HM Government

FTSE 350 Cyber Governance Health Check 2018

March 2019

This document is available in alternative formats on request. Please call +44 (0)207 211 2210 or email enquiries@culture.gov.uk

Any enquiries regarding this publication should be sent to us at cybersecurity@culture.gov.uk

This publication is available for download at www.official-documents.gov.uk.

Table of Contents

Foreword

Technology is a crucial and growing part of modern life and underpins our efforts in the UK to build a world-leading digital economy. We want the UK to continue being at the forefront of digital innovation and security. Protecting and strengthening the UK's digital economy is thus at the heart of what we're doing in Government.

We are still working through the implications of a more connected society and the necessary adjustments that we need to make. As our life and work moves increasingly online, we are exposed to a wider range of potential threats. This is why we have a *National Cyber Security Strategy* setting out a five year plan to protect the nation in cyber space and create a UK fit for the digital age.

The annual FTSE 350 Cyber Governance Health Check has been an important part of our cyber security strategy since 2013. The FTSE 350 - the UK's leading 350 companies - have an important role to play as leaders in the UK economy. Actions taken by the FTSE 350 companies have ripple effects throughout the wider economy. Given this influential role, the maturity of their cyber risk management is an indicator of the health of the broader economy. Moreover, their cyber governance is in many ways a reflection of how companies in the FTSE 350 companies' extensive supply chains are performing. Accordingly, the annual Health Check is a barometer of how corporate Britain is responding to the ongoing challenge of cyber threats.

I am pleased to see the ongoing positive progress on cyber security made by companies which is highlighted throughout this report. It is clear firms are stepping up to the challenge and it is good to see how Government action, such as the introduction of the new Data Protection Act last year, has incentivised a positive response from businesses as a driver for improved security systems.

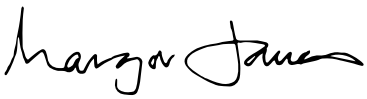
However, the pace and scale of actions taken is not yet sufficient. Whilst 72% of companies now consider cyber a high or very high risk, less than half, only 46%, have a dedicated cyber security budget. Worldwide, we continue to see harmful cyber attacks and significant data breaches at major, household name companies. Many large firms are now investing heavily in cyber security, but attacks over the past year continue to demonstrate the importance of comprehensive cyber risk management strategies. Some common themes continue to be apparent in some of the largest cyber attacks, such as the failure to have a comprehensive understanding of business assets across multiple locations, or not understanding the importance of the supply chain to the overall security of the business.

These are critical issues that need to be supported across an organisation - both by its professionals and its organisational leadership. We therefore need a growing and diverse workforce to fill the gaps that are apparent in the cyber security profession. The Government recognises this skills gap and is supporting industry through the Cyber Skills Immediate Impact Fund, which provides funding and support to boost the number and diversity of those entering the profession.

Senior leaders and boards have a significant role to play in resolving this issue and managing the cyber security risks an organisation faces - they cannot be solved by the IT department alone. Having a better understanding of the potential impact of cyber attacks will equip boards and business owners to recruit the right staff and to take appropriate control of managing their cyber risks.The 2018 Health Check provides us with a compelling case for continued and enhanced action to embed cyber security risk management by company boards and executives.

I want to express my thanks to the board members and staff in the FTSE 350 companies who have contributed towards this year's report. I would also like to thank our partners in the audit firms - PwC, KPMG, EY and Deloitte - for all the help and support they have delivered in the production of this year's Health Check.

I hope this report, along with the wider range of guidance and support offered by the Government, helps in the continued growth and security of our digital economy.

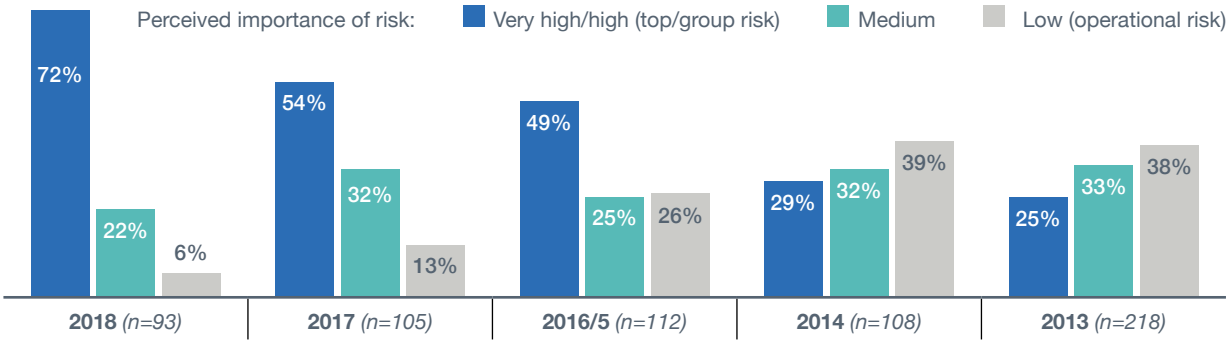


Margot James
Minister for Digital and the Creative Industries

Highlights

Cyber risk perception over time

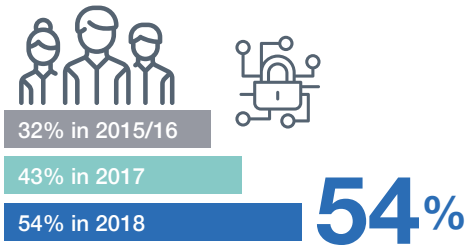
Cyber threats are increasingly seen as high risk in comparison to other risks that businesses face.



Board understanding of organisational assets

An increasing number of boards understand the critical assets at risk, though almost half still do not.

Just over half (54%) of businesses in 2018 rated the board's understanding of critical information, data assets and systems as comprehensive. This compares to 43% of boards in 2017 and 32% in 2015/16 stating they had a clear understanding.[1]



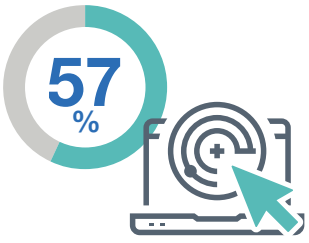
Cyber security strategy

Most businesses have a cyber security strategy, though many have no dedicated budget.

Almost all businesses (96%) have a cyber security strategy. However, only 46% have a dedicated budget for their cyber security strategy.

Incident response plan and testing of it

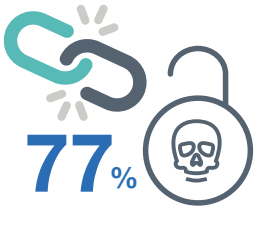
Most businesses have incident response plans, but many are not testing these on a regular basis.



95% of FTSE 350 businesses have an incident response plan, however only 57% test their crisis incident response plans on a regular basis.

Supply chain risks recognition

A majority of boards do not recognise supply chain risks beyond the first tier.



77% of FTSE 350 businesses do not recognise the risks associated with businesses in the supply chain with whom they have no direct contact.

1 The increase in board understanding from 2017 to 2018 is statistically significant at an 80% confidence level. The increase from previous years (2015/16, 2014 and 2013) to 2018 is statistically significant at a confidence level of 99%.

Executive summary

The UK economy faces increasing and evolving cyber threats, so it is important for all UK businesses to be prepared for cyber incidents and manage cyber risks effectively.

The FTSE 350 Cyber Governance Health Check is a means of assessing the extent to which boards and audit committees of FTSE 350 businesses understand and oversee risk management measures that address cyber security threats to their businesses.

The 2018 Health Check discussed in this report is the fifth iteration since 2013. It has found that boards are continuing to make progress in acknowledging, understanding and responding to cyber threats, with a positive trend towards improved governance throughout the areas covered by the Health Check. However, there remains room for improvement, particularly in assessing and dealing with risks in the supply chain, and testing incident response plans to ensure they are and continue to be fit for purpose.

The main findings from the 2018 Health Check are as follows:

Board understanding

1. A greater proportion of boards than ever before perceive the risk of cyber threats as high or very high.

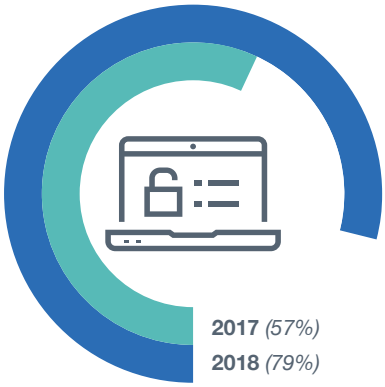
Acknowledgement of cyber threats has increased substantially in 2018, and an increasing majority of businesses now recognise cyber security as a strategic risk management issue. Almost three quarters (72%) of respondents to the latest Health Check report that the board considers the risk of cyber threats to be high or very high in comparison to all risks that the business faces. This compares to just 54% of boards in 2017.

2. Board level understanding of business-critical information, data assets and systems also continues to increase, though not as quickly.

Understanding of business-critical information, data assets and systems is also improving at board level; however, this is not increasing at the same rate as board acknowledgement of cyber threats. Just over half (54%) of respondents to the 2018 Health Check rated board understanding of business-critical assets as fairly comprehensive or comprehensive, compared to 43% of businesses rating board understanding of assets as ***clear*** in 2017. Whilst the increase is encouraging, only 12% of businesses rate their understanding 5 out of 5, indicating the majority of businesses feel that board understanding could be improved.

3. Understanding of the potential impact of loss or disruption associated with cyber threats also continues to increase, though few boards have a comprehensive understanding.

Mirroring the increase in the number of boards rating cyber threats as high or very high risk, boards have developed a more detailed understanding of the potential impact of cyber threats on their business.



Just over three quarters (79%) of respondents rate board understanding of the impact from loss or disruption as comprehensive in 2018, compared with just over half (57%) of businesses rating understanding as clear in 2017.

However, only a minority of businesses (16%) report that their board has a comprehensive understanding of the impact of loss or disruption associated with cyber threats on the types of impact tested in the 2018 Health Check, i.e. customers, share price *and* reputation. This indicates that most businesses feel that board understanding of impacts could be improved.

4. Boards with a more comprehensive understanding of cyber threats and their potential impacts have more extensive cyber governance practices.

Increased implementation of cyber governance measures correlates with the board's understanding of cyber threats and the potential impacts of associated loss or disruption. In general, the more comprehensive the board's understanding, the more extensive their cyber governance practices. Firm conclusions cannot be drawn about causality (more extensive governance may have improved the board's understanding, rather than improvements in understanding leading to more extensive governance); however, it is notable that governance practices are more strongly associated with board understanding than they are with the board's assessment of the risk of cyber threats.

Board engagement

5. Most boards receive information that is up to date and robust, though fewer consider the information they receive to be comprehensive.

71% **Information is up to date**
– 71% rating it 4 or 5 out of 5

71% **Information is robust**
– 71% rating it 4 or 5 out of 5

53% **Information is comprehensive**
– 53% rating it 4 or 5 out of 5

Boards need to make decisions relating to cyber security based on the information that is provided to them. It is important that the information is presented in a way that aligns with and underpins the wider business objectives in order for board members with a non-technical background to understand it. The findings from this 2018 Health Check suggest that information provided to boards in many cases is insufficient.

6. Where businesses have a Chief Information Security Officer (CISO) reporting directly to the board, they are more likely to rate the information they receive as comprehensive.

In businesses where the CISO reports to the board, 72% of boards rate the information they receive as comprehensive (4 or 5 out of 5) compared with 47% of businesses where the CISO does not report to the board.

CISOs often have multiple lines of reporting and to whom they report directly can vary from business to business. The 2018 Health Check has found that the CISO reports directly to the board in one third (35%) of businesses, suggesting that for a greater proportion of businesses the CISO (and information about cyber security) is further removed from the board.

It cannot be concluded from the available data whether the information boards receive is more comprehensive *as a result* of having a CISO reporting to them directly. It is possible that boards with a more comprehensive understanding in general are also more likely to request that the CISO report to them directly. This should be explored in more detail in future Health Checks.

7. Cyber security is increasingly seen as a strategic issue.

Encouragingly, almost all businesses (96%) have a cyber security strategy. Furthermore, a large majority (88%) of businesses report that the board reviews and challenges the information on cyber risk that they receive, rather than simply approving it. This suggests that for most businesses, boards are engaged in cyber risk management. However, less than two thirds of businesses (60%) report that their appetite for risk (the extent and type of risk the business is willing to take) is agreed and written down, and less than half of businesses (46%) have a dedicated budget for their cyber security strategy.

8. The General Data Protection Regulation (GDPR) has contributed to a greater level of board engagement in cyber security issues.

GDPR appears at least partly responsible for the increased attention boards are giving to cyber threats. 77% of businesses responding to the 2018 Health Check reported that board discussion and management of cyber security had increased since GDPR, with more than half of these businesses also introducing increased security measures as a result.

9. Government advice is the most common source of information for FTSE 350 boards.

A majority of boards are responding actively to Government advice, with almost three quarters (73%) of boards reporting that they adhere to and/or use Government advice to help manage the risks that their business faces, and over half (53%) reporting that they have specifically used the Government's 10 Steps to Cyber Security.

Incident management

10. Most businesses have a cyber incident plan, though many plans have not been subjected to an external audit.

The proportion of businesses that have a cyber incident plan has increased from an already high level (90%) in 2017 to 95% in 2018. However, this still suggests as many as 1 in 20 businesses may not have a cyber indent plan. Furthermore, many businesses may not know whether their plans are fit for purpose, with only just over half of businesses (57%) testing their crisis incident response plans on a set regular basis and only one quarter of businesses using external audits to obtain assurance that their incident plans are fit for purpose. Additionally, 1 in 5 boards have undertaken a crisis simulation on cyber risk in the last 12 months.

