

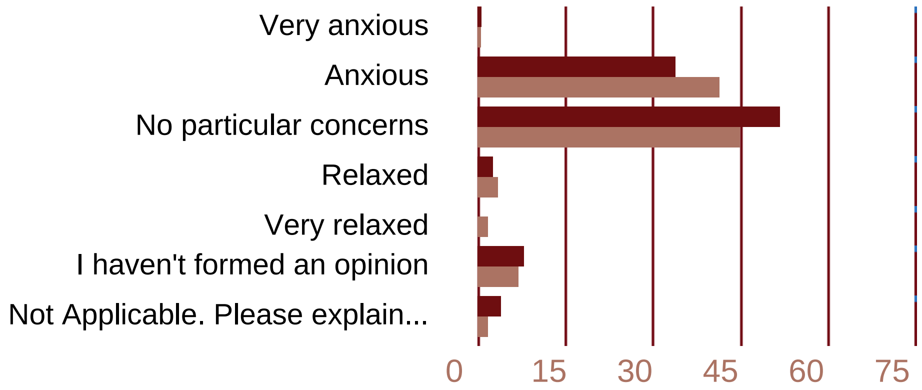
Chairs

Audit Committee Chairs

Total number of companies which provided at least one response: 217
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Leadership

In terms of the company's overall approach to cyber risk, how concerned are you personally?



Percentage of responses
(Total number of responses: 325)

The vast majority of respondents are split between having "no particular concerns" regarding cyber risk and admitting to being "anxious". Overall Audit Chairs are more likely to have stronger opinions regarding cyber risks than Chairs, with more of them reporting being anxious, but also more reporting being relaxed or very relaxed.

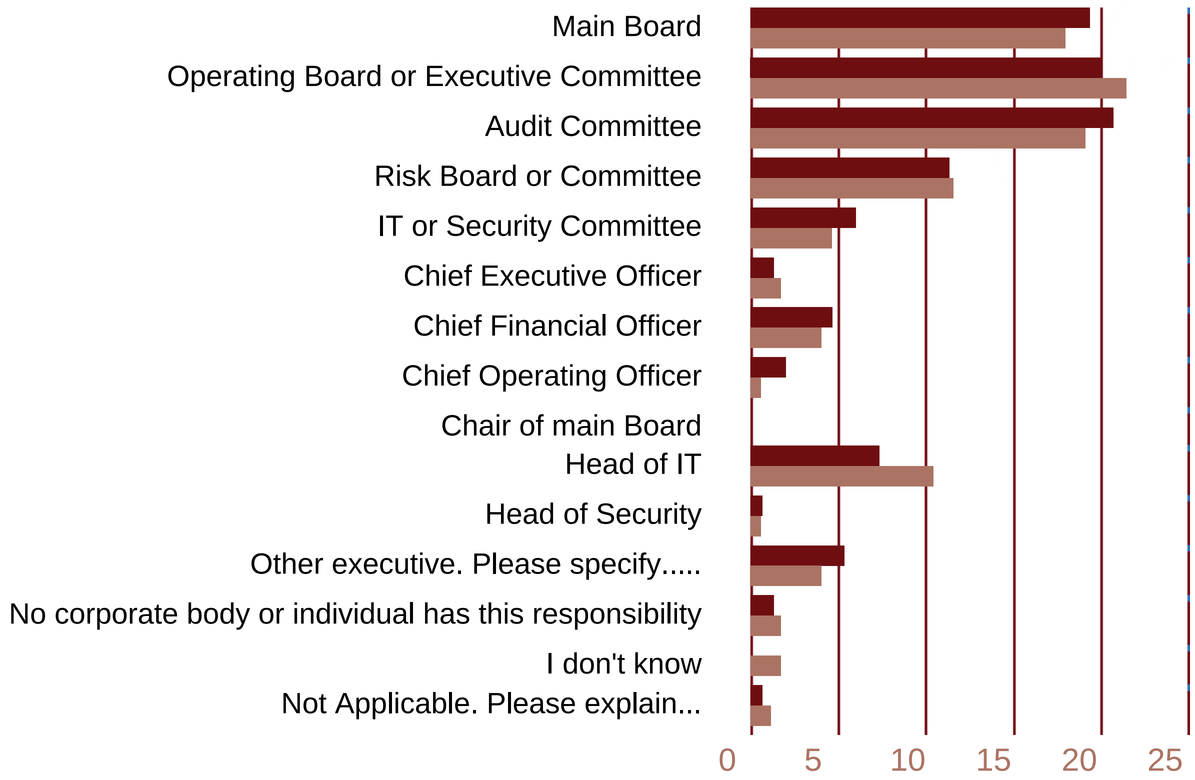
Chairs

Audit Committee Chairs

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 173

Leadership

Which corporate body or individual holds principal governance responsibility for assessing and monitoring the impact and likelihood of cyber threats to the company?



Percentage of responses
(Total number of responses: 325)

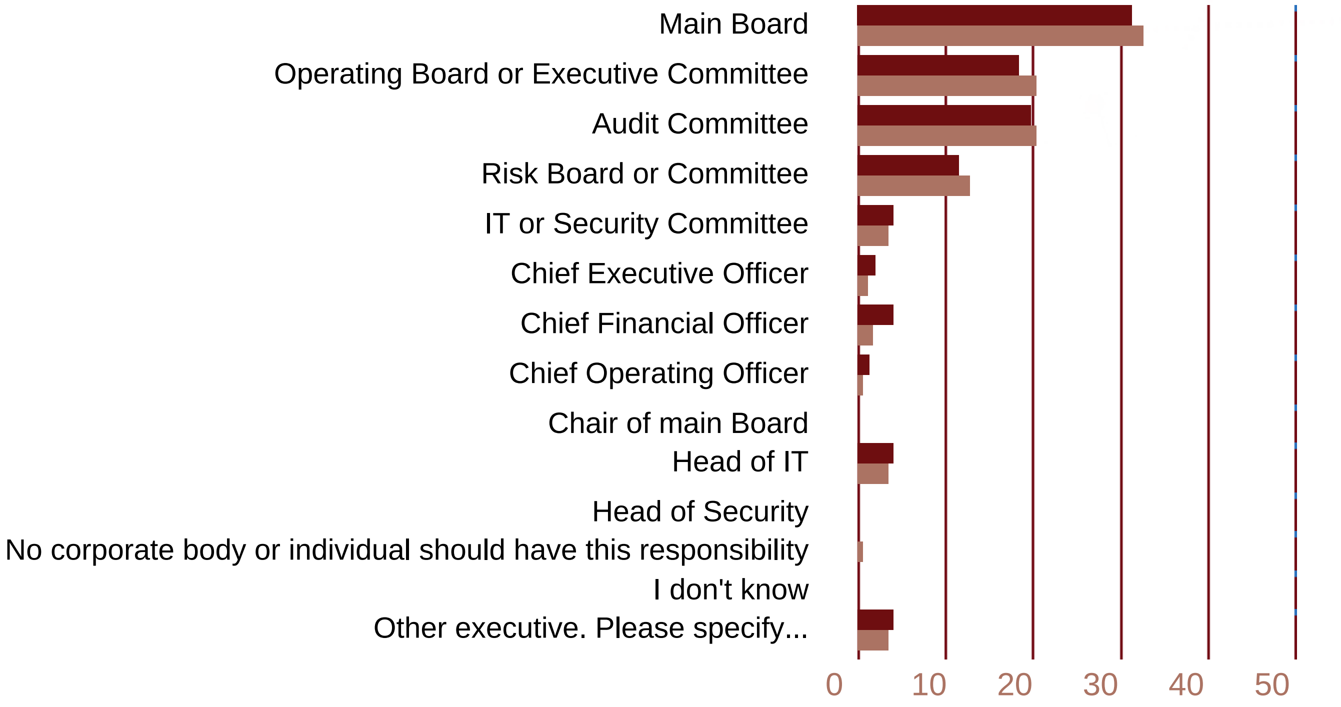
The monitoring and assessment of cyber threats fell to a number of different corporate bodies, the most common being the Executive Committee, the Audit Committee and the main Board. Two percent of Audit Chairs did not know who held responsibility for this, with just 1% of all respondents admitting that no-one held this responsibility.

