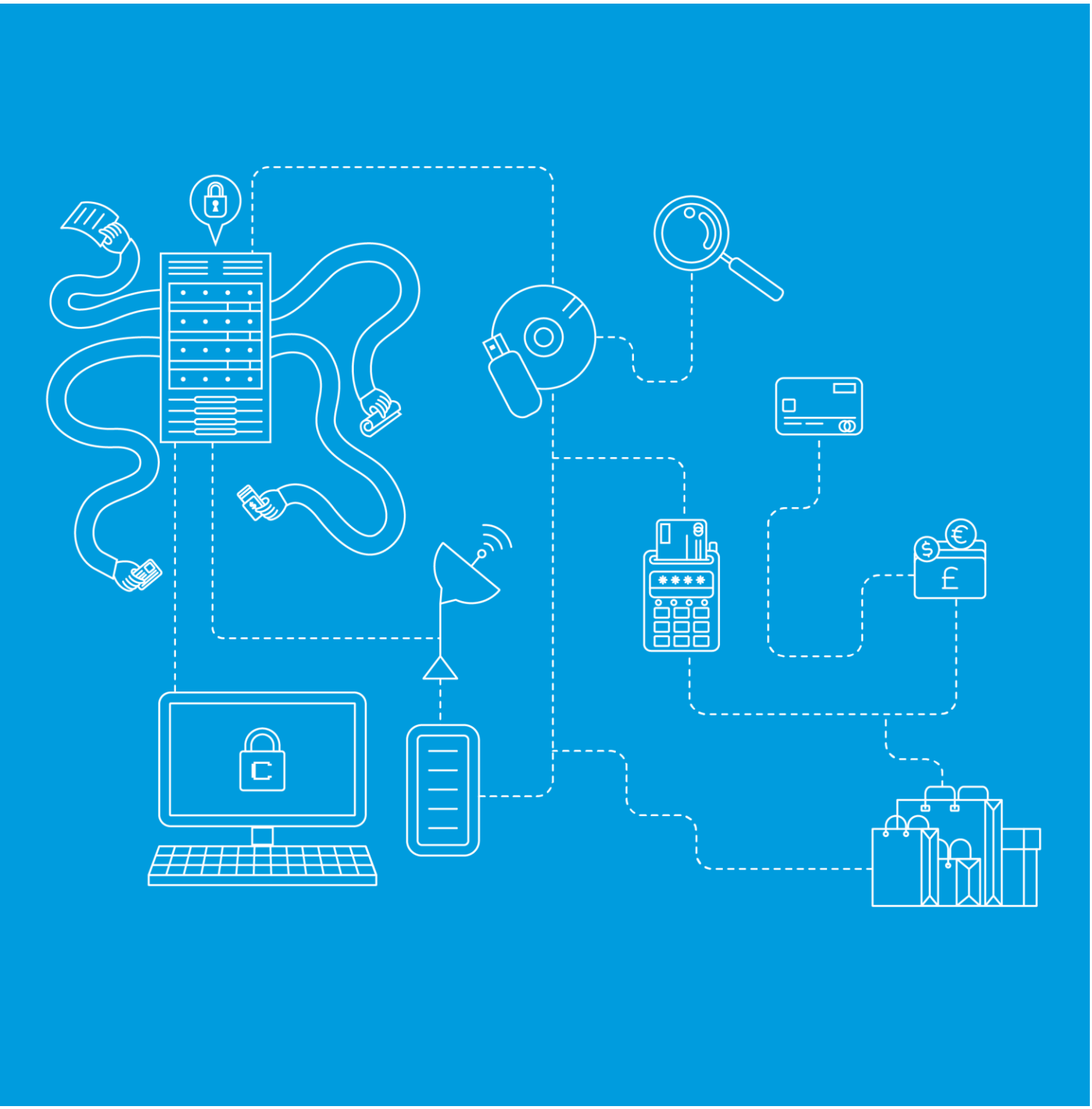


IMPACT OF THE GDPR ON CYBER SECURITY OUTCOMES

Final Report

August 2020

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

CONTENTS

EXECUTIVE SUMMARY

Context

The Department for Digital, Culture, Media and Sport (DCMS) 2016 Cyber Security Regulations and Incentives Review concluded that significant improvements in cyber risk management can be achieved through the implementation of the General Data Protection Regulation (GDPR).[1] This research, undertaken by RSM UK Consulting LLP (RSM), its subcontractor BMG Research Ltd (BMG) and strategic advisors Professor Martin Sadler (University of Bristol) and Dr Geraint Price (Royal Holloway, University of London), tests that conclusion. The findings are informed by a review of existing literature and both quantitative and qualitative fieldwork and analysis. It will inform the new review of cyber security incentives and regulations which is forthcoming.

Key findings

Existing literature on the impact of the NIS Regulations and the GDPR is scarce,[2] especially the impact of the GDPR on individual countries. Thus, firm conclusions on their impact on the UK specifically cannot be drawn from existing research. The results of our primary research, however, showed that most organisations had improved their cyber security when measured against the National Cyber Security Centre (NCSC) security outcomes.[3] The NCSC guidance describes a set of technical security outcomes that are considered to represent appropriate measures under the GDPR.

The primary research showed that, compared to 3 years ago, most organisations had increased their prioritisation of cyber security, including Board level prioritisation, as well as increasing their spend in this area. Most organisations had also introduced new or improved data protection and other cyber security policies, processes, procedures and technical controls, including measures to protect personal data and the systems that process it against cyber attack.

It was also encouraging to note that:

- most organisations had some form of cyber security strategy (69% of Board survey respondents)
- most Board members received updates on cyber security at least once a quarter (52%)
- where organisations had employees that specialised in data protection or cyber security, the majority had created one or more of these roles in the last 3 years (77% and 81% of respondents to the staff survey respectively)

While organisations identified a range of factors that had influenced these changes in their cyber security in the last 3 years, those linked to the GDPR were considered the most important (23% of the combined respondents to both the staff and Board surveys said the introduction of the GDPR was the most important factor). The vast majority of organisations (82%) also said that all of the changes in their cyber security were a result of the introduction of the GDPR at least to a small extent.