Supply chain

11. The supply chain is increasingly becoming a target for cyber attacks; however, recognition of cyber risks in the supply chain appears to be a significant gap amongst a large proportion of businesses.

Whilst recognition of the cyber risks arising from businesses in the supply chain is relatively high (73%), less than a quarter (23%) of businesses recognise the cyber risks associated with businesses that are not directly contracted by the business (fourth party and beyond), leaving them particularly vulnerable to such threats.

Opportunities for improvement

Whilst the 2018 Health Check has seen positive progress in terms of the priority that boards place on cyber security, with boards increasingly viewing cyber security as a strategic issue, the findings suggest there remains much opportunity for improvement.

Almost one in every two FTSE 350 companies (46%) are led by boards that still lack a comprehensive understanding of their critical information, assets and systems.

Boards in this position must take more responsibility for cyber security, and work to improve their understanding, rather than leaving this to the IT department.

Boards should continue to improve their understanding of the impact of loss or disruption associated with cyber threats. Although the potential impacts of cyber threats are better understood now than they were in 2017, one in five boards still have limited understanding of the potential impacts.

Boards with a partial understanding of their critical assets, or a limited understanding of the potential consequence of cyber attacks, cannot ensure their organisation is properly managing the cyber threats they face.

There is also a need for improvement in the comprehensiveness of information being provided to boards, and for boards to be further prepared for cyber incidents, for example, by considering crisis simulations on cyber risk where these have not been undertaken in the last 12 months.

Businesses should consider taking the following steps and accessing the advice and guidance published by the National Cyber Security Centre (NCSC) to improve their management of cyber security and readiness to deal with an incident:

- Increase the skills and knowledge of existing board members so they better understand their business-critical assets and consider recruiting non-executive directors with a technology background to boost the cyber related skills and experience across the board of directors.

- Consider nominating an individual member of the board of directors to take lead responsibility for cyber security risk management.

- Use the NCSC Board toolkit[1] which covers the fundamental aspects of cyber security to:

    - Improve board understanding of cyber threats, enabling boards to request the information they need from their teams, so that they can subsequently make well informed decisions on the risks they face.

    - Support the development of a cyber strategy and ensure that it is aligned with the business objectives.

- Ensure that the Chief Information Security Officer (CISO), or an appropriate staff member, is able to clearly communicate information about cyber security to the board in a way that is aligned with business objectives.

- Test their cyber incident plans regularly to check they are fit for purpose, and consider subjecting them to an external audit.

- Take the NCSC illustrative real-world examples of supply chain attacks[2] into consideration to improve awareness and understanding of the risks. The NCSC have also published guidance proposing a set of 12 principles designed to help businesses establish effective oversight of their supply chain.[3]

1 https://www.ncsc.gov.uk/collection/board-toolkit
2 https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks
3 https://www.ncsc.gov.uk/guidance/supply-chain-security

1. Introduction

1.1. Background

The Government is committed to making the UK one of the safest places in the world to do business online. Part of this objective is to help businesses improve their governance and management of cyber security and to promote widespread adoption of good practice in cyber security.

The FTSE 350 Cyber Governance Health Check survey supports this ambition by providing insights into the cyber governance of the UK's largest businesses, specifically those listed in the FTSE 350. Through the Health Check, the Department for Digital, Culture, Media & Sport (DCMS) aims to:

- Design effective cyber security policy interventions, on the basis of better evidence gathered through the survey;
- Improve and foster engagement between Government and FTSE 350 businesses, to facilitate the Government's efforts to encourage good cyber security practices.

The 2018 Health Check is a non-technical governance questionnaire which assesses the extent to which boards and audit committees of FTSE 350 businesses understand and oversee risk management measures that address cyber security threats to their businesses.

Completion of the questionnaire has resulted in this aggregated report, as well as confidential benchmarking reports for each participating business. Participants should discuss the results with their auditors and trusted advisors.

The UK Government is delivering this project in partnership with businesses that currently audit the vast majority of FTSE 350 businesses: Deloitte, EY, KPMG and PwC.

Whilst the Health Check focuses on businesses in the FTSE 350, the governance behaviours, findings and guidance contained within this report are intended to be useful to organisations of all sizes, including those outside the FTSE 350.

DCMS encourages readers to consider what further steps they and their organisations could be taking to manage their cyber security risk effectively. Those seeking further information to support them with cyber governance should refer to Appendix A of this report, which contains links to key Government cyber security guidance and support of relevance to all businesses.

1.2. Interpreting the results

The FTSE 350 Cyber Governance 2018 Health Check[4] is the fifth Health Check to be undertaken, with four previous Health Checks completed between 2013 and 2017. The questionnaire has been iterated each year to reflect the changing landscape and current challenges and developments. The key themes and question areas have been retained in the 2018 Health Check to allow general comparisons to be made to previous surveys, whilst also providing a fresh and more robust assessment of cyber governance to be used as a baseline for future surveys.

Some areas of questioning are not directly comparable to previous surveys; however, it is still possible to observe and comment on general trends and patterns in the findings.

These include:

- The board's level of understanding of their business' critical information, data assets and systems;
- The board's level of understanding of the potential impacts from the loss of and disruption to critical information, data assets and systems;
- The extent to which the board has explicitly set its appetite for cyber risk;
- How the information provided to the board for the purpose of informing discussions of the cyber risk profile and cyber risk management compares to previous years;
- How cyber risk governance is handled by the board.

The 2018 Health Check is open to all FTSE 350 businesses on a voluntary basis. This may lead to self-selection bias, where those participating in the survey may have different traits and characteristics to those that do not take part. For example, as a group they may be more aware of cyber security issues than those that did not take part. The findings of this survey provide valuable insight into attitudes and behaviours towards cyber security by large businesses; however, readers should not interpret the results as being representative, necessarily, of all FTSE 350 businesses.

Overall, 94 businesses responded to the 2018 Health Check. This compares with 105 respondents in 2017, 113 respondents in 2015/16 and 108 in 2014.

4 https://www.gov.uk/government/publications/cyber-governance-health-check-2018

The survey sample in 2018 is broadly representative of the population in terms of business activity sector, as illustrated in the figure below, though businesses in the financial services and consumer goods sectors are slightly over-represented in the sample and businesses in the industrial goods and services and consumer services sectors are slightly under-represented. This should be kept in mind when interpreting the results.

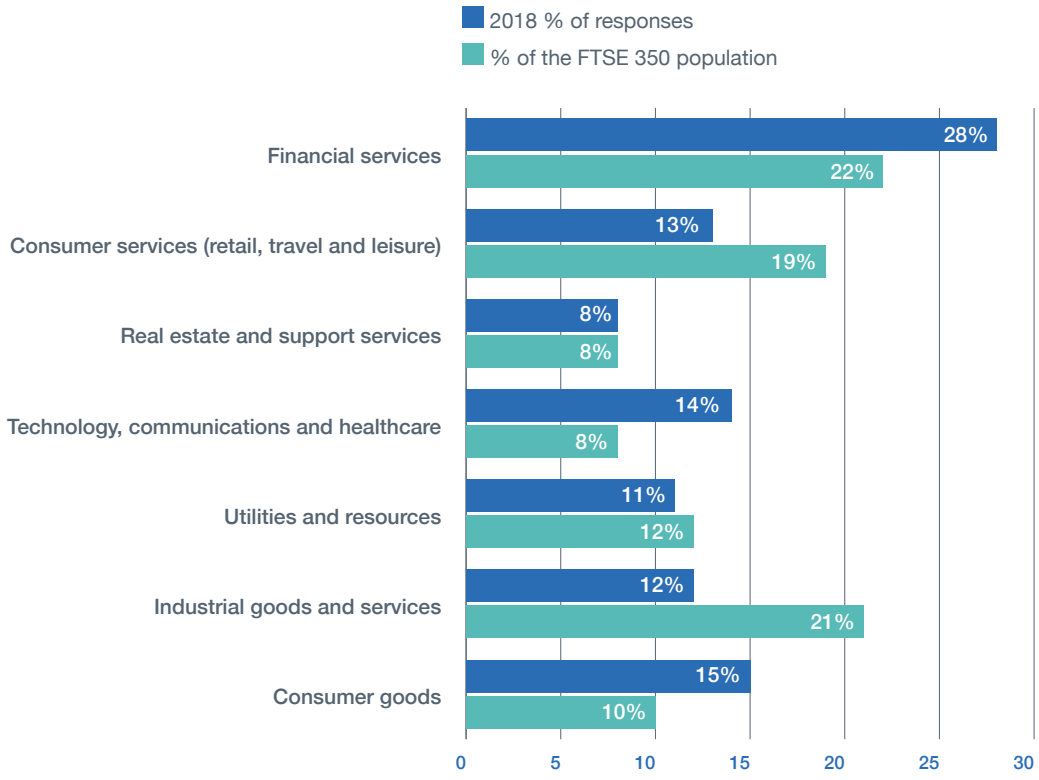
The analysis conducted following completion of the survey included examination of the responses by business activity sector; however, the sample sizes for sectors that constitute a small proportion of the population are low. The survey is not large enough to detect small differences between individual sectors.

As a spread of responses was observed within each sector, it is possible that some differences between sectors may not be reflected in the 2018 Health Check.

Further details about the profile of the 2018 Health Check survey sample, and general trends in the profile of respondent businesses can be found in Appendix C.

The 2018 Health Check survey took place between 1st October and 7th December 2018. Full details of the methodology can be found in Appendix D.

Sector breakdown of respondents



2. Board understanding of cyber security

The National Cyber Security Centre (NCSC) has emphasised that boards of large businesses cannot outsource their cyber security risks and need to understand their role in ensuring their organisation can prosper securely in the digital age. Although board understanding of cyber security has been increasing steadily since the FTSE 350 Cyber Governance Health Check began, many boards have yet to understand cyber risks in the same way or to the same extent they understand financial risks, or health and safety risks.[5]

This section summarises findings from the 2018 Health Check relating to board level understanding of cyber security, including:

- Understanding of the business's critical information, data assets and systems;
- Understanding of the potential impacts of loss of or disruption to these critical assets;
- The perceived risk of cyber threats in comparison to other risks faced by the business.

2.1. Summary

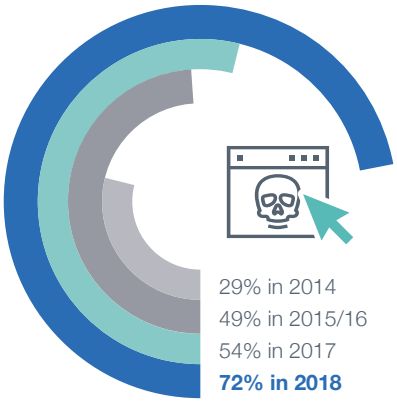
The proportion of boards that understand their business's critical information, data assets and systems, and the potential impact from loss or disruption to these, continues to increase.

- Continuing the upward trend observed in the last Health Check, over half of those responding to the 2018 Health Check (54%) now rate the board's level of understanding of their business's critical information, data assets and systems as comprehensive or fairly comprehensive (rating it 4 or 5 out of 5 where 1 is no understanding and 5 is comprehensive understanding). Almost a third (32%) of businesses up to 2015/16 rated the board to have a *clear* understanding.

5 https://www.ncsc.gov.uk/news/ncsc-releases-core-questions-help-britains-biggest-boards-understand-their-cyber-risk

- Similarly, board understanding of the potential impacts from the loss of or disruption to their information, data and systems has continued to increase, with three quarters of businesses rating board understanding of impacts as comprehensive in 2018, compared with just over half (57%) of businesses rating understanding as clear in 2017.

Acknowledgement of the risk of cyber threats is also increasing, with a considerable majority of boards now rating the risk of cyber threats to be high or very high.



Almost three quarters (72%) of respondents in 2018 reported that the board considered the risk of cyber threats to be high or very high in comparison to all risks that the business faces. This compares to 54% of businesses in 2017, 49% in 2015/16, 29% in 2014 and 25% of businesses in 2013 reporting cyber risk as a top or group level risk.

- Boards in the industrial goods, financial services and technology, communications and healthcare sectors were more likely to rate the risk as high or very high, compared to the other sectors.

- Boards rating the risk of cyber threats as high or very high were more likely than those rating the risks as medium or low to report more comprehensive levels of understanding of their business's critical information, data assets and systems, and the impact from loss or disruption to these.

- The board's assessment of risk is being influenced by wider external factors, such as increased media coverage of cyber security breaches and impacts on the organisations and directors concerned.

- The proportion of boards rating the risk of cyber threats as high or very high is increasing at a faster rate than board-level understanding of threats and impacts.[6]

6 The FTSE 350 Cyber Governance Health Check 2018 was not designed to explore the causality between board understanding and board assessment of risk. This should be explored in subsequent research.

But there is still significant opportunity for improvement.

- Whilst board understanding is improving and a greater proportion of businesses are recognising the risk of cyber threats compared to previous Health Checks, there is still much room for improvement:
    - Only 12% of all businesses rated board understanding of the business's information, data and systems as fully comprehensive (5 out of 5), which suggests that the majority of businesses feel that board understanding could be improved.
    - Only 16% claim their boards have a comprehensive understanding (rating understanding as 5 out of 5) of all types of impact tested – i.e. the potential impacts of cyber threats on customers, share price and reputation.
    - Only 15% of all businesses rate board understanding of their personal, legal and fiduciary responsibilities as comprehensive (5 out of 5).