- **Chairs**
- **Audit Committee Chairs**

Total number of companies which provided at least one response: 216
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Leadership

However you answered the previous question, which corporate body/individual should have that governance responsibility, in your view?



Percentage of responses
(Total number of responses: 321)

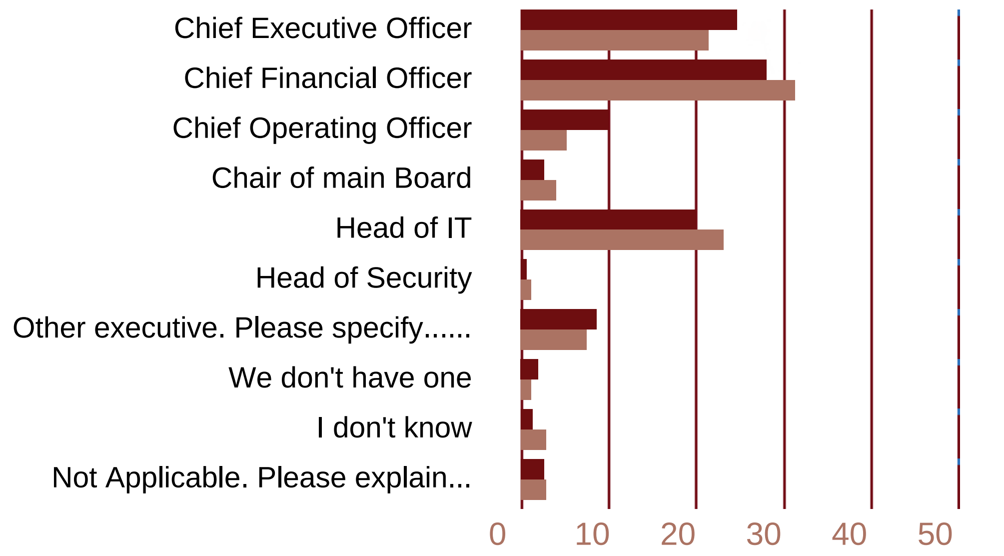
The largest differences with the previous question are that many more respondents thought it should lie with the main Board, and only a small number thought it should reside with the Head of IT.

- **Chairs**
- **Audit Committee Chairs**

Total number of companies which provided at least one response: 213
Total number of Chair responses: 148
Total number of Audit Committee Chair responses: 173

Leadership

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



Percentage of responses
(Total number of responses: 325)

Ownership of cyber risk lies with different senior roles in different companies, with the most commonly identified being the Chief Financial Officer. The Chief Executive Officer and the Head of IT were also commonly identified. It is unclear whether the hierarchical differences in risk owners (Head of IT as opposed to CEO or CFO) is indicative of the importance attached to these risks.

Chairs

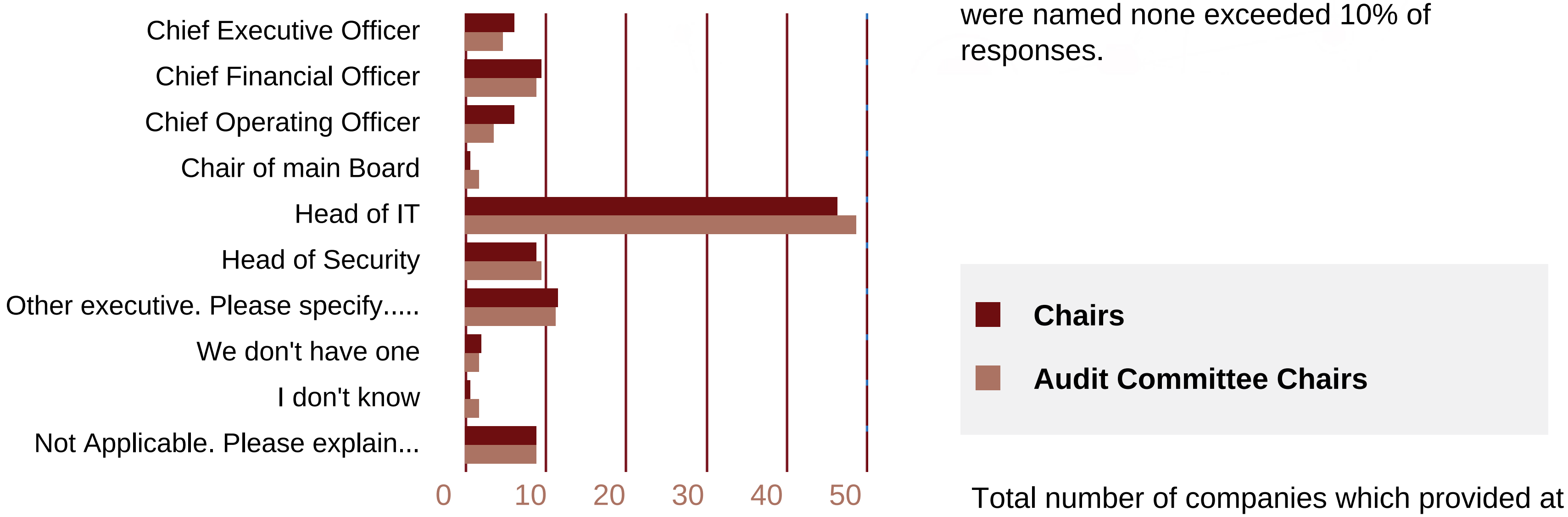
Audit Committee Chairs

Total number of companies which provided at least one response: 217
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Leadership

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

The Head of IT was selected by 47% of all respondents as being the most senior cyber risk manager. While several other posts were named none exceeded 10% of responses.



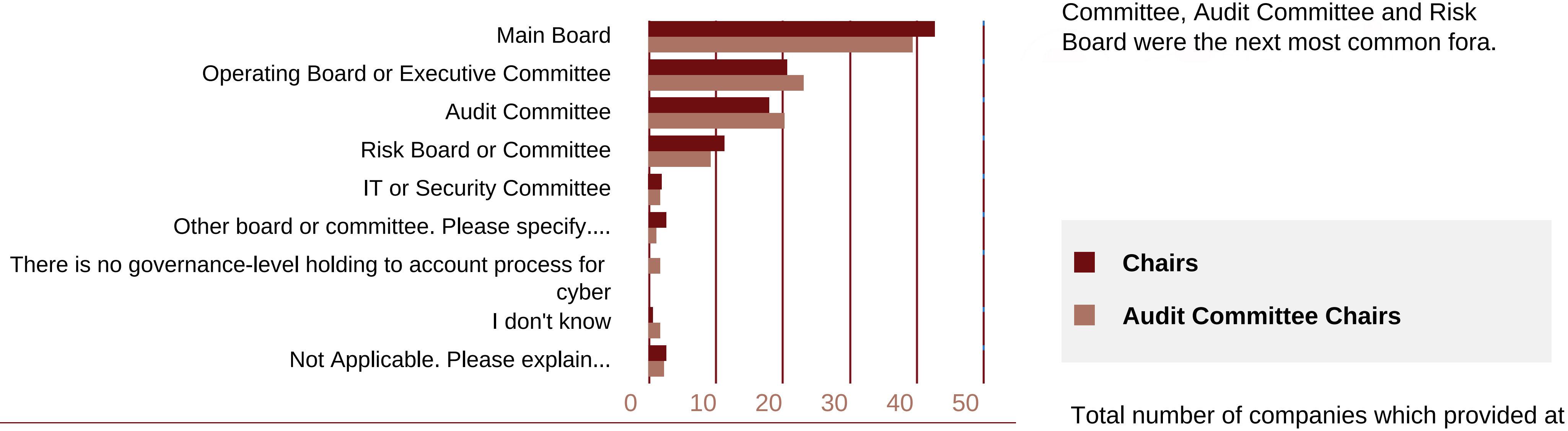
Percentage of responses
(Total number of responses: 318)

Total number of companies which provided at least one response: 215
Total number of Chair responses: 148
Total number of Audit Committee Chair responses: 170

Leadership

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

The cyber risk owner is most commonly held to account at the main Board, though only by 41% of respondents. The Executive Committee, Audit Committee and Risk Board were the next most common fora.