---

[1] *HM Government (2016) Cyber Security Regulation and Incentives Review*
[2] *The NIS Review, published on 28 May 2020, could not be included in this report due to timings.*
[3] *NCSC guidance on GDPR security outcomes: https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes (accessed May 2020)*

Data was also broken down into groups of specific interest for DCMS, chosen to understand in greater detail how the impact of the GDPR has varied across different contexts. This included those who had experienced a cyber security incident, completed a Data Protection Impact Assessment[4] (DPIA) or processed personal data, as well as large businesses,[5] large businesses with complex and interconnected supply chains,[6] Managed Service Providers (MSPs), Local Authorities (LAs) and non-profits providing important public services, Small or Medium-sized Enterprises[7] (SMEs) and across different industries. The research showed that impact of the GDPR did vary according to certain organisational characteristics. Organisations that had conducted a DPIA, those that processed personal data, and those that had experienced a cyber security incident were more likely to have improved their cyber security measures in the last 3 years. It is important to note, however, that there is some overlap between these 3 groups. This suggests that the GDPR has successfully encouraged improvements in cyber risk management for organisations that are within the scope of the regulation.

Experiencing an incident also appears to encourage organisations to act, suggesting that when organisations have knowledge of the damage a breach can have, they are more likely to make improvements. Giving organisations this insight in advance of an incident may help incentivise them to act in future, without having to experience an incident directly.

As with the existing research, we also found that improvements had not been realised equally across all aspects of cyber security. Although the primary research found that most organisations had improved their cyber risk management in the last 3 years, more improvements were reported in relation to governance, risk management, data security and systems security, while less change was evident in relation to procurement and supply chain risk management. Organisations were also more likely to have made changes to data protection than other aspects of cyber security.

This suggests that organisations could benefit from taking a resilience approach, emphasising the importance of improving the detect, respond and recover aspects of cyber security, as well as preventative aspects.

The changes made as a result of the GDPR had been sustained in the vast majority of organisations (84% of all respondents, including both the Board member and staff member surveys). Challenges to sustainability related to the ongoing costs associated with maintaining compliance and staff awareness of the GDPR as an ongoing issue. It may be too soon to determine whether these changes have resulted in a longer-term behaviour change or a cultural shift towards more robust practices. This is a potential area for further research in the future.

Where organisations had not changed their cyber security practices in the last 3 years, in the majority of cases, it was because they felt their existing measures were sufficient (61% of all respondents to both surveys). Interviewees were confident in their organisations' ability to manage risks, protect against attacks, detect threats and minimise the impact of an incident because they had robust policies and procedures in place, and their staff had appropriate cyber security expertise. It is possible, however, that for some organisations this confidence may be misplaced. They may still benefit from assistance in assessing their risk posture and the appropriateness of the measures they have taken.

---

[4] As required by the GDPR, where data processing was likely to result in a high risk to personal data
[5] Private sector organisations with 250 employees or more
[6] Private sector organisations in any industry with: 250 employees or more; a supply chain with more than 3 tiers of suppliers; and for whom the incapacitation of a main supplier by a cyber-attack for 48 hours would have a moderate or severe impact on their day to day business operations or service provision
[7] Private sector organisations with fewer than 250 employees

Some organisations reported detrimental impacts as a result of the GDPR:

- 50% of all respondents to both surveys said that the GDPR had led to excessive caution amongst staff in the handling of data
- 36% reported excessive focus on data protection to the detriment of other aspects of cyber security
- 27% reported excessive investment in cyber security, significantly beyond what is necessary
- 78% of Board members said that cyber security updates had become more focused on data protection than general cyber security

This suggests that organisations could benefit from guidance on the appropriate balance between data protection and other aspects of cyber security.

The evidence also suggests that the GDPR has not impacted all organisations equally. At an industry level:

- organisations in the finance and insurance industry were more likely than the average respondent to have made positive changes to their cyber security in the last 3 years – interviewees attributed this to the volume and nature of personal data that they hold, which could be more valuable to a potential attacker
- the GDPR appears to have been a greater influence on organisations providing public services - those in public administration and defence and those in health were both more likely than the average respondent to say the introduction of the GDPR was the most important factor (36% and 32% of respondents respectively, compared to 23% of all respondents to both surveys)
- organisations in finance and insurance; arts, entertainment, recreation and other services; wholesale and retail; education; health; and public administration and defence were more likely than the average respondent to have attributed all of the changes in their cyber security in the last 3 years to the GDPR (100%, 94%, 90%, 89%, 89% and 89% of respondents respectively said that all of the changes in their organisation's cyber security in the last 3 years were a result of the GDPR at least to a small extent, compared to 82% of all respondents to both surveys)

When considered by special interest group:

- large businesses with complex and interconnected supply chains were more likely to have made changes, particularly in relation to increasing their cyber security capacity and capability as a result of the GDPR than the average respondent- care should be taken when interpreting these findings as the base for this group was less than 100 respondents
- LAs/non-profit organisations providing important public services were more likely than the average respondent to have made changes and to rate 'the introduction of the GDPR' as the most important factor influencing these changes, which indicated that the GDPR had more of an impact on LAs/non-profits providing important public services than the average respondent
- large businesses were more likely than the average respondent to have provided new and improved data protection and specific cyber security training in the last 3 years, which indicates that the GDPR had led to improved staff awareness and training within large businesses
- SMEs were less likely to have made changes than the average respondent, which indicates that the GDPR had less of an impact on SMEs than the average respondent
- MSPs were less likely than other respondents to have changed their cyber security behaviour in the last 3 years, which indicates that the introduction of the GDPR had less of an impact on MSPs directly - however, most MSP interviewees reported that it had positively impacted their relationships with customers/clients

These variations by industry and type of organisation highlight the value of providing more tailored guidance and support, that reflects their different influences and motivations, as well as more clearly linking security outcomes to business goals.

1 INTRODUCTION

1.1 Purpose

RSM UK Consulting LLP (RSM), its subcontractor BMG Research Ltd (BMG) and strategic advisors Professor Martin Sadler (University of Bristol) and Dr Geraint Price (Royal Holloway, University of London), were commissioned by the Department for Digital, Culture, Media and Sport (DCMS) to research the impact that the introduction of the General Data Protection Regulation (GDPR) has had on incentivising organisations across the UK to improve their cyber security outcomes. This report summarises the findings of the literature review, as well as the quantitative and qualitative fieldwork.