Advice

Boards seeking to improve their understanding of cyber security can do so by:

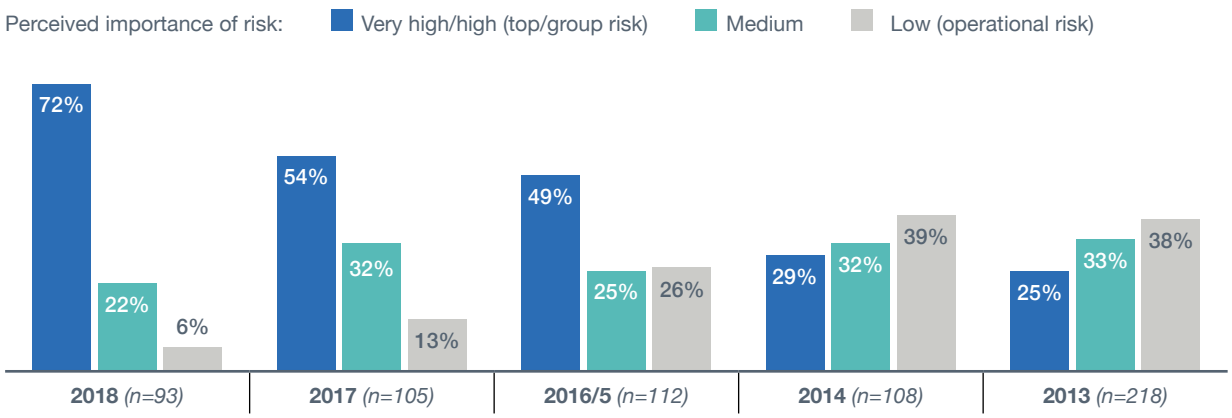
- Using the recently published NCSC Board toolkit[7], which covers the fundamental aspects of cyber security that board members should know about. Launched in 2019, the toolkit is designed to help boards get the information they need to make well informed decisions on the risks they face. Incorporating a series of questions amongst other tools, boards can use the resulting information to understand and prioritise their risks, and to take steps to manage those risks.
- Ensuring that the CISO, or an appropriate staff member, is able to clearly communicate information about cyber security in a way that is aligned with business objectives.
- Recruiting Non-Executive Directors with a technology background.

7 https://www.ncsc.gov.uk/collection/board-toolkit

2.2. Board perceptions of cyber risk

Responses to the 2018 FTSE 350 Cyber Governance Health Check suggest cyber threats are being acknowledged and prioritised by a greater proportion of businesses than ever before. Continuing the general upward trend observed since the Health Check began, 72% of respondents in 2018 reported cyber threats are considered by the board to be very high or high risk in comparison to all risks the business faces.

Perceived importance of cyber risk[8]

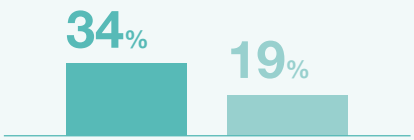


Attitudes towards cyber threats have shifted substantially over the last five years. Almost 4 in 10 respondents in 2013 considered cyber threats to be a low risk or an operational IT issue. Today, an increasing majority of businesses recognise cyber threats as a strategic risk management issue with only 6% in 2018 rating the risk of cyber threats as low in comparison to all risks the business faces.

8 The increase in the proportion of businesses perceiving the importance of cyber risk to be high/very high is statistically significant at 99% confidence level.

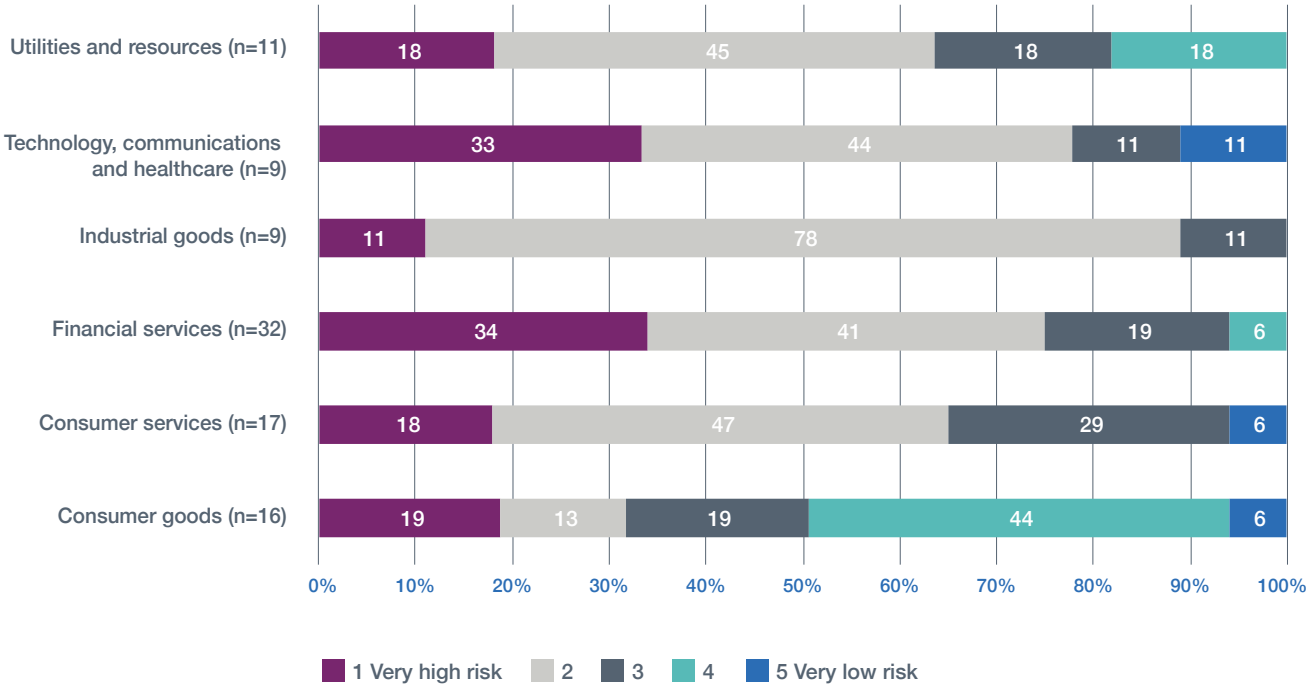
Sector Focus

The perception of cyber risk varies across sectors. Businesses providing financial services are more likely to rate cyber threats as a very high risk compared with businesses in other sectors.[9] Observations of the data also show that boards in the technology, communications and healthcare and industrial goods sectors are more likely to assess the risk of cyber security to be high or very high.



34% of businesses in the financial services sector rate cyber threats very high compared to 19% of businesses in other sectors.

Risk perception by sector

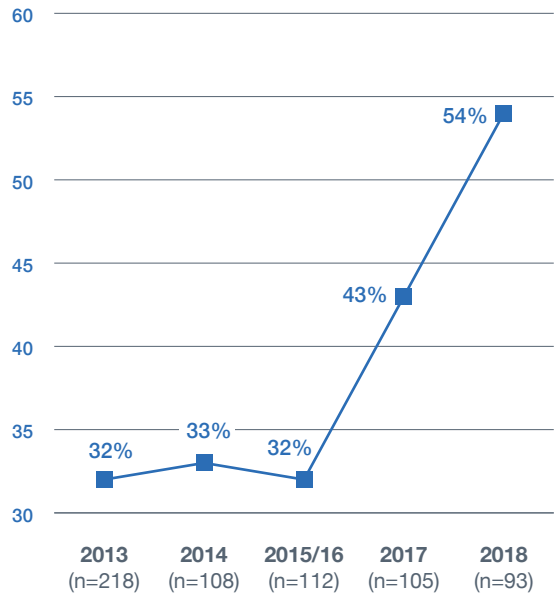


9 Businesses in other sectors have been grouped together here to allow for robust comparison.

2.3. Board understanding of critical assets

As in 2017, the 2018 Health Check has seen a further increase in the proportion of boards with a good understanding of their business's critical information, data assets and systems. Whilst the increase in board understanding is encouraging, board understanding has not increased at the same rate as the board's perception of cyber risk.

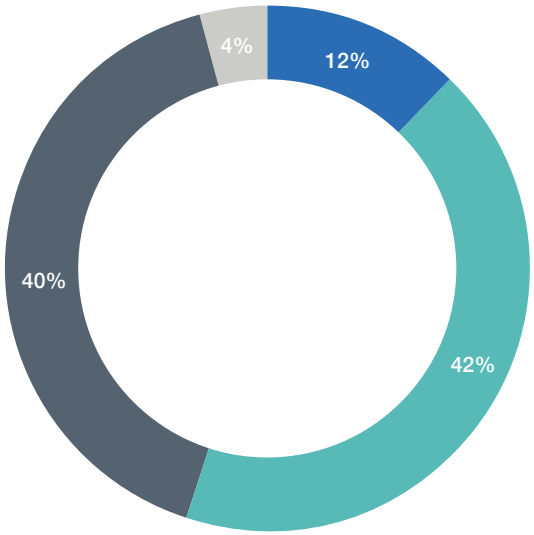
The proportion of businesses rating board understanding of the business's critical information, data assets and systems as comprehensive (4 or 5 on a scale of 1 to 5 in 2018) or clear (top rating in 2013-17) [10]



Despite the increase in understanding over time, only 12% of respondents rated comprehensiveness as 5 out of 5, indicating most respondents felt there was room for the board to improve the breadth of their understanding. Furthermore, given a large proportion of businesses rate the risk of cyber threats as high or very high (72%), almost half (44%) of businesses responding to the 2018 Health Check appear to have boards with a limited or only partial knowledge of their organisation's critical information, data assets and systems. This is indicated by them rating the comprehensiveness of the board's understanding as 2 or 3 out of 5.

10 The increase from 2017 to 2018 is statistically significant at a confidence level of 80%. The increase from previous years (2015/16, 2014 and 2013) to 2018 is statistically significant at a confidence level of 99%.

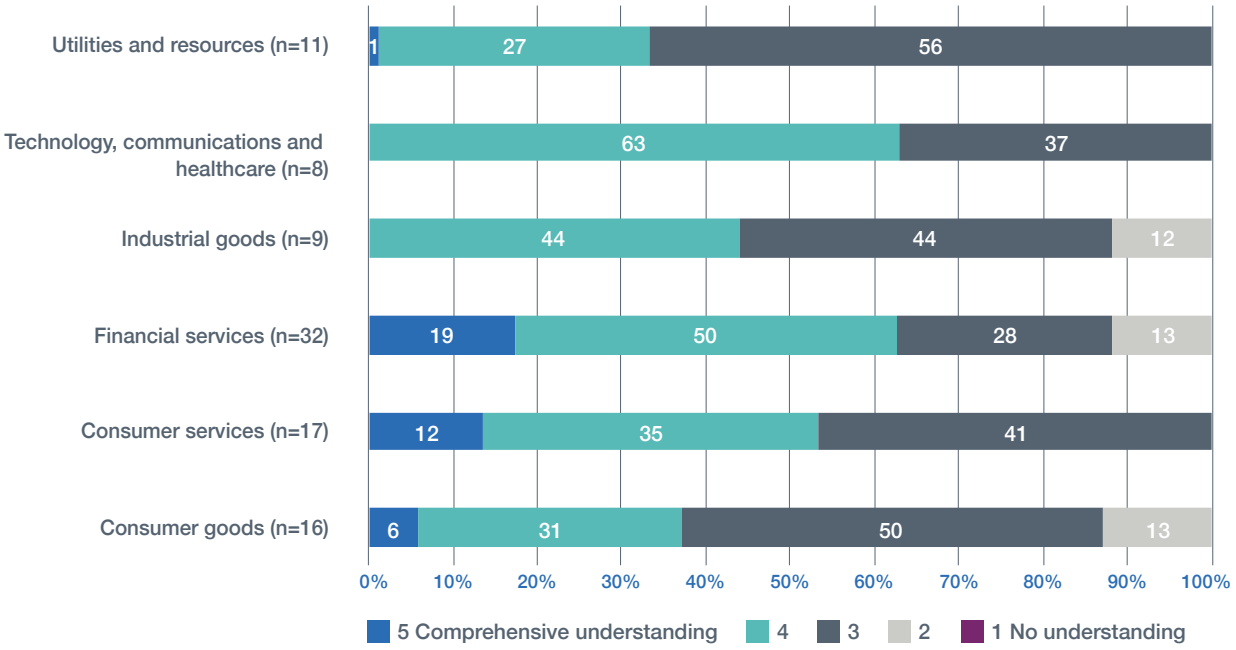
Board understanding of business-critical assets



Sector Focus

Although the sample sizes for individual sectors are too small to comment on significant differences between sectors, the data suggest that the level of understanding does vary by sector. Whilst the financial services sector has the highest proportion rating understanding as comprehensive across all sectors, there is also a noteworthy proportion in this sector reporting that they do not have a comprehensive understanding.