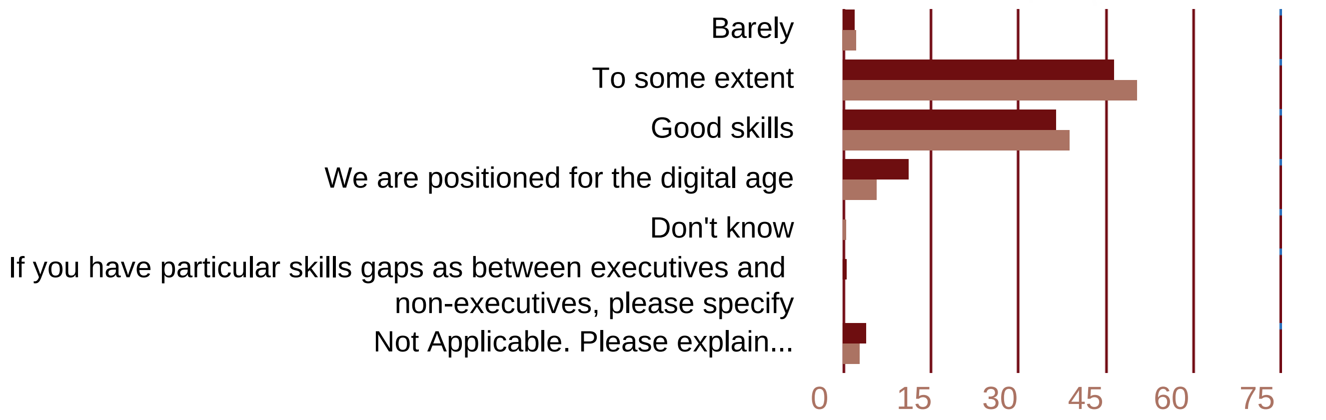


Percentage of responses
(Total number of responses: 325)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Leadership

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



Percentage of responses
(Total number of responses: 326)

Whilst only 2% deemed their Boards "barely" qualified in this respect, beyond this respondents were conservative about their Board's level of skills. Most commonly (48%) they stated their colleagues had the right skills and knowledge "to some extent", (37%) assessed their Board as having "good skills" and only (8%) were confident enough to say that they were "positioned for the digital age".

■ **Chairs**

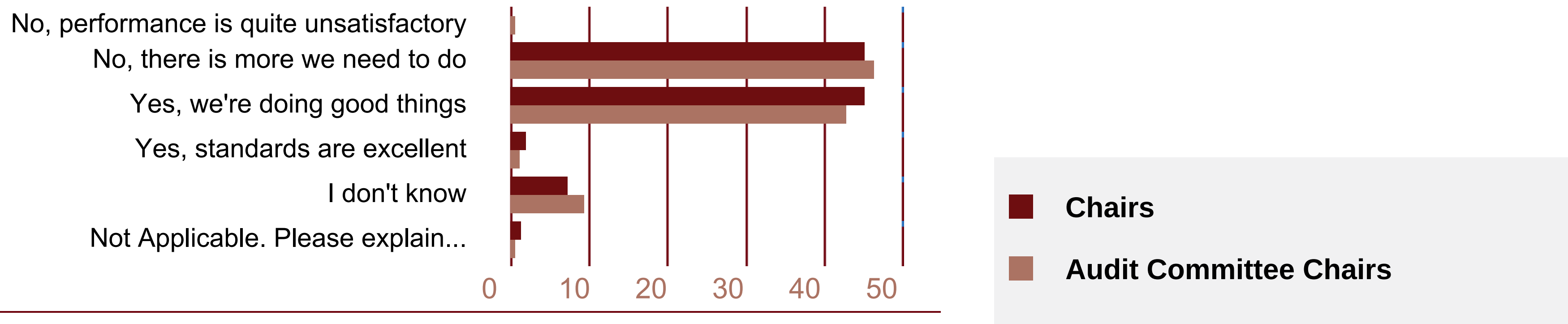
■ **Audit Committee Chairs**

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

Leadership

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

Responses to companies' overall readiness to protect themselves against cyber threats were very polarised, with almost equal numbers stating that "there was more to do" as said their company was doing good things.

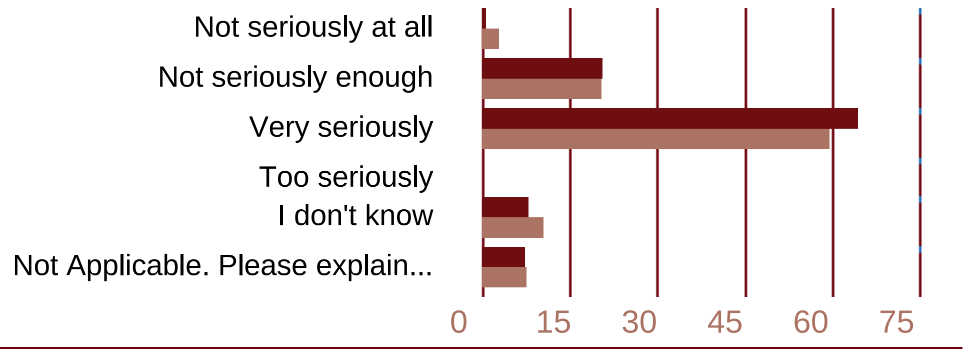


Percentage of responses
(Total number of responses: 324)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 172

Leadership

Are Board colleagues taking the cyber risk sufficiently seriously?



Percentage of responses
(Total number of responses: 325)

Reassuringly the majority of respondents believed that their Boards took cyber threats very seriously. However one fifth of respondents thought their colleagues were not taking it seriously enough, and a further 2% not seriously at all.

Chairs

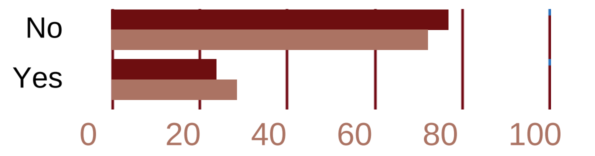
Audit Committee Chairs

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 173

Leadership

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

Three quarters of respondents had not undertaken any cyber or information security training in the last 12 months.



Percentage of responses
(Total number of responses: 325)

Chairs

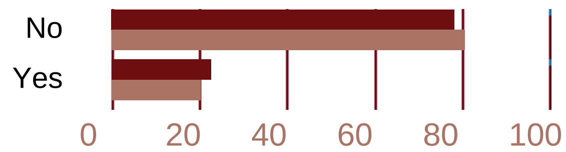
Audit Committee Chairs

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 173

Leadership

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

When asked about fellow Board members 80% of respondents said that none of their colleagues had undertaken cyber security training in the last 12 months.