1.2 Terms of reference

DCMS required research to deliver a better understanding of the impact of the GDPR and Network and Information Systems (NIS) regulations on organisational cyber security outcomes, including:

- a literature review of existing research in the subject area
- quantitative surveys of staff and Board members in a range of organisations to understand the impact that the GDPR has had on their cyber security outcomes
- qualitative interviews with staff and Board members to explore the findings of the quantitative survey in more detail

DCMS's stated key policy objectives for the latter part of the project were: to understand whether the GDPR regulations have had an impact on organisational cyber security outcomes, whether potential improvements have been sustained and whether the GDPR has engendered any unintended consequences.

The research requirements also specified that the survey should include a broad range of organisations including large businesses; large businesses with complex and interconnected supply chains; Managed Service Providers; and Local Authorities and non-profit organisations providing important or essential public services. In addition to this, it was specified that the methodology should be designed to capture and incorporate the views of staff and Board members involved in the implementation of the GDPR, where possible.

1.3 Research questions

The key research questions were:

1. Based on existing research in this subject area, what has been the impact of the GDPR and NIS Regulations on organisations' cyber security outcomes?
2. Have organisations across the economy improved their cyber risk management as a result of the GDPR (using the NCSC cyber security outcomes as criteria for assessing whether organisations have taken the necessary cyber security measures following the introduction of the GDPR)?
3. Have improvements been realised equally or partially across all aspects of cyber security (such as preventing disruption of services, protecting valuable non-personal data and protecting personal data)?
4. For those organisations that have taken appropriate action, has the impact been sustained over one year on from implementation?
5. Where organisations have not taken the actions advised by the NCSC, what are the reasons behind this?
6. Have there been any other/unintended consequences as a result of the introduction of the GDPR (such as prioritisation of data security leading to neglect of other important areas of cyber security)?
7. Has the GDPR improved Board level prioritisation of cyber security?
8. Has the impact of the GDPR varied by industry?

DCMS has a particular policy interest in the following groups:

- large businesses - any private sector organisation with 250 employees or more
- large businesses with complex and interconnected supply chains - private sector organisations in any industry with: 250 employees or more; a supply chain with more than 3 tiers of suppliers; and for whom the incapacitation of a main supplier by a cyber-attack for 48 hours would have a moderate or severe impact on their day to day business operations or service provision
- Managed Service Providers (MSPs) - an outsourced third-party company that manages and assumes the responsibility of a defined set of day-to-day management services to its customers[8]
- Local Authorities and non-profit organisations providing important public services that are not within the scope of the NIS Regulations (LAs/non-profits providing important public services)
- Small or Medium-sized Enterprises (SMEs) - any private sector organisation with fewer than 250 employees

Section 5 presents any variation in the survey responses of these groups, where there was a statistically significant difference.

[8] *MSPs were identified and targeted in our survey sample using Standard Industrial Classification (SIC) codes: 6209- Other information technology and computer service activities; and 6311- Data processing; hosting and related activities. in addition to these sic codes, respondents were asked whether their organisation built or operated outsourced information communication technology services to confirm they were a MSP*

1.4 Research overview

Section 2 of this report is based on a review of existing, external research. Sections 3 to 5 are based on the findings of our quantitative surveys and qualitative interviews of staff and Board members. Section 6 presents our conclusions against the research questions. A detailed methodology is included in Appendix A. Appendix B provides a breakdown of survey respondents based on key characteristics such as organisation size and industry. The survey questionnaires are included in Appendices D to G and the qualitative interview questions are shown in Appendix H.

Sections 3 and 4 summarise the survey and interview findings and present any variation in survey response where there was a statistically significant difference,[9] based on the following characteristics:

- type of respondent - staff and Board members
- industry group – agriculture, forestry and fishing; production; construction; wholesale and retail, repair of motor vehicles; transport and storage (including air transport); accommodation and food services; information and communication; finance and insurance; property; professional, scientific and technical; business administration and support services; public administration and defence; education; health; and arts, entertainment, recreation and other services
- whether or not the organisation processed personal data about consumers, service users or businesses or other organisations
- whether or not it experienced a cyber security incident in the last 3 years that caused disruption to day to day operation or service provision
- whether or not it had completed a Data Protection Impact Assessment (DPIA)

It should be noted that the latter 3 groups were not mutually exclusive (see Figure 1.1). Organisations that processed personal data about consumers, service users or businesses or other organisations were more likely to have completed a DPIA (53% of respondents to the staff survey) or experienced a cyber security incident (16%) than those that did not process personal data (40% and 9% respectively).