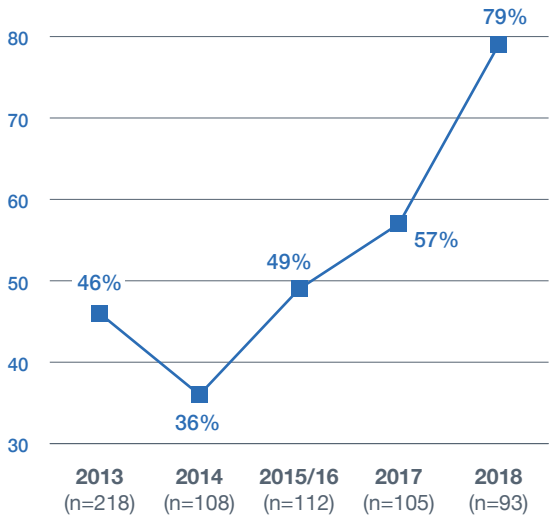
Board understanding of assets by sector



2.4. Board understanding of the impact of cyber threats

Understanding of the potential impact from the loss of and disruption to critical information, data assets and systems has continued to improve in 2018.[11] In the 2018 Health Check, all businesses reported to have at least some understanding of the potential impact. The marked increase in understanding may be linked to an increase in press coverage of cyber attacks and breaches in the last year, as this may have driven boards to consider the potential impact of cyber attacks on their own organisations.

Board understanding of the impact of cyber threats on customers, reputation and short-term share price[12]



11 The increase from 2017 to 2018 is statistically significant at 99% confidence level.

12 Based on proportion of boards with a comprehensive understanding (4 or 5 out of 5) in 2018, taking the average score across the three types of impact tested, and a clear understanding (top rating out of 3 in 2013-7).

Whilst the increase in understanding is a positive finding, only a minority of businesses (16%) claim that their boards have a comprehensive understanding (rating understanding as 5 out of 5) of all three types of impact tested, i.e. the impact on customers, share price and reputation. This indicates board understanding could be improved in a majority of businesses.

The potential impact on reputation is better understood by boards than the impact on short term share price and customers, though there is scope for improvement in understanding in all areas.

80% 80% of businesses rate board understanding of the **impact on customers** as comprehensive (4 or 5 out of 5)

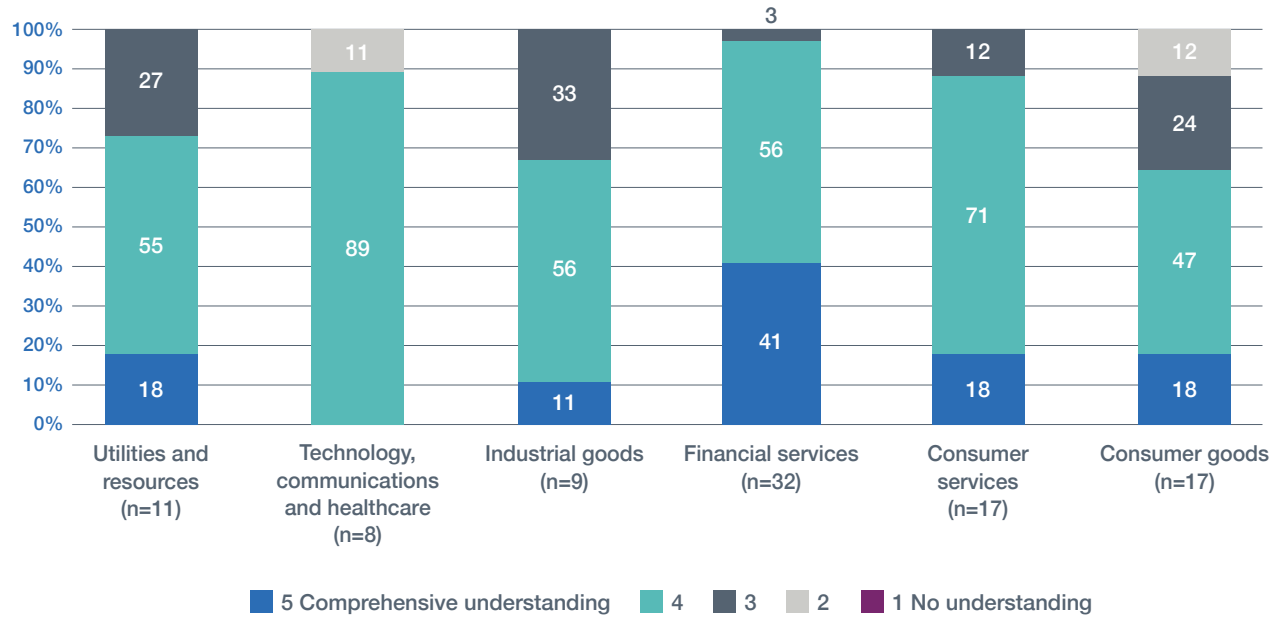
79% 79% of businesses rate board understanding of the impact on **short-term share price** as comprehensive (4 or 5 out of 5)

89% 89% of businesses rate board understanding of the **impact on reputation** as comprehensive (4 or 5 out of 5)

Sector Focus

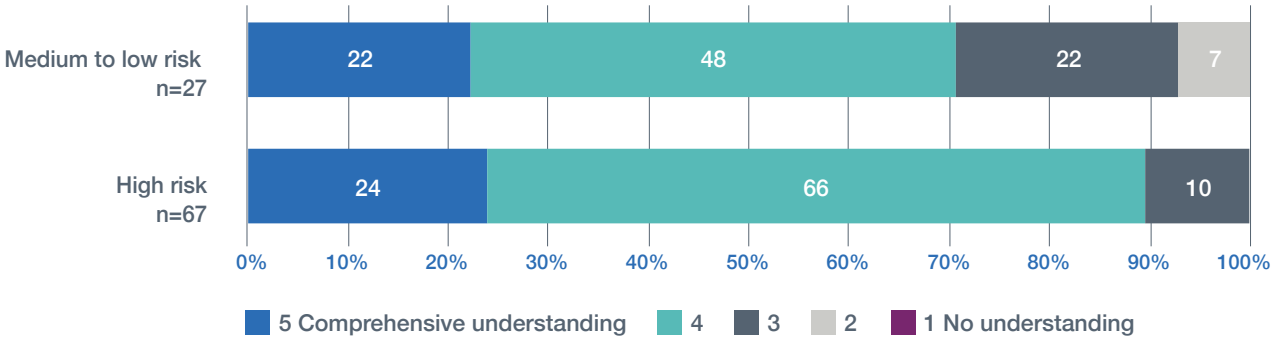
The data shows that a higher proportion of businesses in the financial services, consumer services and the technology, communications and healthcare sectors rate board understanding as comprehensive or fairly comprehensive.

Board understanding of the impact from the loss of or disruption to critical assets by sector[13]



Where boards perceive the risk of cyber threats to be high or very high, they are more likely to have a comprehensive understanding of the potential impacts (compared to businesses where the board perceives the level of risk to be lower). However, around 1 in 10 boards rating the risks as high had only a partial understanding of the impacts.

Level of perceived risk and board understanding of the potential impacts[13]



13 Based on the average rating of understanding across the three types of impact tested – on customers, on short-term share price and on reputation.

2.5. Board understanding of cyber risk responsibilities

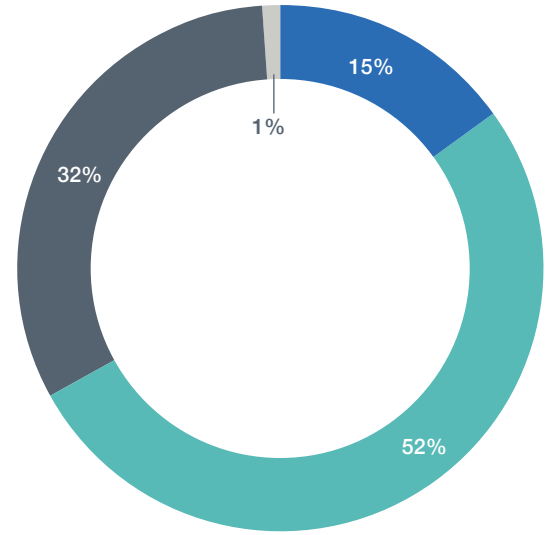
A business's board is bound by a fiduciary duty to operate in the best interests of the business. If a board member is found to have done something that betrays their fiduciary duties, that individual can be held liable by the business or its shareholders. Board members must take reasonable care and diligence, which involves management of risk across the business, including cyber security risks. It is therefore important that the board understands how cyber risk relates to their personal, legal and fiduciary duties.

The 2018 Health Check asked respondents for the first time to rate the board's understanding of these duties in relation to cyber risk. Only 15% of respondents rated their board's understanding as comprehensive (5 out of 5), indicating the majority of businesses would benefit from further information on this subject.

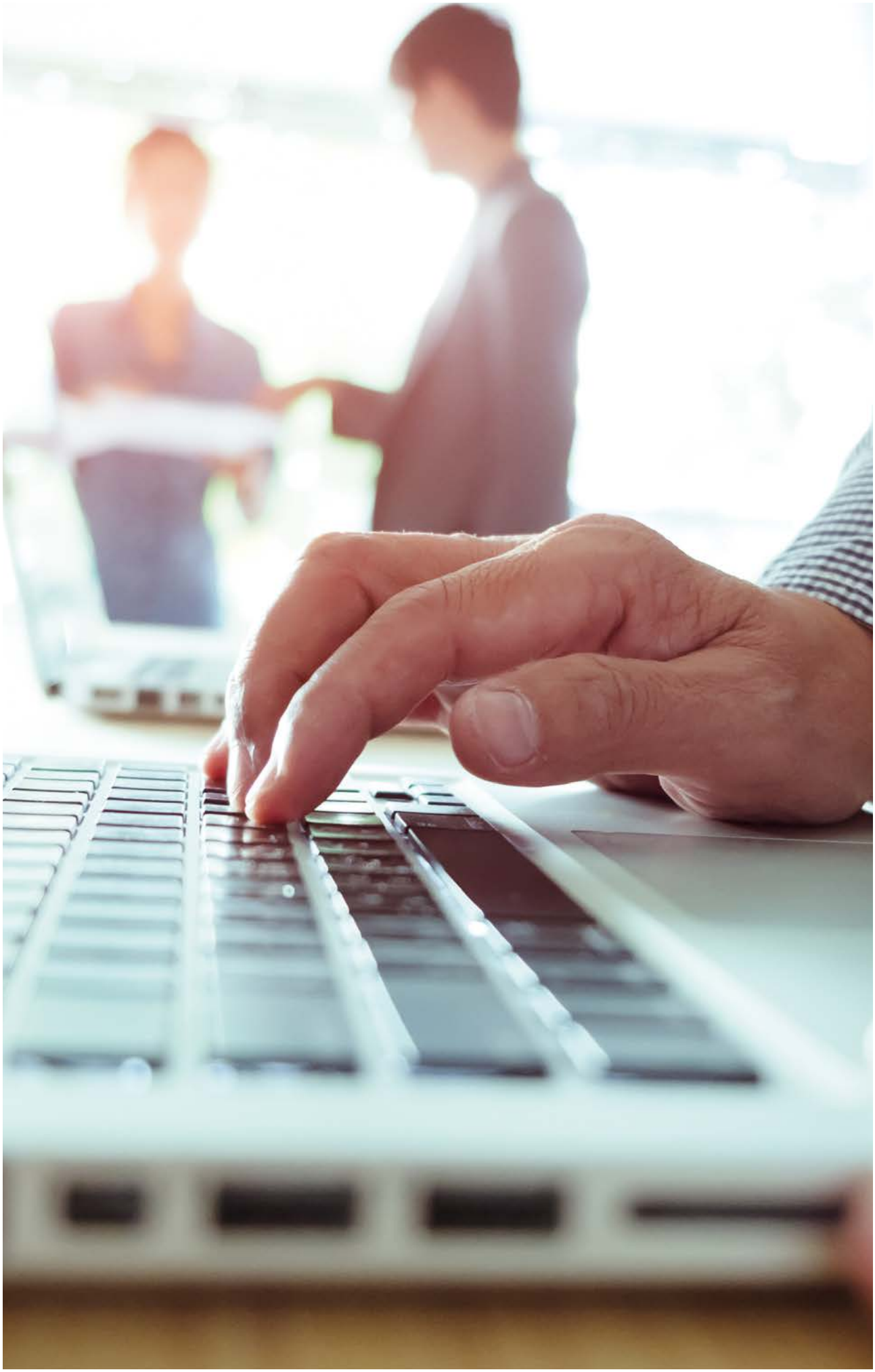
Advice

The Financial Reporting Council has recently updated its Corporate Governance Code[14] which underpins the board's fiduciary duties. Whilst the Code does not contain specific information about cyber risk, the Risk Management and Internal Control section of the Code may be a useful source of advice for board members.

Board understanding of how cyber risk relates to their personal, legal and fiduciary duties



14 https://www.frc.org.uk/getattachment/88bd8c45-50ea-4841-95b0-d2f4f48069a2/2018-UK-Corporate-Governance-Code-FINAL.PDF



3. Board engagement with cyber risk information

Boards rely on their staff to provide them with information that enables effective decision-making on cyber security. It is important that information on cyber risk is presented and communicated in a manner consistent with information presented to the board about other business risks, particularly as many board members will not have a background in technology or cyber security.

This section summarises the evidence arising from the FTSE 350 Cyber Governance Health Check relating to how boards engage with cyber risk information, including:

- How the board receives information, i.e. who the Chief Information Security Officer (CISO) reports to, the board's perception of the information they receive in terms of its comprehensiveness, robustness and the extent to which it is up to date, and the sources of advice and guidance used or adhered to.
- How the board makes decisions relating to cyber security i.e. whether they have a cyber security strategy, how cyber governance is handled by the board and the impact of GDPR on board engagement with cyber security.
- How the board disseminates cyber security information i.e. how clearly they set their appetite for cyber risk and share it across the business.