Percentage of responses
(Total number of responses: 311)

Chairs

Audit Committee Chairs

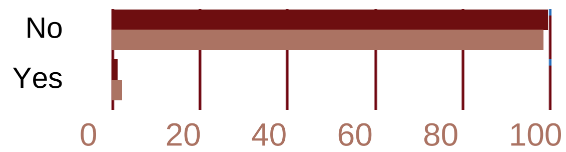
Total number of companies which provided at least one response: 212
Total number of Chair responses: 147
Total number of Audit Committee Chair responses: 164

Leadership

Have you signed up to the World Economic Forum's "Partnering for Cyber Resilience" Principles?*

***** *http://www.weforum.org/issues/partnering-cyber-resilience-pcr.***

Only 2% of respondents said that their company had signed up to the World Economic Forum's "Partnering for Cyber Resilience" Principles.



Percentage of responses
(Total number of responses: 318)

Chairs

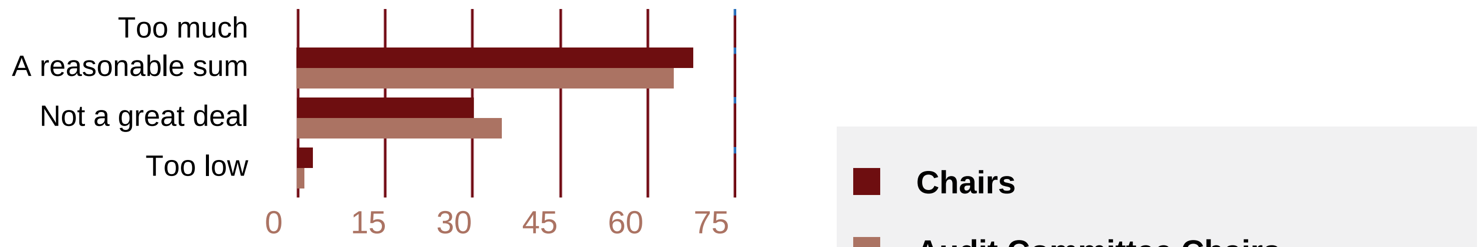
Audit Committee Chairs

Total number of companies which provided at least one response: 215
Total number of Chair responses: 149
Total number of Audit Committee Chair responses: 169

Leadership

How much does the company invest in cyber defences?

Two thirds of respondents said that their company invested "a reasonable sum" in cyber defences. The vast majority of the remainder deemed the cyber defence budget as being "not a great deal". No one regarded spending on cyber defences as being too much.



Percentage of responses
(Total number of responses: 314)

Total number of companies which provided at least one response: 212
Total number of Chair responses: 150
Total number of Audit Committee Chair responses: 164

Risk management

Summary of findings

The vast majority (91%) of respondents reported that their companies had **formal risk management systems** in place that were at least "reasonably mature", and this result was quite similar across all sectors.

Over half (56%) of respondents said that their company's **strategic risk register included a cyber risk category**. The more cyber mature Technology and Communications sector were the most likely to have a specific cyber risk category (67%), while the Pharmaceuticals, Biotechnology and Healthcare sector were the least likely (40%), while other sectors were quite close to the overall result.

Half of respondents (49%), in the context of it being **understandable to a Board audience**, said cyber risks were described in a "basic" manner within the strategic risk register with 19% answering "comprehensively" and 15% stating that these risks were "not well" described. Again the Technology and Communications sector was the most positive in this aspect, with 36% describing comprehensive description of cyber risks, and only 4% responding "not well". The Utilities and Resources sector were also strong on comprehensive risk description with 28%, while the Pharmaceutical, Biotech and Healthcare sector were the most likely to respond "not well" (27%).

When asked about the **importance of cyber risks in comparison to other risks** faced by the company, the response was - low (38%), medium (32%) then top (25%). The Real Estate and Support Services sector were the most likely to class cyber risks as low (69%), followed by the Consumer Goods sector (54%), which also was the least likely to consider these risk as being of top importance (13%). In common with trends from the previous questions the Technology and Communications sector attached the highest importance to cyber risks with 36% replying "top". The Industrial Goods and Services sector was the most polarised with the most similar proportion of answers for low (37%) or top (31%).

Only 17% of respondents felt that their Boards had **clearly set and understood their appetite for cyber risk**, with a further 35% describing a loosely set appetite and 43% not at all. The Financial Services sector were the most likely to have clearly set and understood cyber risk appetites (28%), whilst those in the Consumer Goods sector were the least likely to have any (58%).

Some 41% of respondents said their Boards had just basic understanding of where the company's **key information and data assets are shared with third parties**, such as suppliers, customers, advisors or outsourcing partners.

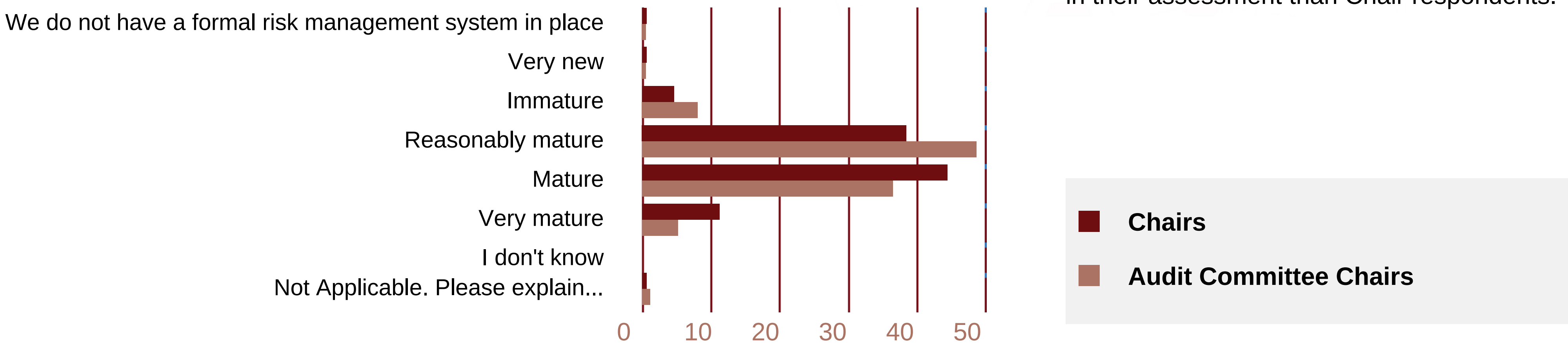
A further 41% of respondents rated this understanding as "marginally acceptable" or "poor". Only 12% thought their Boards had a very clear understanding of their third party sharing arrangements. Respondents from the Financial Services sector were the most positive about their Board's understanding with 29% reporting a very clear understanding and only 23% a marginal or poor understanding. The Technology and Communications sector was also significantly more positive. No respondents from the Pharmaceuticals, Biotech and Health Care sector or Consumer Goods sector thought their Boards had a clear understanding of third party sharing arrangements, rating their Boards as having a marginal or poor understanding in 66% and 39% of cases respectively.

Just 31% of respondents were able to confirm that their company had contract **clauses with their suppliers** and other third parties regarding cyber risk, while 14% had other arrangements such as pre-contract due diligence, third party audit and third party self assessments. The Technology and Communications sector was the most likely to employ some sort of formal arrangement with 63% of responses (41% for contract clauses and 22% other methods). The Industrial Goods and Services sector was the least likely with 31% (29% for contract clauses).

Risk management

How mature, and developed, is your formal risk management system?

The majority of respondents rank their risk management systems as being reasonably mature or very mature, with Audit Chair respondents being slightly more pessimistic in their assessment than Chair respondents.