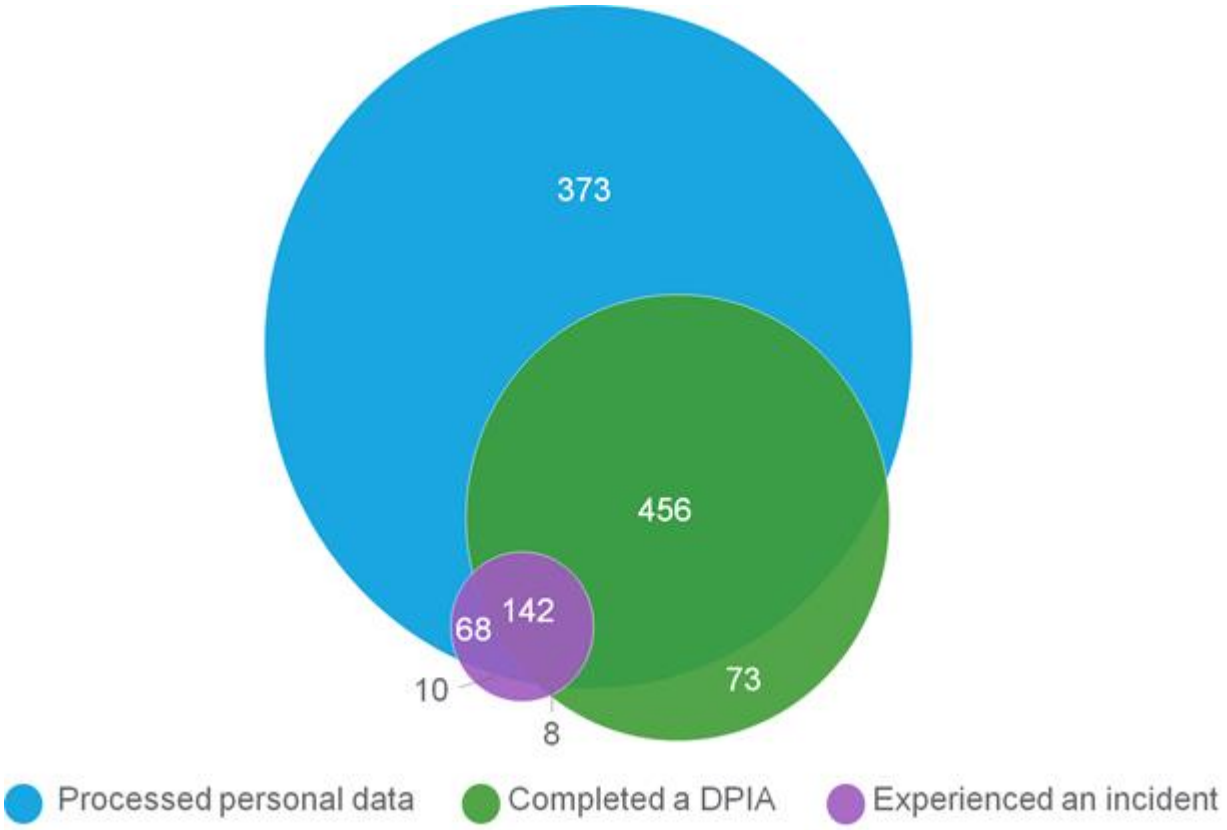
Throughout this report, participants in the quantitative survey are referred to as respondents, whilst participants in the qualitative interviews are referred to as interviewees.

The survey figures used throughout this report are based on the weighted base. The unweighted base has also been included for reference.

A number of survey questions were targeted at Board members only. Board members were a subset of total respondents. Due to the smaller number of responses within this group (104), responses to the Board member only questions have not been broken down any further.

[9] *Z-tests were performed on all questions and t-tests were performed on numerical data to 95% confidence level*

Figure 1.1: Relationship between respondents that had processed personal data, completed a DPIA and experienced a cyber security incident



Source: Staff/Board survey Q4/BQ2. Which of the following types of personal data, if any, does your organisation process? Q9/BQ7. Has your organisation experienced a cyber security incident which has caused disruption to your day to day business operations or service provision in the last 3 years? and Staff survey Q29. Has your organisation done one or more DPIA?
Unweighted Base: 1,130
Notes: The numbers presented represent the absolute number of respondents in each unique category, for example, 142 respondents processed personal data and experienced a cyber security incident and completed a DPIA.

The total number of responses achieved (1,233) was above target (1,170), resulting in a margin of error of +/-3% at the 95% confidence level. This means that we can be confident that the responses received are representative of the views of the wider population of organisations in the UK. Appendix B provides details of the profile of survey respondents. We also received sufficient responses from respondents with certain characteristics to allow us to generalise findings of these groups, including:

- private sector organisations - we can be confident that the responses received are representative of the views of the wider population of UK businesses (to +/-4% margin of error at the 95% confidence level)
- SMEs - we can be confident that the responses received are representative of the views of the wider population of SMEs in the UK (to +/-4% margin of error at the 95% confidence level)

A third of respondents to the staff survey were IT/Cyber professionals (378 respondents).

The vast majority of respondents to both the staff and Board surveys (95%) had heard of the GDPR before taking part in the survey. However, it is concerning that 5% of respondents had not heard of the regulation. Respondents in LAs/non-profits providing important public services and large businesses were more likely to have heard of the GDPR than SMEs (100% of LAs/non-profits providing important public services and 99% of large businesses compared to 94% in SMEs).

Respondents in the education, public administration and defence, and health industries were also more likely to state they had heard of the GDPR (100% of education, 99% of public administration and defence and 99% of health industry respondents). Moreover, organisations that processed personal data, experienced a cyber security incident or completed a DPIA were more likely to have heard about the GDPR (97% of organisations that processed personal data answered yes compared to 90% of those that did not, 98% of organisations that had experienced an incident compared to 95% of all respondents, and 98% of organisations that had completed a DPIA compared to the average). There was no statistically significant variation in response by IT or cyber security professionals.

A total of 67 respondents to the quantitative survey took part in the qualitative interviews. This included a diverse mix of interviewees based on the key characteristics of interest (see Appendix A: Methodology). The frequency of the qualitative responses is described using the following scale:

- 'none' or 'no' = 0 interviewees (or 0%)
- 'minority' = 1-16 interviewees (or 1-24%)
- 'some' = 17-33 interviewees (or 25-49%)
- 'most' = 34-49 interviewees (or 51-74%)
- 'vast majority' = 50-66 interviewees (or 75-99%)
- 'all' = 67 interviews (or 100%)

1.5 Limitations

In some instances, the number of responses received from respondents with certain characteristics was below target, resulting in a higher margin of error (6-10%). These included:

- large businesses
- large businesses with complex and interconnected supply chains
- MSPs
- LAs/non-profits providing important public services

Due to the size of the sample it was not possible to achieve responses that would be representative of the views of the wider population by industry.

This means that, while total responses and responses for private sector organisations and SMEs can be generalised, the survey findings for large businesses, large businesses with complex and interconnected supply chains, MSPs, LAs/non-profits providing important public services and by industry are indicative and should not be generalised to represent the wider population.

2 LITERATURE REVIEW

Summary

The infancy of the GDPR[10] and NIS[11] regulations meant there was limited academic, peer-reviewed literature on how the GDPR impacted cyber security behaviours and actions of organisations, particularly UK specific literature. The NIS Review, published on 28 May 2020, could not be included in our review due to the timings. Thus, firm conclusions on the impact of these regulations on the UK specifically cannot be drawn from existing research.

The existing research showed that organisations had invested more in cyber security, and many companies had reported improvements to cyber security policies, since the introduction of the GDPR. However, it was less clear if the correct governance structures were in place (such as appropriate data protection and information security policies and processes) or if organisations were prioritising cyber security in the same way as other business risks. While there have been noted improvements in technical solutions such as device encryption, there was limited evidence of management training or incident response planning and regular testing and updating of processes.