3.1. Summary

Whilst a majority of businesses report that information about cyber security that the board receives is up to date and robust, fewer businesses report that the information is comprehensive.

For the purpose of informing discussion of cyber risk management:

71% 71% of businesses rate the information the board receives as **up to date** (4 or 5 out of 5 where 1 is not up to date and 5 is up to date)

71% 71% of businesses rate the information the board receives as **robust** (4 or 5 out of 5 where 1 is not robust and 5 is robust)

53% 53% of businesses rate the information the board receives as **comprehensive** (4 or 5 out of 5 where 1 is not comprehensive and 5 comprehensive)

Furthermore, more than a quarter of businesses responding to the 2018 Health Check selected the middle of the scale or below in the three areas tested, indicating that the information provided to boards in many cases is insufficient. Feedback from the audit firms supporting delivery of the 2018 Health Check suggests that some boards may not be getting the data they want, presented in context, with an experienced or evidence-based understanding of the impact.

More than one third (35%) of businesses responding to the FTSE 350 Cyber Governance Health Check have a Chief Information Security Officer (CISO) that reports to the board.

- However, this leaves two thirds of businesses where the board is further removed from the CISO, presumably with at least one additional reporting line in the hierarchy.
- Interestingly, the 2018 Health Check has found that respondents were more likely to rate the information the board receives as comprehensive where there is a CISO reporting to the board. However, it is not certain that this is fully attributable to direct reporting by the CISO.

Percentage rating the information the board receives as comprehensive

70% of the businesses where the CISO reports to the board, rate the information as comprehensive (4 or 5 out of 5) compared with 44% of businesses where the CISO does not report to the board.

The 2018 Health Check has found that a majority of boards are now engaged in cyber security, view cyber security as a strategic issue and are actively trying to manage their cyber risks.

- Encouragingly, almost all businesses (96%) have a cyber security strategy, and the majority of businesses (88%) report that their board reviews and challenges the information on cyber risk that they receive, rather than simply approving it. This suggests that cyber security is seen as a strategic issue by the majority of businesses.

- However, only two thirds (67%) of businesses have a strategy that is aligned with their business objectives, suggesting that for many businesses cyber security is not being fully integrated into the business and operational decision-making processes.

- Furthermore, less than two thirds (60%) of businesses report that their appetite for risk (the extent and type of risk the business is willing to take) is agreed and written down. Therefore, for more than a third (40%) of businesses, there is a risk that not all staff members share the same vision as the board regarding the level and type of risk that they are willing to take.

Board engagement in cyber security has improved since the introduction of GDPR.

- The introduction of GDPR has contributed, at least in part, to boards paying increased attention to cyber threats and cyber security issues. 77% of businesses report that board discussion and management of cyber security had increased since GDPR, and more than half of these businesses have introduced increased measures as a result.

The greater the understanding that boards have of their information, data and systems, the more likely they are to have also agreed, written down and communicated their appetite for cyber risk.

- Of those that rated understanding as high or very high, 44% have agreed, written down and communicated their appetite for cyber risk.

- This compares to 24% of businesses that rate understanding of assets as medium or low that have done so.

15 https://www.ncsc.gov.uk/collection/board-toolkit

3.2. Receipt of information

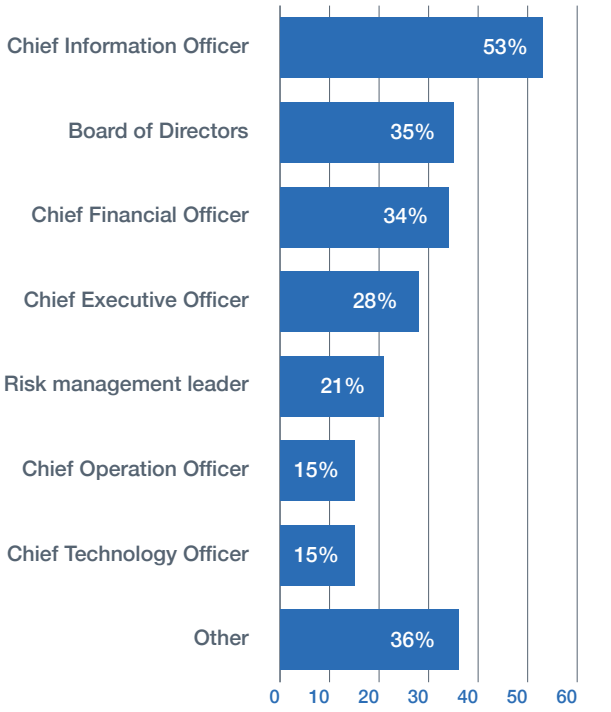
3.2.1 The role of the Chief Information Security Officer

NCSC guidance suggests that Chief Information Security Officers (CISOs) are one of the greatest assets an organisation has, and their role in improving board knowledge of relevant cyber security issues should not be underestimated. Where possible, it is recommended that CISOs report directly to the CEO or board of directors so that senior leadership have the latest information and to speed up decision making regarding cyber security.[16] However, it may not be appropriate in all organisations for the CISO to report directly to the board. For example, it is also important that boards receive cyber risk information that is presented in relation to the wider context of the organisation, and there may be a more appropriate individual within the business to do this.

For almost half of the businesses (45%) that responded to the 2018 Health Check, their CISO either reports to the board of directors or to the CEO and in 13% of businesses the CISO reports to both. Whilst this is encouraging, it does suggest that for the other half of businesses the CISO does not have direct communication lines with their board which could affect the business's ability to respond quickly to cyber threats.

For half (50%) of businesses, the CISO has one line of reporting. For the other half (50%) of businesses, the CISO reports to multiple individuals within the business, with up to seven reporting lines. In over a quarter of businesses (28%) the CISO has three or more reporting lines.

Who the Chief Information Security Officer regularly reports to (multiple answers possible)



Of those that selected 'other,' the CISO reported most frequently to the audit committee or chair (7 responses), or the Chief Risk Officer (3 responses).

Board understanding of the business's critical assets and the impacts from the loss of or disruption to them is higher among businesses where the CISO reports to the board, although it is not possible to attribute this to the direct reporting of the CISO. Similarly, for businesses where the CISO reports to the board, the board are more likely to view cyber risk as high. Again, this may suggest that more direct communication between the CISO and the board leads to a better understanding of the risk. However, it is possible that boards that view the risk of cyber threats as high

16 https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda

demand more in terms of the information they require and so direct reporting by the CISO is more likely.

3.2.2 Information provided to the board

CISOs and other members of management are tasked with providing the board with comprehensive, robust information about cyber security. The individuals who brief the board on these matters tend to be highly technical professionals, who must align their communications with the business-wide risk management strategy and business objectives in order to ensure that boards understand the relevance of cyber security in achieving their business mission.

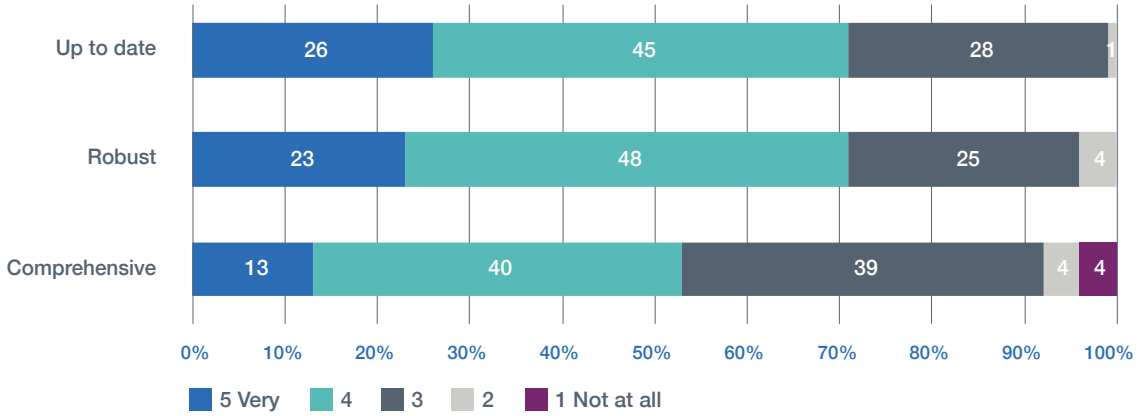
The 2018 Health Check has found that where CISOs report to the board, the board is more likely to rate the information as comprehensive.

Proportion of boards rating the information that they receive as comprehensive (4 or 5 out of 5)

	% of boards rating information received as comprehensive
Businesses where the CISO reports to the board	72%
Businesses where the CISO does not report to the board	47%

Whilst a majority (71%) of businesses report that information received by the board is up to date and robust, only half (53%) report that the information is comprehensive for the purpose of informing discussions relating to cyber risk profile and cyber risk management. For each of the areas tested, one in three businesses (or more) responding to the 2018 Health Check selected the middle category or below, suggesting the information provided to boards in many cases is insufficient.

The extent to which the information provided to the board is comprehensive, robust and up to date



It is worth noting that in the 2017 Health Check, 8% of businesses reported that they receive 'very little insight' with regards to up to date management information and threat intelligence to underpin the board's discussion of cyber risk. When compared to the responses in the 2018 Health Check (with 1% of businesses rating the extent to which information is up to date as 1 or 2 out of 5) this suggests businesses are receiving more up to date information in general.

Interestingly, some boards rating the risk of cyber threats as high are not receiving information they believe is comprehensive, robust or up to date. Of those that provided lower ratings (3 or below out of 5) when asked if the information provided to the board was comprehensive, robust and up to date (14 businesses), half were businesses that rated the level of perceived risk as high. This may be because boards that rate the risk as high have higher demands and expectations of information provided to them. Wider factors outside the control of individual businesses may also be contributing to information not being comprehensive, robust or up to date. These include general shortages or skills gaps in the field of cyber security which have been explored in recent studies and Government reports such as the 'Cyber Security Skills and the UK's Critical National Infrastructure' report published in July 2018[17] and as stated in the 'Initial National Cyber Skills Strategy' published in December 2018.[18]

Advice

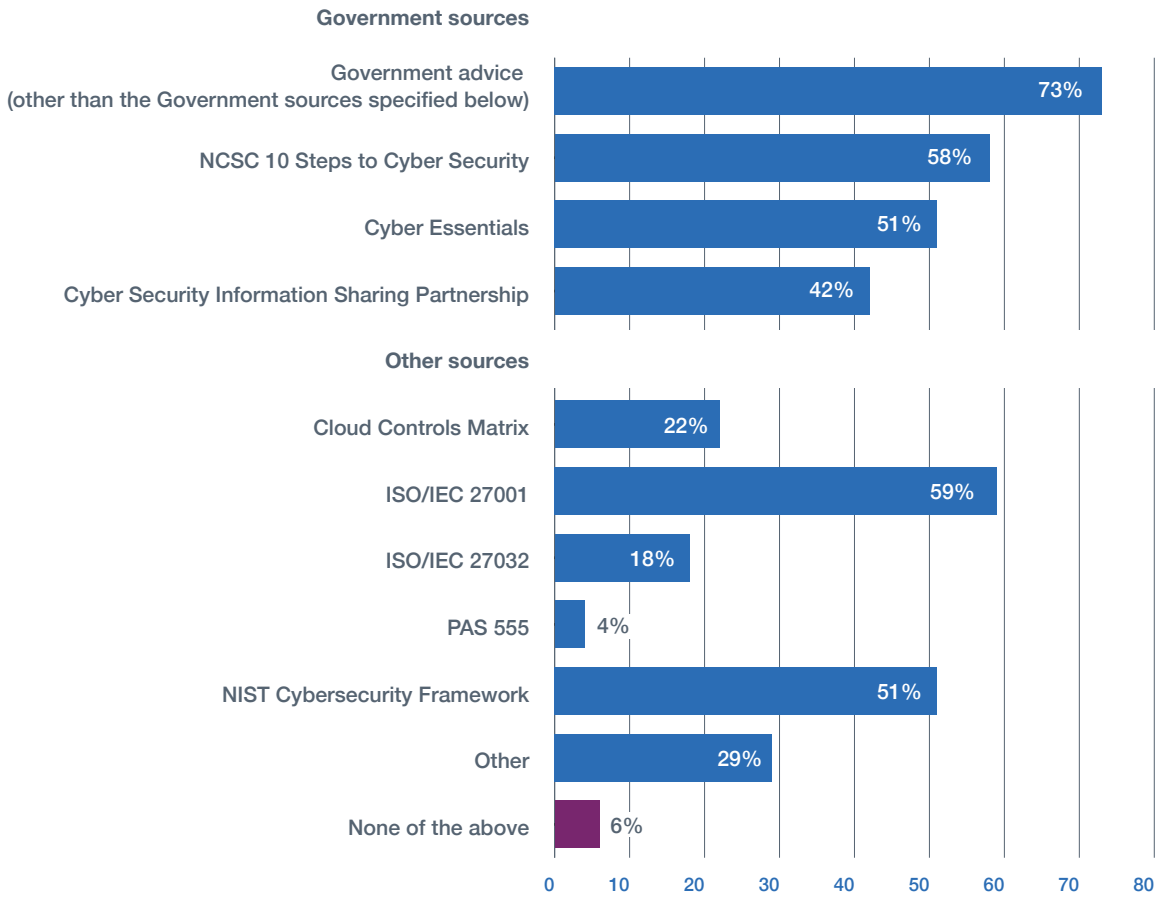
The recently released NCSC Board toolkit[19] provides a helpful starting point to explore an organisation's priorities in managing cyber risks.