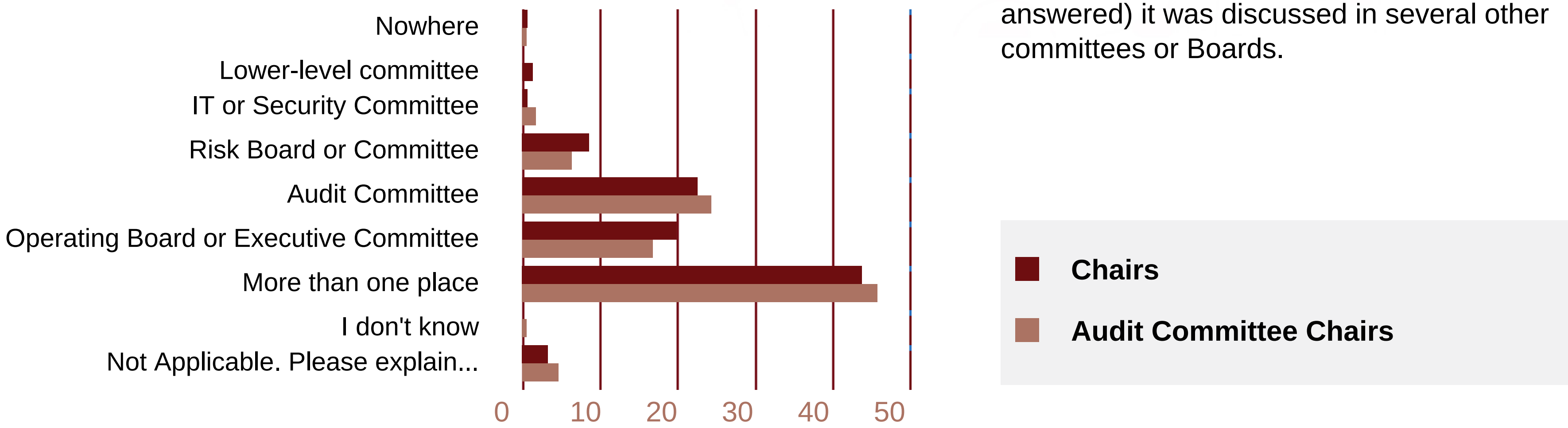


Percentage of responses
(Total number of responses: 326)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

Risk management

Where else is the strategic risk register reviewed/discussed?



Percentage of responses
(Total number of responses: 326)

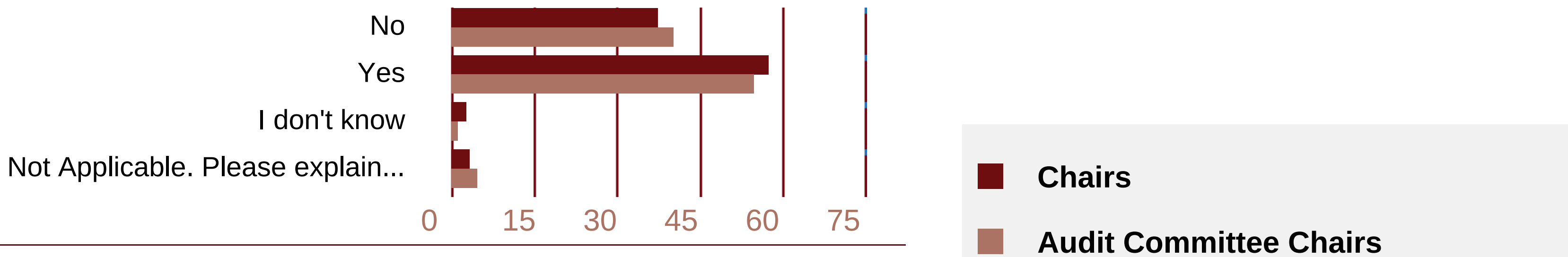
The majority of companies discussed the strategic risk register in other governance groups in addition to the main Board. In 43-45% of cases (depending which role answered) it was discussed in several other committees or Boards.

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 174

Risk management

Does the company's strategic risk register include a 'cyber risk' category?

Over half of respondents companies have a specific 'cyber risk' category within their strategic risk register.



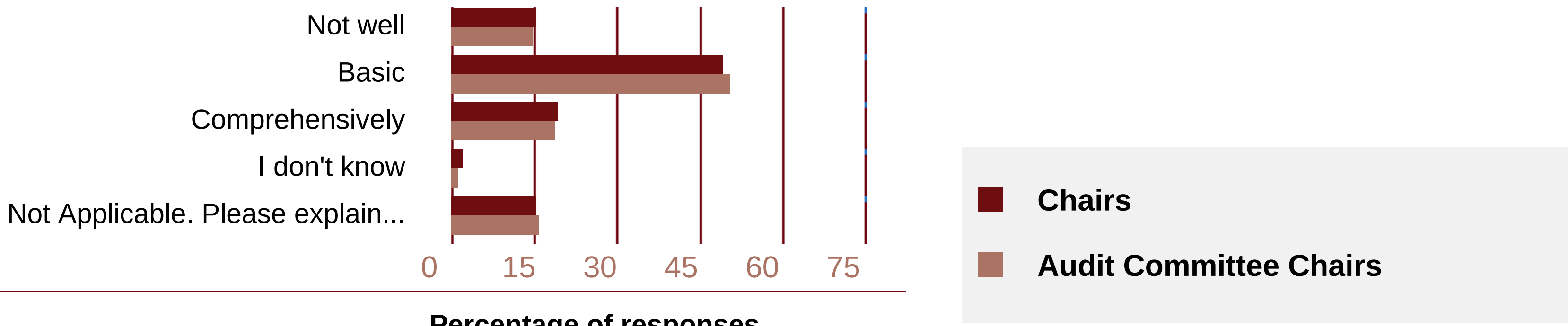
Percentage of responses (Total number of responses: 324)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 173

Risk management

In the strategic risk register, how well described (i.e. understandable to a general Board audience) are cyber risks, and the potential consequences for the business?

In the opinion of most of our respondents the description of cyber risks within the strategic risks register is basic or lower.



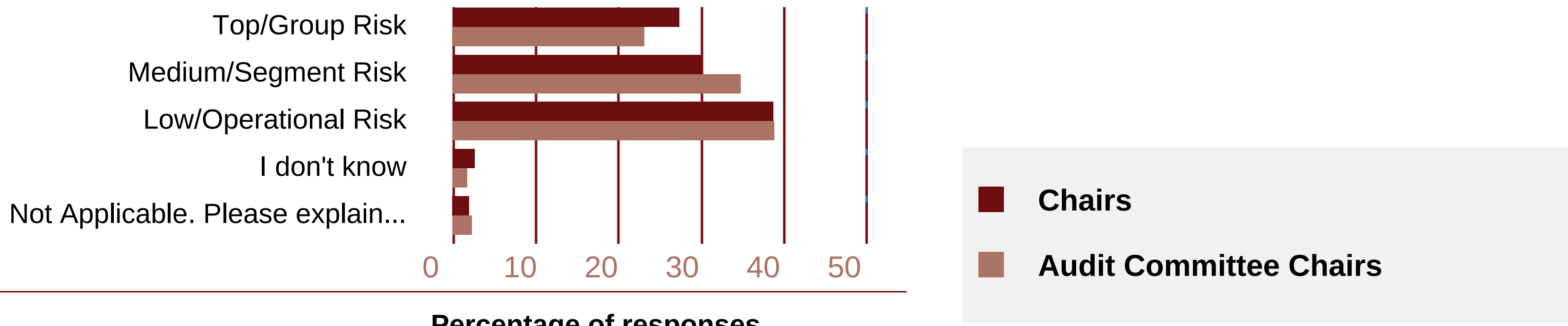
Percentage of responses
(Total number of responses: 324)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 172

Risk management

How significant or important is cyber risk, when compared with all other strategic risks the company faces?