Though the GDPR impacted on information security in relation to data protection, there was no robust evidence of impact on other areas of cyber security to the same extent. In addition, the 2020 Cyber Security Breaches Survey[12] suggested that there was still more that organisations could do to improve their cyber security (such as audits, cyber insurance, supplier risks and breach reporting).

Larger companies were better prepared for the introduction of the GDPR due to having more resources and management infrastructure to support compliance measures. However, there was a lack of evidence on if, how or why the impact of the GDPR varied across different industries.

There were mixed views on Board level prioritisation of cyber security. Some research suggested there had been improvements in the management of cyber security and Board level discussions. Other reports suggested that Boards were continuing to neglect cyber security as a business risk, indicating that more could be done to understand how to change these mindsets.

There was limited secondary evidence on whether the impacts would be sustained. It was too soon to determine whether changes had resulted in longer-term behaviour change or a cultural shift towards more robust practices.

We sought to address the gaps in the existing research through our primary research.

[10] *The GDPR came into force in May 2018*
[11] *The NIS Directive came into force in May 2018*
[12] *DCMS, Ipsos MORI and University of Portsmouth (2020) Cyber Security Breaches Survey 2020*

2.1 Introduction

This section provides an overview of existing, external research on how the NIS Regulations and the GDPR have impacted the cyber security behaviours and actions of organisations. The DCMS 2016 Cyber Security Regulation and Incentives Review[13] concluded that significant improvements in cyber risk management could be achieved through implementation of the GDPR. This was to be supplemented by a number of measures to more clearly link data protection with cyber security, including closer working of the Information Commissioner's Office (ICO) and the NCSC. It also noted that the government would regularly review the need for regulation and further activity in this area. The findings in this section provide an overview of the evidence available to date exploring whether the expectation that the implementation of the GDPR would improve cyber risk management has been met. A detailed methodology for the literature review is included in Appendix A.

2.2 Context

The GDPR – the GDPR came into force in May 2018. It was incorporated into the Data Protection Act 2018, which replaced the 1998 Act, and places greater obligations on how organisations handle personal data. The GDPR applies to 'personal data', meaning any information relating to an identifiable person who could be directly or indirectly identified, particularly by reference to an identifier. The GDPR requires personal data to be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organisational measures are used. The GDPR applies to processing carried out by organisations operating within the European Union (EU). It also applies to organisations outside the EU that offer goods or services to individuals in the EU.[14] The GDPR has been incorporated into UK data protection law via the EU Withdrawal Act.

The GDPR includes a maximum fine of up to 4% of annual global turnover or €20 million – whichever is greater – for organisations that infringe its requirements. Supervisory authorities such as the UK's ICO can also take a range of other actions, including:

- issuing warnings and reprimands
- imposing a temporary or permanent ban on data processing
- ordering the rectification, restriction or erasure of data
- suspending data transfers to third countries

The NIS Regulations – the NIS Regulations came into force on 10 May 2018. They provide legal measures aimed at boosting the overall level of security (both cyber and physical resilience) of network and information systems for the provision of certain digital services (online marketplaces, online search engines, cloud computing services) and essential services (transport, energy, water, health, and digital infrastructure services). The NIS Regulations continue to apply in the UK following its exit from the EU and will continue to apply following the end of the transition period.

Difference between the GDPR and the NIS Regulations– the GDPR and NIS Regulations address different issues: the GDPR relates to the processing of personal data, while the NIS Regulations relate to the security of network and information systems. However, there were similarities between them: the GDPR has provisions relating to security and most organisations covered by the NIS

[13] *HM Government (2016) Cyber Security Regulation and Incentives Review*
[14] *https://ico.org.uk/for-organisations/in-your-sector/business/guide-to-the-general-data-protection-regulation-gdpr-faqs/ (accessed November 2019)*

Regulations are likely to also be data controllers or data processors. The NIS Regulations apply to fewer organisations than the GDPR, such as operators of essential services (OES) or relevant digital service providers (rDSP).[15] Further information comparing the GDPR and the NIS Regulations can be found in Section 2.3.8.

2.3 Literature review findings

The key findings from the literature review are summarised under the following headings which reflect the key objectives of this research.

2.3.1 Improvement in cyber risk management[16]

Research completed by RSM[17] in 2019 found that 68% of businesses across Europe[18] reported investment in cyber security due to the GDPR requirements; 62% agreed that the GDPR compliance had resulted in more investment in cyber security; and 51% agreed that the GDPR had made their business safer from cybercrime. UK respondents reported that:

- 75% of companies from the UK reported investment in cyber security due to the GDPR requirements
- 52% agreed that the GDPR compliance had resulted in more investment in cyber security
- 42% agreed that the GDPR had made their business safer from cyber crime

In addition, a 2017 survey[19] of 1,300 executives, representing a range of industries and organisations worldwide, found a correlation between being prepared for the GDPR and strong cyber risk management practices. It found that organisations preparing for, or compliant with, the GDPR were over 1.5 times more likely to have reported an increase in cyber risk management spending, as well as the adoption of more cyber risk management practices overall. When comparing businesses that had no GDPR plan with those that said they were compliant or were developing a GDPR plan:[20]

- 38% compared to 56% said that they encrypted organisational desktop and laptops, something explicitly encouraged by the GDPR
- 17% compared to 56% said that they have engaged in penetration testing, something strongly implied by the GDPR[21]

The same study[22] also found that respondents who reported developing a plan or being fully compliant with the GDPR rules were more than 3 times as likely to have adopted some cyber security measures, and more than 4 times as likely to have adopted some cyber resiliency measures compared to those who had not started planning. Respondents with a higher level of the GDPR readiness were more than 1.5 times as likely to have purchased or strengthened their cyber risk insurance.