17 https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/706/70602.htm
18 https://www.gov.uk/government/publications/cyber-security-skills-strategy
19 https://www.ncsc.gov.uk/collection/board-toolkit

3.2.3 Sources of advice and guidance

Businesses are using multiple sources of advice and guidance to manage their organisation's cyber risk, with Government advice being the method most cited by businesses in this Health Check.

Sources of advice and guidance adhered to or used by businesses in managing cyber risk (multiple answers possible)



Other sources of advice and guidance cited by a few respondents include the Information Security Forum (ISF) (cited by five respondents), Information Sharing and Analysis Centres (ISACs), IEC62443, Open Web Application Security Project (OWASP), Centre for Internet Security (CIS) Controls, Cloud Security Alliance, SafePharma, NIST 800-171, and Cyber security for defence suppliers (Def Stan 05-138). Some respondents stated that they also sought advice from professional advisors and consultants, while a few said they received guidance through attending seminars and conferences and following the footsteps of their peers in the industry.

85% of businesses are adhering to or using more than one source of advice to manage their own cyber risk.

Businesses where the board assesses the risk of cyber security to be high or very high tend to adhere to or use more sources of advice (4 on average) compared to businesses where the board rate the risk of cyber security as medium to low (3 on average). Similarly, businesses who have a more comprehensive understanding of the potential impact from the loss of or disruption to their information, data and systems are more likely to use or adhere to more sources of advice (4 on average) compared to those who have a medium to low understanding (3 sources on average). Given the significant increase in the proportion of boards acknowledging the risk of cyber threats, the findings suggest boards will be increasingly receptive to further Government advice and guidance on cyber security.

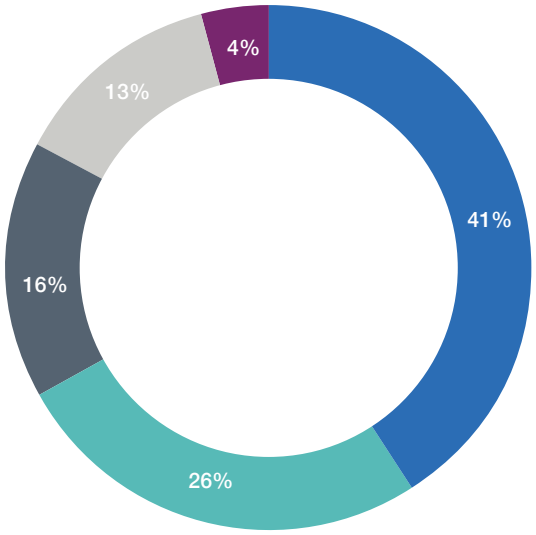
3.3. Board decision-making

3.3.1 Cyber security strategy

A key purpose of a cyber security strategy is to coordinate organisational efforts to prevent cyber security attacks and mitigate cyber risks. Having a cyber security strategy supports a business to better understand the cyber security environment, and to take a more proactive approach to preventing attacks. It is important that cyber security strategies align with the business objectives to ensure that the business's goals, objectives and KPIs disseminate to employee performance metrics and ensure cyber security is embedded throughout the organisation.

Encouragingly, the 2018 Health Check has found that the vast majority of businesses (96%) have a cyber security strategy, although only two thirds (67%) of businesses have a strategy that is aligned with their business objectives. This suggests roughly one third of businesses still view cyber security as a predominantly operational issue rather than a strategic matter.

Businesses with a cyber security strategy



Response (n=90)

- Yes, we have a dedicated risk based cyber strategy aligned with business objectives and supported by a dedicated budget
- Yes, we have a dedicated cyber strategy aligned with business objectives
- Yes, we have a cyber strategy, but it is largely focussed on technology improvements and implementation
- Yes, we have a cyber strategy as part of our IT strategy
- No, we do not have a formal cyber strategy

Businesses are more likely to have a dedicated cyber strategy aligned with business objectives and supported by a dedicated budget where the board perceives the risk of cyber risk to be high or very high. Findings indicate businesses that have a dedicated strategy are more likely to:

- Have a board which has written down their appetite for risk and communicated it to all staff;
- Have a board that reviews and challenges information on cyber security provided to it;
- Have a board with a better understanding of their personal, legal and fiduciary duties;
- Use more forms of advice and guidance in managing their cyber security risk.

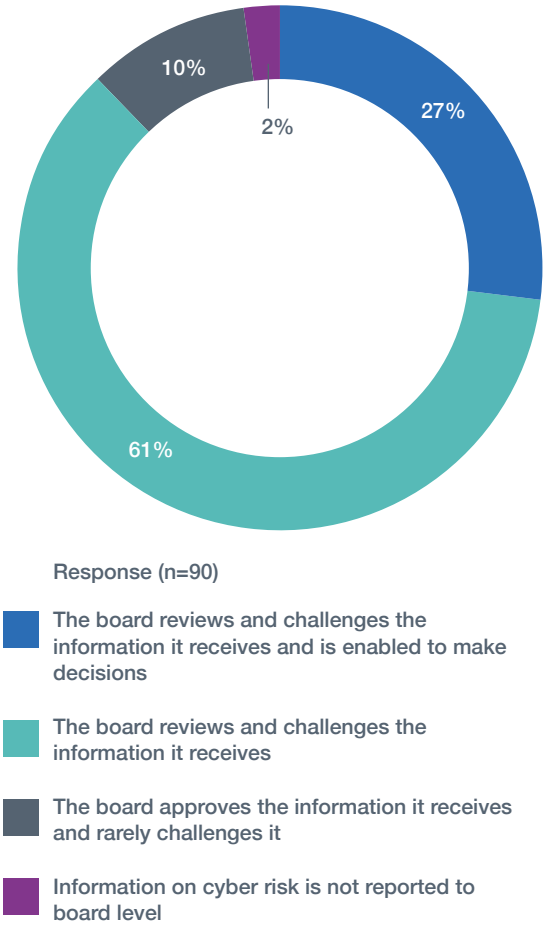
This indicates cyber security is genuinely more embedded in businesses with a dedicated cyber strategy, whether because of the strategy or otherwise.

3.3.2 Cyber risk governance

The 2018 Health Check results suggests that the vast majority of boards are now engaging in cyber security and are actively trying to manage their cyber risks.

Almost all boards (98%) are considering cyber risk and most boards (88%) are reporting that they review and challenge the information they receive, rather than simply approving it. This compares with 50% of businesses that reported in 2017 that the board reviews and challenges reports on the security of their customers, and 10% of businesses in 2017 that said the board actively manages their cyber risk profile throughout the year.

How cyber risk governance is handled by the board



The findings suggest improving board understanding of business-critical information, data assets and systems is an important step in fully embedding governance of cyber risks. Boards that rate their understanding of business-critical information, data assets and systems as comprehensive or fairly comprehensive are more likely to review and challenge the information they receive.

96% 96% (n=48) of boards who rate their understanding of their business's information, data and systems as **comprehensive** or fairly comprehensive review and challenge the information it receives.

83% 83% (n=40) of boards who rate their understanding of their business's information, data and systems as **less comprehensive** (3 out of 5 or below) review and challenge the information it receives.

Board understanding of business-critical assets is improving more slowly compared to board acknowledgement of cyber threats. As such, understanding the business's assets should continue to be an area of focus for NCSC and others providing guidance for board members.

3.3.3 Cyber risk appetite

Explicitly setting appetite for risk – i.e. outlining the amount and type of risk that the business is willing to take through a set of qualitative statements and associated quantitative metrics – is important to ensure that all relevant staff members share the same vision as the board. Not explicitly communicating appetite for cyber risk to relevant staff members increases the risk of staff members making decisions or taking action that could leave the business more vulnerable to a cyber attack.

Continuing the trend observed in the 2017 Health Check, an increasing proportion of businesses are setting and communicating their risk appetite compared to previous Health Checks. However, many businesses could be doing more in this regard.

In 2018:

33% report that they have set their appetite for cyber risk through the board agreeing, writing it down and communicating it to all relevant staff.

27% report that the board has agreed and written it down, but it has not been shared widely.

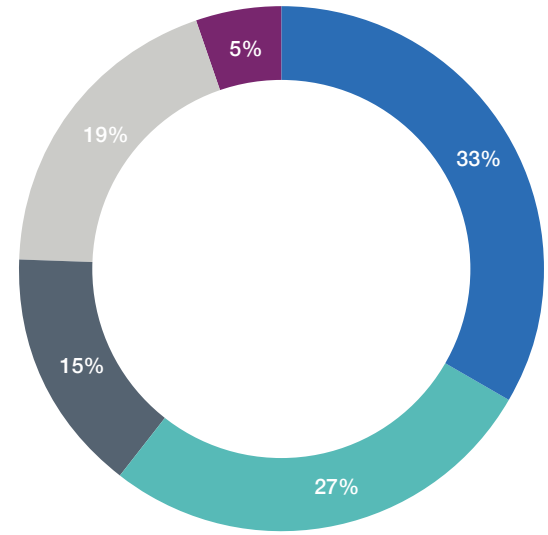
In 2017:

53% of businesses reported that the board's appetite for cyber risk was clearly set and understood.

In 2015/16:

33% of businesses reported that the board's appetite for cyber risk was clearly set and understood.

The extent to which the board has explicitly set its cyber risk appetite



Response (n=94)

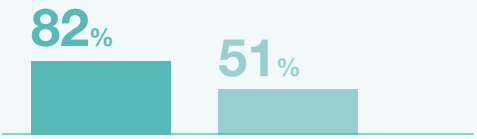
- The board has agreed, written it down and communicated to all relevant staff
- The board has agreed and written it down, but it has not been shared widely
- The board has agreed but not written it down
- The board has discussed cyber risk appetite, but has not yet agreed its appetite
- The board has not discussed cyber risk appetite explicitly

The greater the understanding that boards have of their assets, the more likely they are to have also agreed, written down and communicated their appetite for cyber risk.

Of those that rated understanding as comprehensive or fairly comprehensive, 44% have agreed, written down and communicated their appetite for cyber risk. This compares to 24% of businesses that rate understanding of assets as less comprehensive.

Sector Focus

Businesses in the financial services sector are much more likely to have agreed and documented their appetite for cyber security risk.



82% (23/28) of financial services businesses have agreed and written down their risk appetite compared to 51% of businesses across the other sectors.

Advice

The NCSC risk management guidance[20] is a useful source of advice for businesses wanting to more clearly set their risk appetite for cyber security.

20 https://www.ncsc.gov.uk/collection/risk-management-collection

3.3.4 Impact of the General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) requires that personal data must be processed securely using appropriate technical and organisational measures. The regulation does not mandate a specific set of cyber security measures but rather expects businesses to take 'appropriate' action and manage risk. There are significant penalties for individuals and businesses for non-compliance with GDPR.

The 2018 Health Check indicates that GDPR has increased the attention FTSE 350 boards give to cyber risk. Over three quarters of businesses (77%) report that board discussion and management of cyber risk has increased since the introduction of GDPR, and more than half (55%) of these businesses have increased measures as a result. Businesses introducing increased measures in response to GDPR (41% of all businesses) were more likely to test their crisis plans on a regular basis, and to have involved the board in a crisis simulation exercise within the last 12 months.

Boards introducing additional measures in response to GDPR were more likely to:

- Test their crisis plans on a regular basis (62% of this group do so compared to 55% of those that have not changed measures since GDPR).
- Have board involvement in a crisis simulation exercise – 30% of this group have a board that has been involved in crisis simulation in the last 12 months compared to 20% (4 out of 20) who have not increased measures since GDPR.

The impact that GDPR has had on the priority that businesses attach to cyber security is currently being explored through qualitative research in the latest DCMS Cyber Security Breaches Survey 2018.

Advice

The NCSC have worked with the Information Commissioner's Office (ICO) to develop a set of GDPR Security Outcomes. This guidance[21] provides an overview of what GDPR says about security and describes a set of security related outcomes that all organisations processing personal data should seek to achieve.

21 https://www.ncsc.gov.uk/GDPR and https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes

4. Board involvement in incident management

Cyber incidents can affect all types of businesses and therefore it is important that all businesses are prepared. Businesses should have an incident response plan to help them respond quickly and limit long-term damage to the business's reputation. Incident response plans should be tested regularly to ensure they are fit for purpose and are able to effectively prepare the organisation to respond to continually evolving threats.

This section summarises evidence relating to the board's involvement in incident management, including:

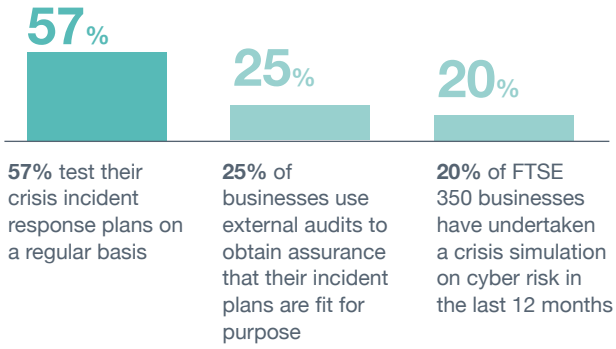
- The number of businesses responding to the 2018 FTSE 350 Cyber Governance Health Check that have experienced a major cyber incident in the last 12 months.
- Whether businesses have an incident response plan in place.
- The extent to which and how regularly incident response plans are tested, and the mechanisms used to verify that plans are fit for purpose.
- Whether boards have been involved in cyber crisis simulations.