In comparison to other risks, respondents ranked cyber risk as being of low (38%) or medium importance (32%). However 25% rated cyber security issues as having top level importance.



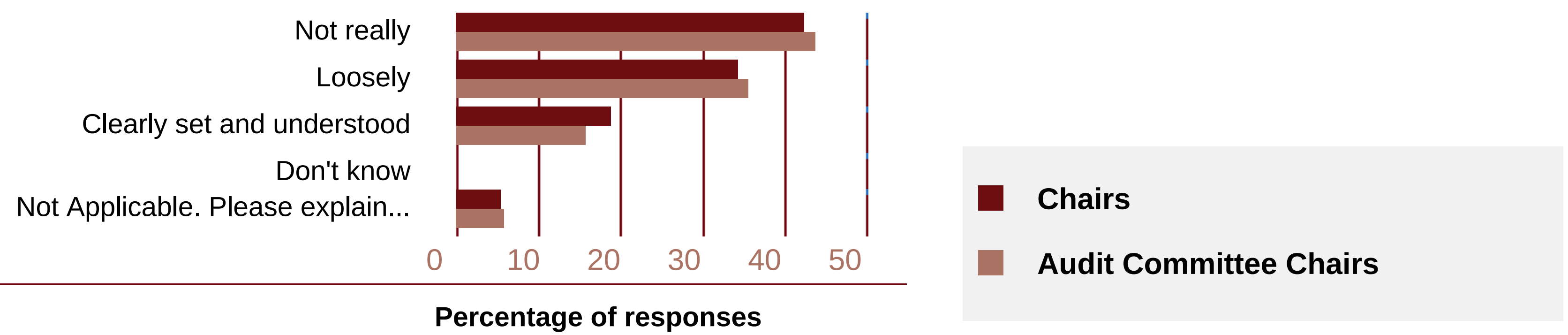
Percentage of responses (Total number of responses: 325)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

Risk management

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

Most companies have not, or have only loosely set their appetite for cyber risk. Only 17% of all respondents claimed they have clearly set and understood their tolerances for such risks.



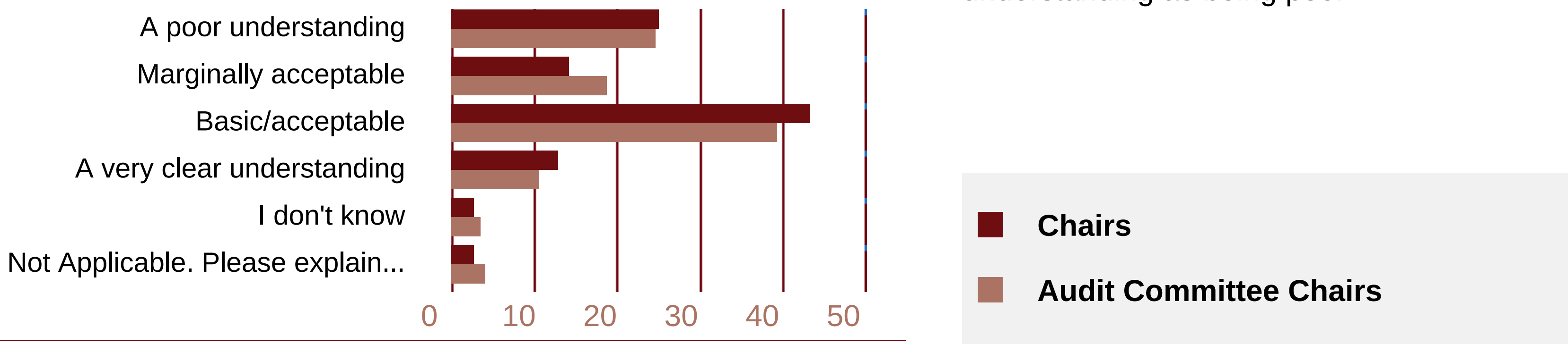
Percentage of responses
(Total number of responses: 323)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 150
Total number of Audit Committee Chair responses: 173

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)?

Around 41% of respondents believed that their Board had a basic or acceptable understanding of their companies information and data sharing activities. A quarter of respondents rated this understanding as being poor.

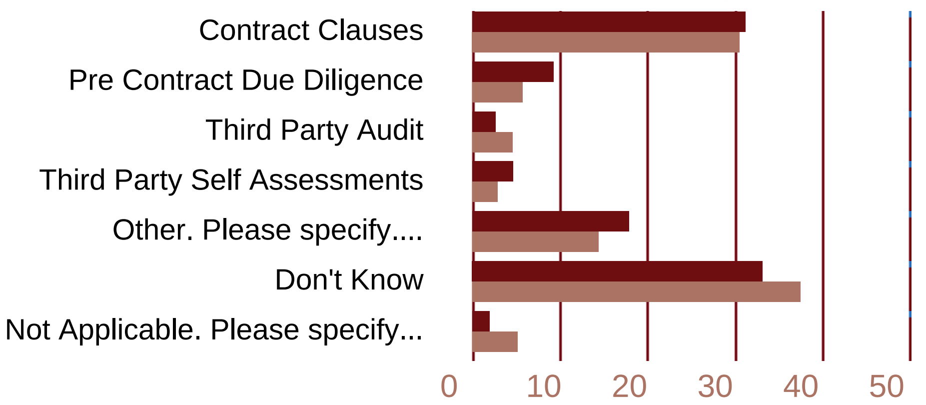


Percentage of responses
(Total number of responses: 321)

Total number of companies which provided at least one response: 215
Total number of Chair responses: 149
Total number of Audit Committee Chair responses: 172

Risk management

How has your company addressed cyber risks with its suppliers and other relevant third parties?



Percentage of responses
(Total number of responses: 327)

Neither Chairs nor Audit Chairs had a strong understanding of how their companies had addressed cyber risks with their suppliers and other third parties, with the most common answer for both being "don't know". However 31% of all respondents were able to confirm the use of contract clauses in this regard.

Chairs

Audit Committee Chairs

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 175

Awareness of help and support

Summary of findings

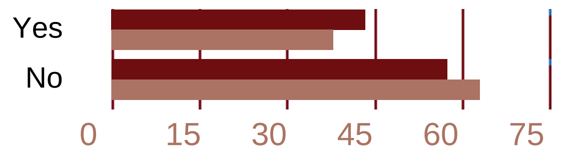
Only 40% of respondents to the survey were aware of any organisational standards, guidance or certifications that their companies followed with regards to cyber security. Only 21% of respondents from the Consumer Goods sector knew of these while respondents from Technology and Communications sector (64%) and the Utilities and Resources sector (62%) were the most aware.

The Government estimates that up to 80% of cyber threats could be thwarted by the basic security measures detailed in the **Governments "10 Steps" to Cyber Security guidance**, and 39% of survey respondents knew that their companies had assessed themselves against this guidance in some manner. Some 36% of participants said that their companies had not done so. In the Technology and Communications Sector 61% of respondents were aware of some assessment against these steps while in the Real Estate and Support Services and the Retail, Travel and Leisure sectors this figure was 31%.

Awareness of help and support

Are you aware of any organisational standards, guidance or certifications that your company follows/holds for cyber security?

The majority of respondents were not aware of the cyber security standards, guidelines or certifications their companies follow or hold.