This 2017 survey concluded that cyber risk management was both a cause and consequence of the GDPR compliance, noting that while practices such as cyber incident planning and cyber insurance

---

[15] https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/ *(accessed November 2019)*
[16] *Cyber risk management refers to the process of identifying, analysing, evaluating and addressing the cyber risks in an organisation*
[17] *RSM (2019) Catch 22: Digital transformation and its impact on cybersecurity*
[18] *RSM's 'Catch 22: Digital transformation and its impact on cybersecurity' report comprises responses to a range of questions posed to 597 companies in 33 European countries, spanning multiple industries and sizes, with recorded turnovers varying from less than €30 million to over €300 million. 56% of the respondents are on the management board with a further 31% reporting directly to the board.*
[19] *Marsh and McLennan (2017) GDPR Preparedness: An Indicator of Cyber Risk Management*
[20] *ibid*
[21] *Article 32 of the GDPR (General Data Protection Regulation) requires organisations to implement technical measures to ensure data security. It highlights the need for "a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".*
[22] *Marsh and McLennan (2017) GDPR Preparedness: An Indicator of Cyber Risk Management*

were not explicitly required, they helped firms to meet the GDPR 72-hour data breach notification guidance. It also suggested that the adoption of cyber risk management measures made GDPR compliance easier and the process of achieving compliance had spurred organisations to adopt and improve cyber security, cyber risk mitigation, and cyber resiliency practices. [23]

Additional research[24] based on a 2019 global cyber risk perception survey found that there had been an increase in the percentage of businesses ranking cyber risk as a top 5 concern for their organisation, increasing from 62% in 2017 to 79% in 2019. The same research noted that this does not necessarily equate to improved cyber risk management. The research found that only 38% of respondents cited the GDPR as a driver for any area of increased cyber risk investment and that organisations' confidence in their ability to manage the risk declined.

Other recent research noted that changes in cyber risk management could have, in part, been attributed to the introduction of the GDPR. For example, the 2020 Cyber Security Breaches Survey[25] found that 38% of businesses and 42% of charities in the UK had made changes to their cyber security policies and processes as a result of the GDPR. The changes reported were, in some cases, attributed to the GDPR. However, there was no data from the current literature that evaluated the impact of the GDPR in a UK context.

Research[23] also highlighted that there were other drivers of change in cyber security risk management, investment and behaviours. This is evident in a 2019 global cyber risk perception survey[26], which found that cyber incidents were the main trigger for increases in cyber risk management investments. This research identified that organisations may have had a reactive approach to cyber security, with regulations such as the GDPR being reported as a less common reason for increasing investment in cyber security. Specifically, it reports that the following factors impacted on an organisation's planned budget allocation in relation to risk management[27]:

- a cyber incident/attack on their organisation (64%)
- news of a cyber incident/attack on another organisation (46%)
- adoption of new or emerging technologies (43%)
- new or changing regulations (such as the EU GDPR) (38%)
- change in leadership within the organisation (19%)
- required by a key customer (12%)
- experiencing a merger or acquisition (7%)

Conclusion

The research suggests that the combination of the GDPR and other drivers has led to organisations prioritising and investing more in cyber security. This has led to self-reported improvements in the cyber security policies of many companies, including developing procedures for reporting cyber-attacks, adopting cyber risk management measures, and implementing cyber resilience measures. Although many of the research sources referred to a global context, rather than a specifically British

---

[23] Marsh and McLennan (2017) GDPR Preparedness: An Indicator of Cyber Risk Management
[24] Marsh and McLennan (2019) 2019 Global Cyber Risk Perception Survey. This report is based on findings from the 2019 Marsh Microsoft Global Cyber Risk Perception Survey administered between February and March 2019. Overall, 1,500 business leaders participated in the global survey, representing a range of key functions, including risk management, information technology/information security, finance, legal/compliance, C-suite officers, and boards of directors. Survey respondents were based in Latin America and Caribbean; Europe; United States and Canada; Asia and Pacific; Middle East and Africa
[25] DCMS, Ipsos Mori and University of Portsmouth (2020) Cyber Security Breaches Survey 2020. Findings from this survey are based on a random probability telephone survey of 1,348 UK businesses and 337 UK registered charities was undertaken from 9 October 2019 to 23 December 2019.
[26] Marsh and McLennan (2019) 2019 Global Cyber Risk Perception Survey
[27] Percentage selecting as a driver for any area of increased cyber risk investment. Base: All answering & stating they plan to invest more, excluding 'don't know' responses: n=615 (2019)

one, the findings were indicative of changes within UK businesses as the impact of the GDPR is likely to be felt similarly across the EU.

2.3.2 Rationale for not taking the actions advised by the NCSC

The NCSC and the ICO developed guidance[28] which provides an overview of what the GDPR stipulates about security and describes a set of technical security outcomes that represent appropriate measures under the GDPR. The technical security outcomes[29] were designed to provide detail on how to comply with principle (f) of the broader principles of the GDPR.[30] Specifically it provides guidance in relation to:

- managing security risks
- protecting personal data against cyber attack
- detecting security events
- minimising the impact

However, several recent surveys found that many companies had not yet carried out actions in relation to these areas.

A 2019 report on data protection and privacy by Capgemini[31] found that GDPR compliance had not met initial expectations. This finding was based on a survey of 1,100 compliance, privacy, data protection and IT executives across 10 countries (including the UK) and 8 industries. The report noted that, while 78% of executives surveyed about the GDPR in 2018 expected to be compliant, when it came into effect in May 2018 only 28% reported being compliant with the GDPR. A further 30% reported that they were close to complete compliance, however were still resolving remaining issues. It reported that non-compliance was a worldwide, cross-industry issue as none of the countries or industries surveyed matched the aspirations they had in 2018.

The report also highlighted that achieving and maintaining compliance posed significant challenges, including:

- acquiring and training new talent - two-thirds of organisations had hired full-time employees to support GDPR compliance efforts
- upgrading IT systems - over a third pointed to legacy IT systems as a major challenge to the GDPR compliance
- updating policing and procedures - almost all organisations (90%) had received data subjects' queries related to the GDPR and 13% had received more than 5,000 queries in the past year

Research by Crown Records Management[32] in 2019 also suggested that over 75% of organisations had faced challenges in complying with the GDPR requirements. Its survey of 103 senior managers, IT and data professionals[33] found that only 23% of businesses rated their compliance capabilities around the GDPR as 'very good'. The research found that almost 50% of respondents felt that their organisation's data storage methods required improvement and attention (46%), followed by data retrieval processes (44%) and data storage and protection (43%).[34]

---

[28] https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes *(accessed October 2019)*
[29] *The outcomes intend to provide a common set of expectations that can be met, either through following existing guidance, using particular services or, development of a bespoke approach*
[30] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
[31] *Capgemini (2019) Championing Data Protection and Privacy: a source of competitive advantage in the digital century*
[32] https://www.govtechleaders.com/2019/05/29/organisations-are-still-struggling-with-gdpr-compliance/ *(accessed October 2019)*
[33] *The survey was conducted by Sapio Research in March 2019. They interviewed 103 senior managers, IT and data professionals in companies with over 250 employees*
[34] https://thefintechtimes.com/gdpr-compliance-one-year/ *(accessed October 2019)*

In addition, a 2019 survey of 1,400 SMEs by Shred-it[35] found that smaller firms generally had a 'positive understanding and engagement with the principles of the GDPR'. However, while 72% of UK SMEs stated they were 'very aware' of the GDPR requirements, 60% reported that the changes to data protection law have had a 'slight' or 'no' impact on their business, and only 32% of SMEs said the GDPR has had a 'great' or 'considerable' impact.