4.1. Summary

11% of businesses responding to the 2018 Health Check report that they have experienced a major cyber attack or incident causing disruption to business operations in the last 12 months.

These businesses do not have any common characteristics, emphasising that cyber incidents can affect all types of businesses. There is a need for all businesses to be prepared to respond to a cyber attack or breach.

Whilst the proportion of businesses that have a cyber incident plan has increased, the evidence suggests fewer businesses are testing their plans regularly and obtaining assurance that their incident plans are fit for purpose.

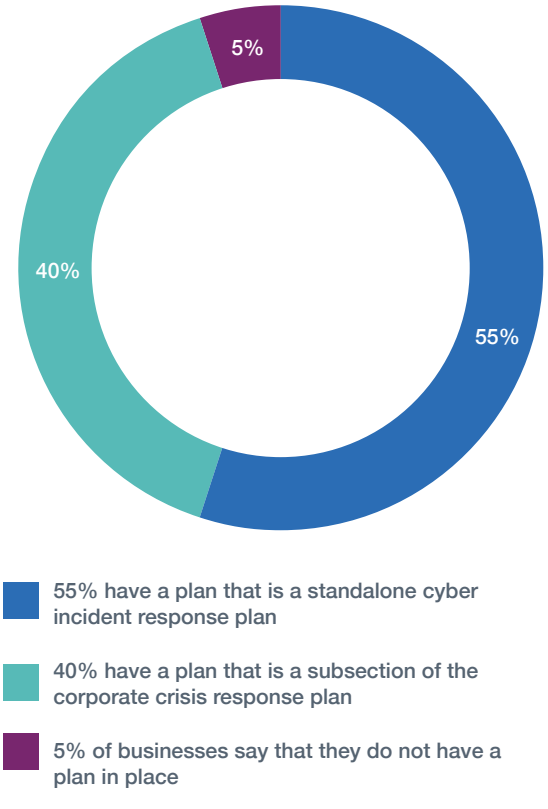


Encouragingly, the proportion of businesses that have a cyber incident plan has increased from an already high level (90%) in 2017 to 95% in 2018.

However, a majority of businesses could be doing more to ensure their incident plans are fit for purpose through testing them regularly and subjecting them to external audits. Businesses need to understand the resources they would need in a crisis, what data they would need access to and what communications they will disseminate to customers, any victims, employees and their shareholders. These plans should be prepared in advance of a potential crisis and tested through exercising the process.

4.2. Cyber incident plans

A good cyber incident response plan will help a business to respond quickly to cyber threats, and subsequently limit long-term damage to the business's reputation. The vast majority of businesses (90%) already had a cyber incident plan in the 2017 Health Check, though this number has increased in 2018 to 95%.



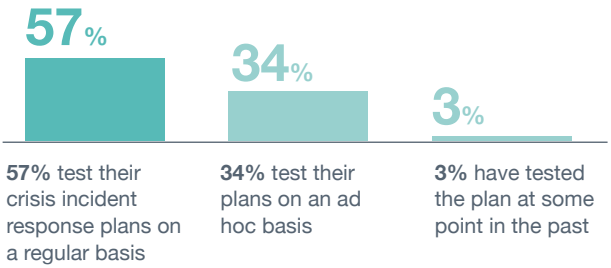
Businesses with a board that has a more comprehensive understanding of their assets and of the potential impact from the loss of or disruption to assets are not necessarily any more associated with having a standalone cyber incident plan than businesses where the board has a less comprehensive understanding, suggesting a range of other factors are involved in the decision to develop a standalone cyber incident response plan.

Rather concerningly, out of the 66 businesses, that report cyber threats are a high or very high risk for the board, there are three (4%) that do not have a cyber incident plan in place. These businesses and others in the same position are encouraged to develop cyber incident response plans.

4.2.1 Incident plan testing

Cyber threats evolve over time, and therefore it is important to test cyber incident response plans regularly to ensure they are fit for purpose and to ensure that everybody in the organisation understands their responsibility in case of an incident. Furthermore, businesses can seek advice on their cyber incident plan through an external audit.

Despite almost all businesses having a cyber incident plan, only just over half of businesses test their plans on a regular basis. Those that do not test plans regularly are at greater risk of longer-term damage to the business if a cyber incident were to occur.



Sector Focus

Businesses in the financial services sector are slightly more likely to test their plan more regularly, with 61% doing so compared to 49% in other sectors.

Most businesses use a combination of methods to assure that their incident response plans are fit for purpose. Half of businesses use internal audits to obain assurance their plans are fit for purpose, while a quarter of businesses use external audits. Other common methods cited by respondents include penetration testing, vulnerability testing, benchmarking, discussions with third party consultants and internal discussions with relevant members of staff.

"Our internal audit function supported by external subject matter experts are charged with assessing this. Our cyber security strategy has been reviewed by our auditors and a security specialist firm. We are currently in the process of having this year's cyber security strategy reviewed and benchmarked against our peers in the market by an independent external organisation."

Financial services business

"Regular quarterly reports on security strategy and incidents and outcome from Security Boards, regular crisis simulation and cyber specific crisis simulation (the next of which is scheduled for early 2019), external briefings to the board (e.g. from NCSC, MoD, external consultants), specific incident briefings (as appropriate) and regular audit of security methods and practices (previously along IAMM guidance)."

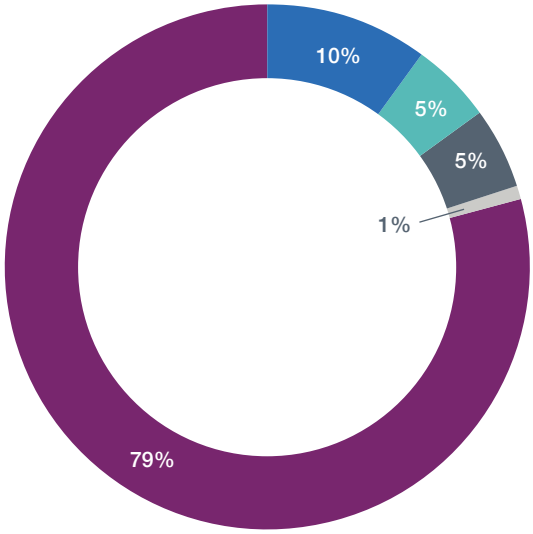
Industrial goods business

4.3. Board participation in crisis simulations

Crisis simulations are designed to enable participants to experience what it is like to respond to a sophisticated cyber attack, increasing their level of awareness and gauging their readiness to manage a cyber security incident.

Only around 1 in 5 boards of FTSE 350 businesses have undertaken a crisis simulation on cyber risk in the last 12 months. Although not directly comparable, it is worth noting that in the 2017 Health Check, 28% of businesses reported that the board had received either some training or comprehensive training to deal with a cyber incident in the previous 12 months.

Board involvement in a crisis simulation on cyber risk in the past 12 months



Response (n=93)

- Yes, as part of a cyber specific crisis simulation tailored to the organisation
- Yes, as part of a cyber specific crisis simulation exercise
- Yes, as part of a broader crisis simulation exercise
- Yes, as part of a Gold command level crisis simulation exercise
- No

Sector Focus

Out of the 18 businesses that reported board involvement in a crisis simulation exercise in the last 12 months, 10 are in the financial services sector and 5 are in the consumer services sector.

5. Supply chain risk management

The supply chain is increasingly becoming a target for cyber attacks, as identified in the NCA/ NCSC report "The Cyber Threat to UK business 2017,"[22] so it is important that boards are aware of the threat, and ensure appropriate measures are in place to minimise supply chain risks.

This section summarises the evidence arising from the 2018 Health Check in relation to:

- Whether boards recognise the risk associated with businesses in their supply chain, i.e. third-party businesses and businesses further down the supply chain;
- Whether businesses recognise the risks associated with software;
- How businesses are enforcing cyber security in their supply chain.

5.1. Summary

Recognition of cyber risks that arise from businesses in the supply chain is relatively high (73%). However, recognition of cyber security risks from businesses that are not directly contracted by the business (second tier or fourth party and beyond) is low (23% of businesses). Similarly, a majority of businesses (64%) do not recognise the risks associated with all types of software. Recognition of supply chain risks at the second-tier level are more likely in businesses where:

- The board rates their understanding of their business' information, data and systems as comprehensive or fairly comprehensive;
- The board assesses the risk of cyber security to be high or very high;
- The CISO reports to the board.

Businesses should use flow down requirements for minimum security standards in contracts with suppliers. Encouragingly, two thirds of businesses (67%) report that they use contractual terms as an enforcement mechanism with their suppliers.

22 https://nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file

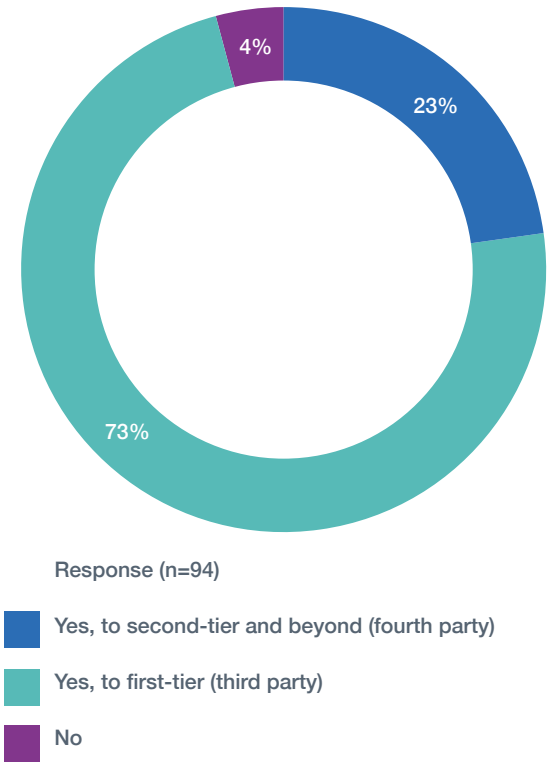
Advice

The NCSC has published a selection of illustrative real-world examples of supply chain attacks that outline the challenges organisations face, including the risks associated with third party software providers, website builders, and third-party data stores.[23] The NCSC has also published guidance proposing a set of 12 principles, designed to help businesses establish effective oversight of their supply chain.[24]

5.2. Recognition of supply chain risks

It is important that boards are aware of the threat of cyber risks arising though the supply chain given that it is increasingly becoming a target for cyber attacks. Whilst the majority of boards (73%) recognise the cyber risks that arise from businesses within its supply chains at a first-tier level (third parties), a much smaller proportion (23%) of businesses recognise the risk at a second-tier level (fourth party) and beyond. This means that three quarters (77%) of businesses do not recognise the risks associated with businesses in the supply chain with whom they do not contract directly.

Board recognition of the risk of cyber threats arising from businesses within its supply chain



23 https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks
24 https://www.ncsc.gov.uk/guidance/supply-chain-security

Businesses are more likely to recognise supply chain risks at the second-tier and beyond where:

- The board assesses the risk of cyber security to be high or very high compared to businesses where the board assesses the risk to be medium to low.

Board assessment of risk	Yes, to second-tier and beyond (fourth party)	Yes, to first-tier (third party)	No
very high or high (n=67)	27%	70%	3%
medium to low (n=27)	11%	85%	4%

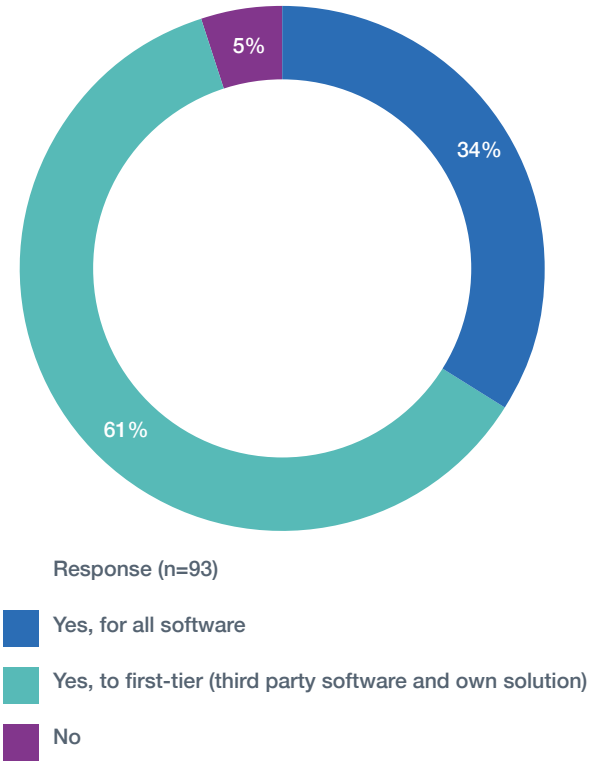
- The CISO reports to the board compared to businesses where the CISO does not report to the board.

Whilst there is a need for a majority of boards to recognise risks in the supply chain beyond the first-tier, the findings suggest those perceiving the risk of cyber threats in general as medium to low may be particularly vulnerable to risks in the supply chain.

5.3. Recognition of software risks

Whilst a large proportion of boards (61%) recognise the risks associated with the software it develops and maintains within the business and through third party businesses, only a third of businesses recognise the risk associated with ***all*** software used by third parties and beyond.