Percentage of responses (Total number of responses: 324)

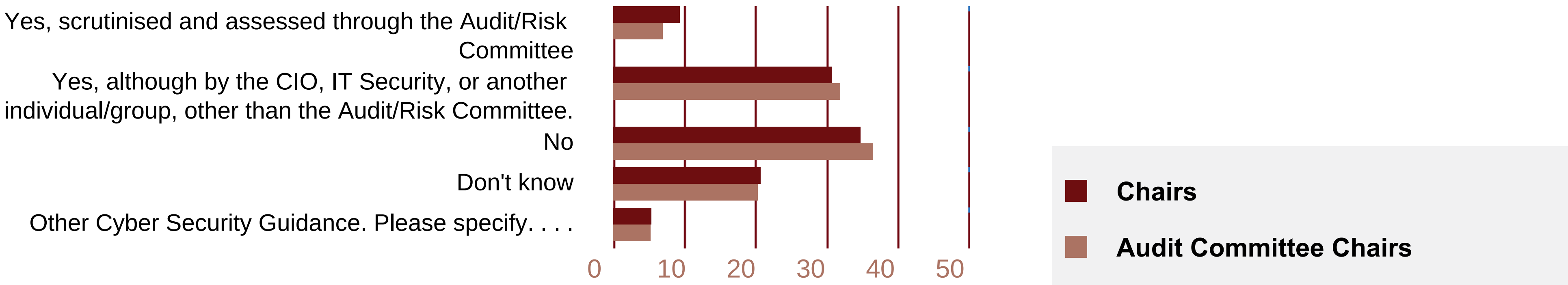
Total number of companies which provided at least one response: 216
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 173

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" to Cyber Security Guidance

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

39% of respondents stated that their company had assessed themselves against the Government's "10 Steps" guidance. However, just 8% of these had done so through their company's Audit or Risk Committee.



Percentage of responses
(Total number of responses: 325)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 174

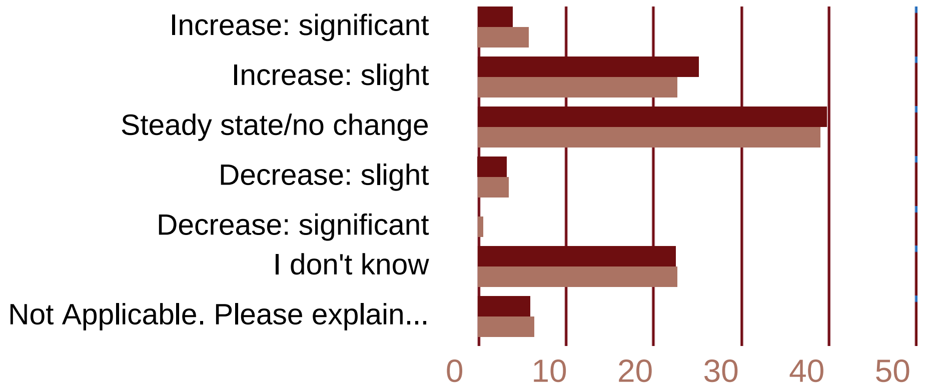
Many respondents were totally unaware of the **level of cyber incidents experienced by their company** in the last year, while 39% thought it was roughly the same as the previous year, with 24% reporting a slight increase, and only 5% noting a significant increase on the previous year. The Technology and Communications sector was the most likely to report a slight or significant increase in the level of cyber compromises (50%).

Many respondents felt unable to rate their company's **response to the cyber threats** faced in the last year; however 29% rated their company as having performed "quite well" and a further 14% "excellent". No respondents rated their company's performance as being poor while the Utilities and Resources sector was the most likely to be rated excellent (31%). The Retail, Travel and Leisure sector was the most positive overall with 64% rating their company as having performed "quite well" or to an "excellent standard".

Responses to cyber threats were considered across a number of internal groups with the most commonly named being the Executive Board, the main Board or the Audit Committee, with no organisational body having a majority. Even within the different sectors there was no **clear policy as to where cyber security compromises should be considered.**

Cyber incidents

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



Percentage of responses
(Total number of responses: 325)

While over a fifth of respondents did not know the answer to this question, 39% believed the level of cyber incidents had been steady over the last year. Of those stating there had been a change, far more said it had increased either slightly or significantly than those claiming a fall.

Chairs

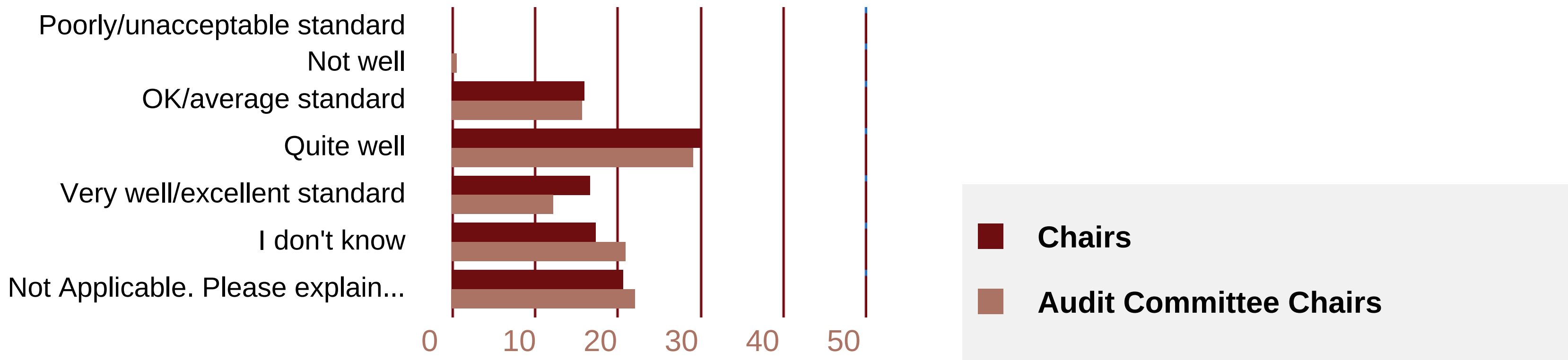
Audit Committee Chairs

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 173

Cyber incidents

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

Many respondents did not know the answer to this question, and did not have any knowledge of the specific actions taken. However, almost all the remaining responses were positive.

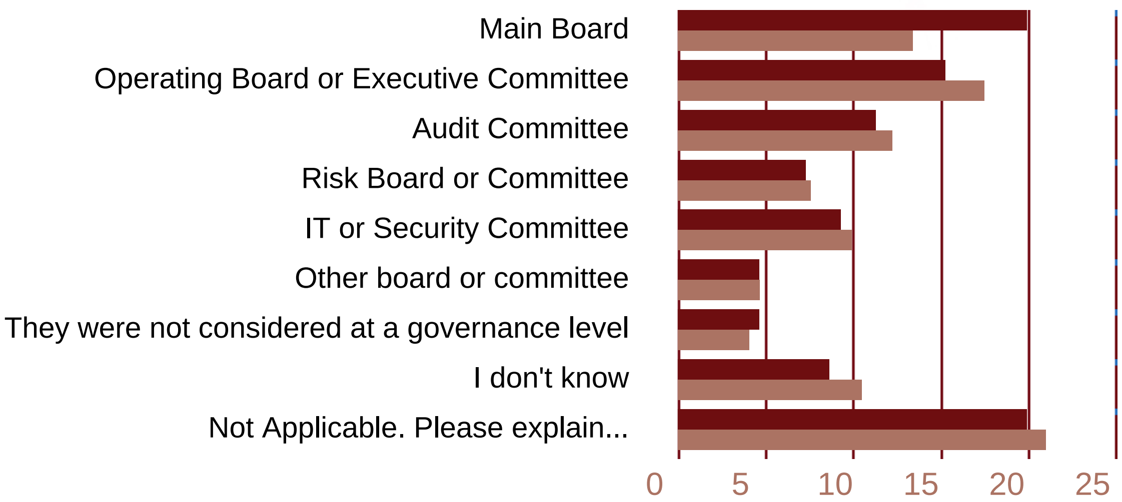


Percentage of responses
(Total number of responses: 324)

Total number of companies which provided at least one response: 217
Total number of Chair responses: 151
Total number of Audit Committee Chair responses: 173

Cyber incidents

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



Percentage of responses
(Total number of responses: 325)

The most common answers were the main Board, the Executive Committee and the Audit Committee. However, responses here were much more evenly spread than previous questions on cyber security risk governance.