It has been hypothesised that the main reason for non-compliance with the GDPR was that many organisations, especially SMEs, lacked the resources to become compliant and have struggled to do so. As a result, these organisations have not been able to realise the full security outcomes envisaged by the NCSC. It should be noted that the existing literature does not address this issue. We have, therefore, undertaken primary research to address this gap.

Conclusion

There were several difficulties in complying with the GDPR, including: challenges with updating policies, costs of upgrading IT systems, and difficulties with acquiring new talent to support GDPR compliance. This has resulted in many organisations not achieving the NCSC's GDPR security outcomes. However, due to the relatively recent implementation of the GDPR, there was a lack of large-scale statistical surveys measuring compliance/improvements, or lack thereof, for UK-based organisations against the GDPR cyber security outcomes.

2.3.3 Impact on all aspects of cyber security

DCMS's 2019 annual Cyber Security Breaches Survey[36] of UK organisations found that while the GDPR had played an important role in 'raising the floor', it may have unintentionally made some organisations think about cyber security almost exclusively in terms of data protection. It also suggested that advances in the number of staff attending training on cyber security may have been due to the uptake of the GDPR training where the actual cyber security content could have been relatively small. Specifically, it notes:

> *'when asked about seeking out cyber security training…several participants discussed their GDPR-related training, suggesting that they saw the two topics of the GDPR and cyber security as interlinked. In fact, the GDPR currently seemed to be a more significant strategic priority for some of the participating organisations than cyber security on its own terms'.*

[35] *The independent survey of 1,439 SMEs was commissioned to gather insight on attitudes to data protection. The survey included unprompted questions and covered a range of businesses in specific market industries across the United Kingdom with 85% having 10 to 49 employees. https://www.shredit.co.uk/en-gb/resource-centre/infographics/gdpr-compliance-survey (accessed October 2019)*

[36] *DCMS, Ipsos Mori and University of Portsmouth (2019) Cyber Security Breaches Survey 2019*

Cyber security can be broken down into several different elements, including[37]:

- application security – the security of applications and software downloaded onto a computer or network
- information security - safeguarding sensitive information from illegitimate access, usage, revelation, disruption, alteration, reading, inspection, damage or recording. The GDPR is an example of information security
- network security - comprehensive security policies and provisions adopted in an adaptive and proactive manner by the network administrator for thwarting and monitoring unauthorised access
- disaster recovery/business continuity planning – the procedures in place for a business to continue operating both during and after a cyber-attack
- end user education – educating technology users so that they are aware of best practice to protect themselves from a cyber-attack

There were mixed views on the extent to which the GDPR had led to improvements across all of these areas.

Research by Capgemini[38] in a mix of 10 European, American and Asian countries found that the GDPR had led to greater than expected improvement in internal processes. This found that 91% of executives from compliant organisations reported improvements in the processes for handling and managing personal data. It reported that a number of areas had benefited, including IT transformation, cyber security practices, and organisational change.

However, the 2020 Cyber Security Breaches Survey [39] of UK organisations found that (in line with the previous year), despite most organisations having technical controls such as secure configuration, firewalls and malware protection, they were less likely to have formal cyber security policies, particularly covering home working or what can be stored on removable devices.

Further research highlighted an increased focus on information security. The ICO had seen the number of reports from all data controllers quadruple following the introduction of the GDPR.[40] This suggests an increased focus on detecting and reporting cyber security incidents relating to personal data and was likely due to the new data breach notification requirements under the GDPR[41] (links to NCSC security outcome C: detect security events). However, the ICO noted that more than 82% of the personal data breaches reported to it since the GDPR had taken effect required no action from the organisation[42] and initially highlighted a problem of 'over-reporting' in September 2018.[43]

This is supported by a 2019 global cyber risk perception survey[44] which found there may be differences between an organisation's perception of cyber risk as a top-priority and their approach to managing it. Results from this survey suggested that organisations were focusing more on technology and prevention than on prioritising the time, resources, and activities needed to build cyber resilience.[45] As a result, organisations believed they could eliminate or manage their cyber risk primarily through technology, rather than through planning, transfer and response measures.

---

[37] http://www.crossdomainsolutions.com/cyber-security/elements/ *(accessed October 2019)*
[38] *Capgemini (2019) Championing Data Protection and Privacy: a source of competitive advantage in the digital century*
[39] *DCMS, Ipsos Mori and University of Portsmouth (2020) Cyber Security Breaches Survey 2020*
[40] HTTPS://WWW.PUBLICTECHNOLOGY.NET/ARTICLES/NEWS/GDPR-BLAMED-DOUBLING-WHITEHALL'S-RECORDED-DATA-BREACHE *(accessed October 2019)*
[41] *This requires organisations to report incidents within 72 hours of becoming aware of them*
[42] https://www.pinsentmasons.com/out-law/news/report-flags-gdprs-impact-on-data-breach-notification-*(accessed October 2019)*
[43] *Ibid*
[44] *Marsh and McLennan (2019) 2019 Global Cyber Risk Perception Survey*
[45] *Cyber resilience is the ability to prepare for, respond to and recover from cyber-attacks.*

Specifically, it was found that:

- 88% said information technology/information security was 1 of the 3 main owners of cyber risk management, followed by executive leadership/Board (65%) and risk management (49%)
- only 17% of executives say they spent more than a few days on cyber risk over the past year
- 30% of organisations reported having used quantitative methods to express cyber risk exposures, up from 17% in 2017
- 83% had strengthened computer and system security over the past 2 years, however less than 30% have conducted management training or modelled cyber loss scenarios
- among areas in which firms plan to increase risk management spending over the next 3 years, 67% cited cybersecurity technology/mitigation

This research also suggested that only a small number of organisations took actions to create a strong cyber security culture with appropriate standards for governance, prioritisation, management focus and ownership, suggesting 'this places them at a disadvantage both in building cyber resilience and in confronting the increasing cyber challenges of a changing technology and supply chain environment'.[46]

Research on the cost of cyber crime[47] also found that there had been a consistent increase in spending on prevention/mitigation of cyber attacks or advanced threats to their cyber security ('containment spend'). This was due to the expansion of cybersecurity, compliance and regulatory requirements, such as the GDPR.