Board recognition of risks associated with software



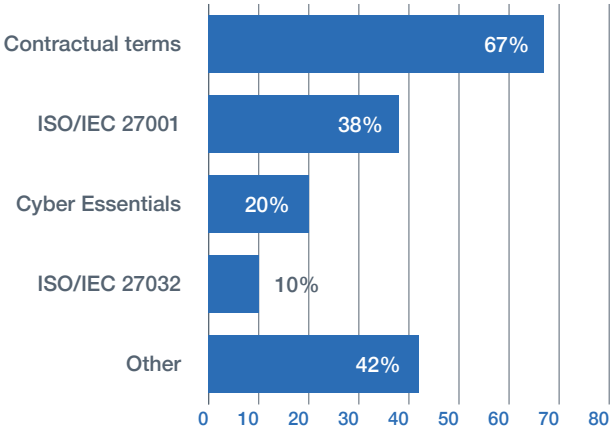
Businesses where the board assesses the risk of cyber security as high or very high are more likely to recognise the risks associated with all software as part of its cyber risk management.

Board assessment of risk	Yes, for all software	Yes, to first-tier (third party software and own solution)	No
very high or high (n=66)	39%	56%	5%
medium to low (n=27)	19%	74%	7%

5.4. Managing risks in the supply chain

Most businesses are using multiple frameworks to enforce cyber security in their supply chain, with contractual terms being the most commonly cited method used by businesses responding to the 2018 Health Check.

Frameworks used to enforce cyber security in the supply chain (multiple answers possible)



Of those that selected 'other', only a few specified the framework that they use. These include:

- Pre-contract due diligence
- National Institute of Standards and Technology
- Service Organisation Control 2 (SOC2) standards
- Customs-Trade Partnership Against Terrorism (C-TPAT)
- The Payment Card Industry Security Standard (PCI DSS)
- IEC 62443
- Defence Cyber Protection Partnership
- Joint Supply Chain Accreditation Register (JOSCAR)

Those that use ISO/IEC27001 and/or Cyber Essentials for managing their own cyber risk also use these standards to manage risks in their supply chain. However, contractual terms is the main way to manage the supply chain amongst this group of businesses.

Advice

Those who would like further information and guidance about managing risks in the supply chain should refer to the latest NCSC guidance on the subject.[25]

25 https://www.ncsc.gov.uk/guidance/supply-chain-security

Appendix A Resources

2018 FTSE 350 Cyber Governance Health Check
https://www.gov.uk/government/publications/cyber-governance-health-check-2018

Cyber Security Breaches Survey 2018
https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

NCSC Board toolkit
https://www.ncsc.gov.uk/collection/board-toolkit

NCSC 10 Steps to Cyber Security
https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

NCSC 10 Steps: A Board Level Responsibility
https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility

NCSC Principles of Supply Chain Security
https://www.ncsc.gov.uk/collection/supply-chain-security

NCSC Governance of Cyber Risk
https://www.ncsc.gov.uk/collection/risk-management-collection?curPage=/collection/risk-management-collection/governance-cyber-risk

NCSC Risk Management Collection
https://www.ncsc.gov.uk/collection/risk-management-collection

Cyber Essentials
https://www.cyberessentials.ncsc.gov.uk

The Cyber Threat to UK Business 2017-2018 NCSC Report
https://www.ncsc.gov.uk/cyberthreat

Appendix B 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

Consumer Services

Retailers
Travel and Leisure
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

Appendix C Respondent profile

Sectors

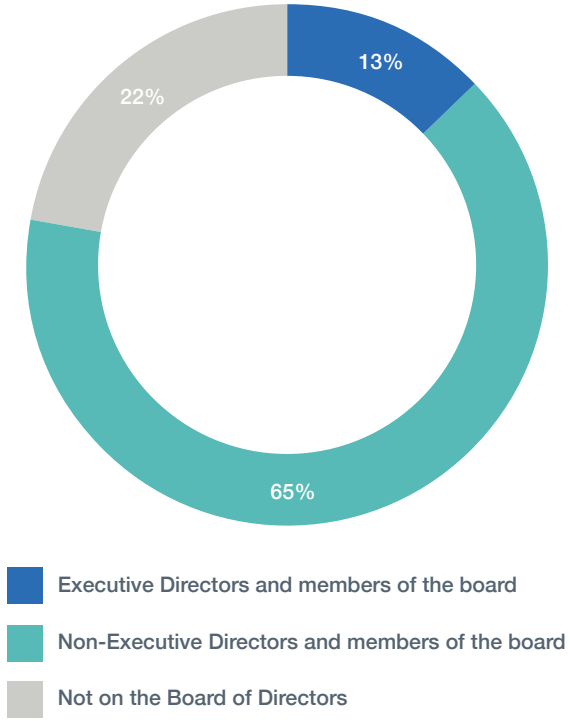
As per previous surveys, the largest number of responses are from the financial services sector (28% of all responses), followed by consumer goods (15%) and technology, communications and healthcare (14%) which is reflective of the sectoral breakdown in the population of FTSE 350 businesses.

The proportion of financial services businesses responding to the survey has increased year on year and increased five percentage points from 23% in 2017 to 28% in 2018. In contrast, the proportion of businesses responding from the real estate sector has generally decreased since 2014 and specifically declined since 2014, having decreased seven percentage points from 15% in 2017 to 8% in 2018.

Sector breakdown of respondents

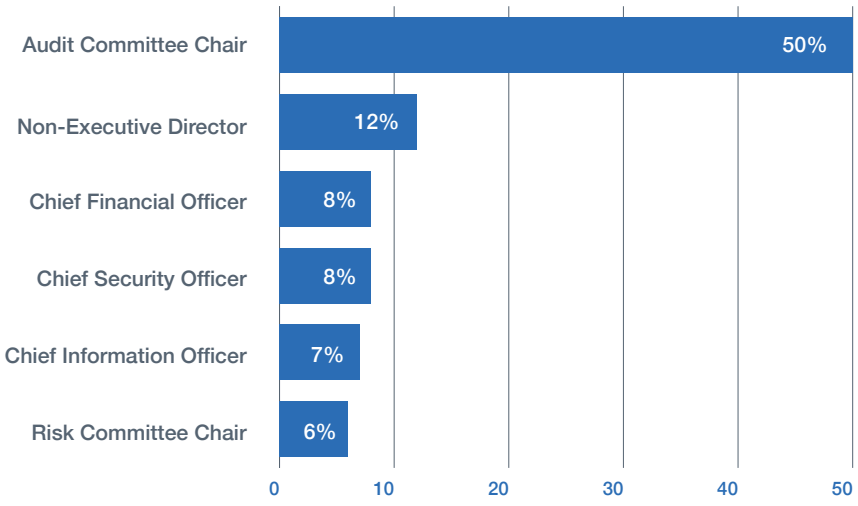
Sector	Percentage of respondents			
	2018	2017	2015/6	2014
Financial services	28	23	22	19
Consumer services (retail, travel and leisure)	13	17	14	15
Real estate and support services	8	15	12	17
Technology, communications and healthcare	14	13	14	10
Utilities and resources	11	9	10	9
Industrial goods and services	12	15	17	19
Consumer goods	15	7	11	12

Respondents' positions in their organisation (n=83)



- The proportion of Executive Directors that responded to the survey is a similar proportion to those that responded to previous surveys.
- The majority (7 out of 10) of Executive Directors and members of the board are the Chief Financial Officer, with the remaining respondents (3 out of 10) being the Chief Operating Officer.
- Almost all of the respondents that are a Non-Executive Director and member of the board are also the Audit Committee Chair (90%; 50 out of 55 Non-Executive Directors and members of the board).
- The majority of respondents that are not members of the Board of Directors were either Chief Information Security Officer (8 out of 20) or Chief Information Officer (7 out of 20).

Respondents' top 6 roles



Appendix D Methodology

Questionnaire

A number of changes have been made to the 2018 survey compared to previous iterations in order to make the questionnaire more robust and increase the validity of the data collected. The changes to the questionnaire mean that there are some limitations around the extent to which results can be compared to previous years. For example there are:

- New questions added to the 2018 survey, resulting in a lack of comparable data for these questions;
- Questions that are similar in terms of wording but the response scale has changed, e.g. three point scale to five point scale. Responses have been re-coded to fit into a similar scale, and a comparison has been made to previous surveys where relevant;
- The question wording and/or the responses have been changed and therefore direct comparisons cannot be made. However, in some cases qualitative comments have been made on how the findings compare to previous years.

Sample

The list of FTSE 350 businesses was sourced from the Telegraph and downloaded on 12th August 2018.[26] The list included all businesses that had been on the FTSE list within the previous 12 months. Only businesses that are audited by one of the four audit firms of Deloitte, EY, KPMG and PwC were invited to participate in the Health Check. A total of 367 businesses were invited to participate in the survey.

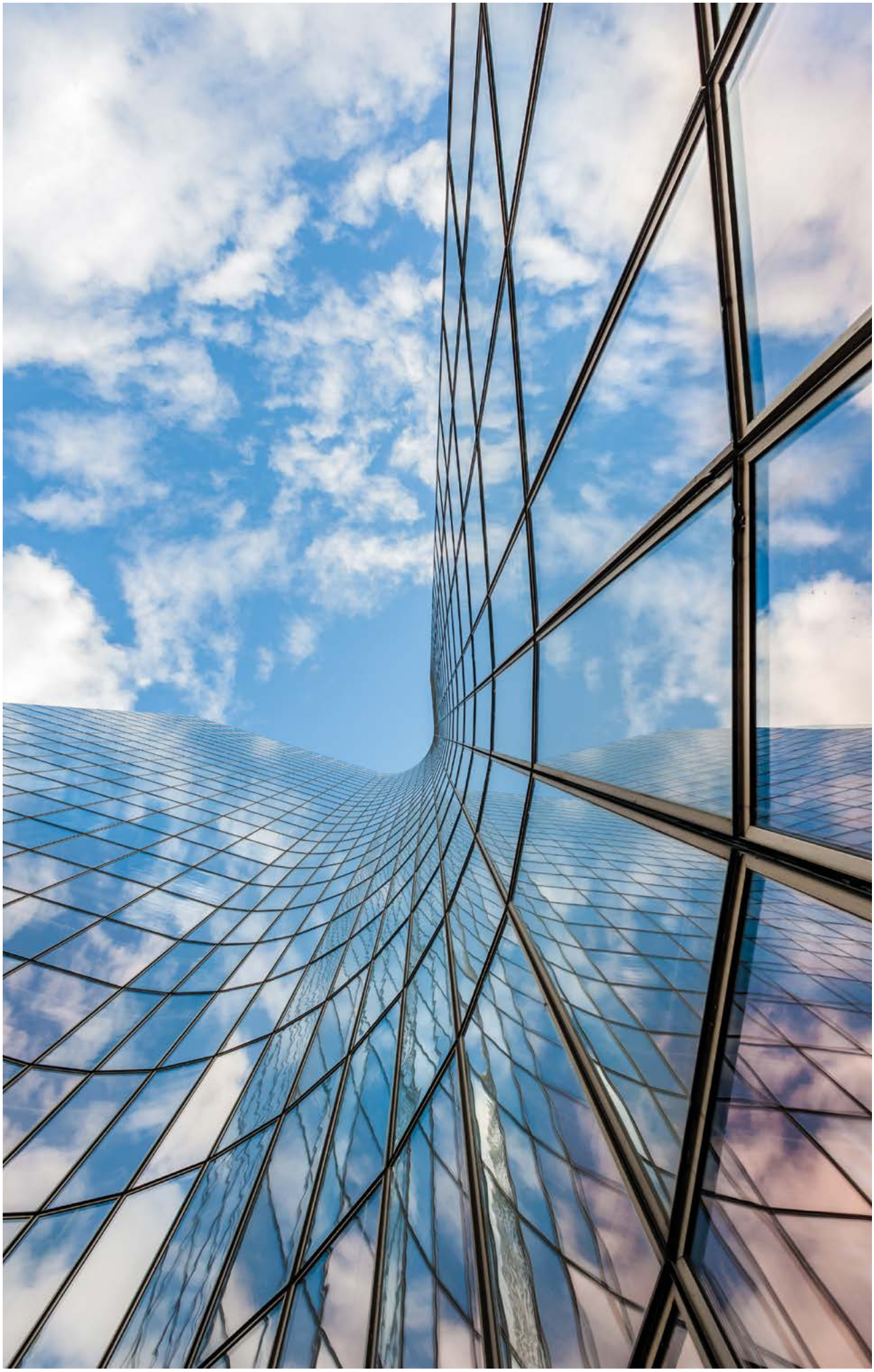
Method

The survey was set up on an online system which could be accessed by both audit firms and the FTSE 350 businesses. Audit firms approached the businesses that were their clients and encouraged them to complete the survey.

The survey was launched on 1st October 2018 and closed on 7th December 2018.

The work has been undertaken in compliance with ISO20252, the International Standard for Social and Market Research. Winning Moves is registered to the Standard.

26 This source (**http://shares.telegraph.co.uk/indices/?index=NMX**) was used as it allowed identification of businesses that had been on the FTSE 350 within the 12 months prior.



Department for
Digital, Culture,
Media & Sport

100 Parliament Street,
London, SW1A 2BQ,
United Kingdom

E: cybersecurity@culture.gov.uk

Administered by Winning Moves
on behalf of The Department for
Digital, Culture, Media & Sport

www.winningmoves.com