■ **Chairs**

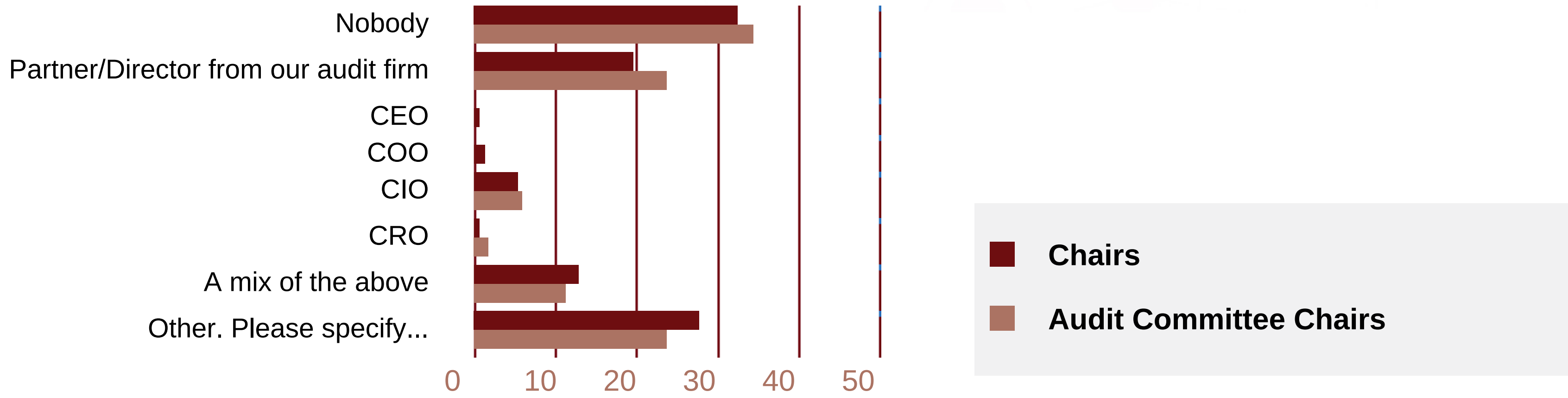
■ **Audit Committee Chairs**

Total number of companies which provided at least one response: 217
Total number of Chair responses: 152
Total number of Audit Committee Chair responses: 173

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?

Many respondents had sought the assistance of colleagues in completing this questionnaire with only a third stating they completed the survey alone.



Percentage of responses
(Total number of responses: 319)

Total number of companies which provided at least one response: 216
Total number of Chair responses: 149
Total number of Audit Committee Chair responses: 170

Methodology

Summary of findings

The Tracker ran from 9 September to 11 October 2013. The survey was sent out to all FTSE 350 companies and achieved a response rate of 62% (217 companies). This report is a collation of the combined anonymous responses of the Chairs and Audit Chairs of those companies.

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

Pharma, Biotech and Health Care
Health Care Equipment and Services
Pharmaceuticals and Biotech

Retail, Travel and Leisure
Retailers
Travel and Leisure

Real Estate and Support Services
Real Estate
Support Services

Technology and Communications
Media
Tech Hardware
Tech Software and Services
Telecommunications

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

Annex B - HMG guidance and support

Introduction

The National Cyber Security Programme (NCSP) is managed and co-ordinated on behalf of Government by the Office of Cyber Security and Information Assurance in the Cabinet Office. Working under the auspices of the NCSP, individual government departments and agencies have developed, supplied or recommended the support and guidance outlined below.

This guidance should assist your organisation as it seeks to implement good cyber governance and risk management, identify and mitigate vulnerability and react to cyber incidents.

a) Key Government Cyber Security Guidance:

• Ten Steps to Cyber Security:
www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

• Cyber Security: What small businesses (including supply chain) need to know:
www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know

b) CPNI's Cyber Risk Management Advice and Cyber Security Guidance

The Centre for the Protection of National Infrastructure (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 at: www.cpni.gov.uk, for example:

- **Strategic and technical:** 20 critical security controls for effective cyber defence
- **Technology-specific advice:** examples include mobile devices, SCADA security and cloud computing
- **Personnel security advice:** security culture and awareness; employee risk management and risk assessment guidance
- **Threat-based:** examples include distributed denial of service, spear phishing, insider misuse of IT; online reconnaissance.

Annex B - HMG guidance and support

c) CPNI's Cyber Risk Advisory Service
The Cyber Risk Advisory Service delivers advice to senior executives and board members of the UK's most economically important companies and academic institutions, to inform their understanding of the impact of cyber threats, and the effect on the long-term performance and competitiveness of the organisation.

The in-depth support provided assists executives in reviewing their corporate risk management strategy, helping them to interpret the cyber threat and determine the organisation's exposure (risk). This service is only available to organisations which meet specific eligibility requirements. For more information, please email enquiries@cpni.gsi.gov.uk

d) CESG's Industry Schemes
CESG, the information security arm of GCHQ, works closely with the cyber security industry to enable industry to provide certified cyber security services to government and to industry. These services are provided by a variety of companies including specialist SMEs, audit houses, major consultancies, and multinational companies. Services include:

- Risk management consultancy through the CESG Listed Advisor Scheme (CLAS): www.cesg.gov.uk/servicecatalogue/CLAS/Pages/CLAS.aspx

- Penetration testing of networks and systems to assess their vulnerability to an attacker through the CHECK scheme: www.cesg.gov.uk/servicecatalogue/CHECK/Pages/index.aspx - and the industry body's equivalent run by the Council of Registered Ethical Security Testers, CREST: www.crest-approved.org

- Cyber Incident Response 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. See: www.cesg.gov.uk/servicecatalogue/cir/Pages/Cyber-Incident-Response.aspx

Annex B - HMG guidance and support

CESG is now focussing on standards for monitoring capabilities to enable industry and government to purchase cyber monitoring products and services to assist in the detection of cyber incidents. www.cesg.gov.uk

e) 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 (both large and SME) partners can exchange information on threats and vulnerabilities in real time. www.cisp.org.uk

f) National Cyber Crime Unit (NCCU)
The National Cyber Crime Unit within the new National Crime Agency (NCA) is the UK's law enforcement lead on the most serious, organised and complex cyber crime. Responsibilities previously undertaken by the Metropolitan Police Service's Police Central e-Crime Unit have now been transferred into the NCCU, following the launch of the National Crime Agency on 7 October 2013. The NCA will work with Action Fraud, National Fraud Intelligence Bureau, CISP and others to ensure that law enforcement engagement with industry is clear, dynamic and reciprocal. The NCA is not a crime reporting agency, so any of crime will need to be reported to Action Fraud or to a police force. www.nationalcrimeagency.gov.uk

g) 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

Other useful websites:
The World Economic Forum's Partnering for Cyber Resilience is a global, multi-industry, multi-stakeholder initiative to improve cyber resilience, raise business standards and to contribute to a safer and stronger connected society. The initiative asks leaders to sign a set of Principles, and offers organisations tools to evaluate and improve their capabilities.
www.weforum.org/issues/partnering-cyber-resilience-pcr

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

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

BIS/13/1293