Furthermore a study on GDPR preparedness,[48] before the regulation was implemented, identified that cyber risk management activities with higher participation levels were cyber security measures focused on defence. For example, of the businesses who indicated they were preparing for the GDPR or were already compliant with the GDPR:

- 67% stated that their organisation had conducted a cyber security gap analysis
- 56% reported their organisation conducted penetration testing
- 66% reported their organisation implemented or enhanced phishing awareness training for employees

Conclusion

The research suggests that the GDPR has led to an improvement in internal data handling and management processes and more companies were investing in activities that lessen the severity of cyber attacks. However, it is also suggested that a focus on GDPR compliance has led to, in some cases, a disproportionate emphasis on information security and data protection, as opposed to other cyber security measures.

2.3.4 Extent to which the impact had been sustained

There is limited evidence regarding whether the reported impacts of the GDPR on cyber security practices have, or will be, sustained. It is too soon to determine if the change in cyber security measures being reported has resulted in a longer-term behaviour change or cultural shift towards more robust practices. For example, a recent article noted that 'genuine cyber-resilience comes from corporate muscle-memory, which is developed from incident response planning with legal,

[46] *Marsh and McLennan (2019) 2019 Global Cyber Risk Perception Survey*
[47] *Accenture Security (2019) Cost of Cybercrime. Based on interviews with 2,647 senior leaders from 355 companies across 11 countries in 16 industries*
[48] *Marsh and McLennan (2017) GDPR Preparedness: An Indicator of Cyber Risk Management*

communications and IT security stakeholders, and which is sustained by testing and updating processes on a regular basis.'[49]

This is also reflected in the Capgemini research[50], which highlighted that the effort to maintain data protection and privacy compliance is ongoing. This research noted that 'the GDPR is not something you will ever be done with. It is something that you need to work on continuously.' One of the findings from the Cyber Security Breaches Survey 2020[51] was that continuous improvement is not guaranteed. It was clear from the findings of the 2020 survey that the GDPR had played a major role in getting organisations to review and update their cyber security policies and processes. The 2020 survey showed that, while many of these improvements had been maintained, they were not being enhanced. Particular areas identified that require improvements were supplier risk, audit processes and the reporting of breaches.[52]

Conclusion

Due to the relatively recent implementation of the GDPR, it is not yet possible to comment on if and/or how any impacts (intended and unintended) on cyber security will be sustained. As an enforcement mechanism, the GDPR will continue to mature over time, and it is possible new or different impacts could emerge. Further research will be required to determine if its intended outcomes have been achieved and to measure its sustained impact.

2.3.5 Variation by industry

The GDPR incorporated a broad range of obligations[53] on organisations processing the personal data of EU residents. Changes introduced by the legislation include accountability and governance, data processing principles, privacy rights of individuals, obtaining consent, transferring data and data breach notifications. The impact of the GDPR has varied across different industries and size of companies.

Industry

Recent research[54] on the impact of the GDPR on the financial services industry in EU countries stated that these businesses had found compliance easier than businesses in other industries. It suggests that this was due to a history of complying with strict privacy and data protection rules set by financial regulators, which required a strategic approach and detailed procedures. Key findings from this research included:

Executive management/Board involvement – the executive management and supervisory boards in the finance and insurance industry tended to be better at monitoring their data protection policies and GDPR compliance procedures than their counterparts in other industries. This was in part due to the strict requirements of a heavily regulated industry, where huge fines can be imposed on those that transgress.

Financial services sub-industries – the research suggests that the GDPR has had less of an impact on the investment management industry compared to the retail banking and insurance industries. This was due to many investment management businesses operating mainly, or only, on

---

[49] https://www.information-age.com/cyber-security-breaches-fall-123481460/ *(accessed October 2019)*
[50] *Capgemini (2019) Championing Data Protection and Privacy: a source of competitive advantage in the digital century*
[51] *DCMS, Ipsos Mori and University of Portsmouth (2020) Cyber Security Breaches Survey 2020*
[52] *Ibid*
[53] *The GDPR includes 99 articles setting out the rights of individuals and obligations placed on organisations covered by the regulation*
[54] *Deloitte (2019) After the dust settles: How Financial Services are taking a sustainable approach to GDPR compliance in a new era for privacy, one year on. This report is based on interviews with data privacy specialists in Deloitte, financial services organisations, and the UK's Information Commissioner's Office. It also draws on Deloitte's November 2018 survey, A new era for privacy: GDPR six months on. The 2018 survey elicited responses from 1,100 data protection specialists working in companies across all private sectors in 7 EU countries (UK, Spain, Italy, Netherlands, France, Germany and Sweden)*

a business-to-business (B2B) basis, rather than on a business-to-consumer (B2C) basis, and therefore holding less personal data. The exceptions were the wealth management sub-industry of investment management, which dealt with high-net worth individuals and businesses that held vast amounts of personal data, including special category data. It was unclear from the literature if this was because fewer changes to cyber risk management were required to be compliant with the GDPR.

Company size

Size of the organisation may also influence the impact of the GDPR. A piece of research[55] on the GDPR as an indicator of risk management, which surveyed over 1,300 executives, found respondents at larger organisations were more likely to have reported higher levels of the GDPR compliance. This was in part due to having more resources to invest in compliance, as well as having the management infrastructure to support compliance measures. In addition, the report suggested that many larger companies also had significant operations in the US, where data protection practices and breach notification policies had been aggressively articulated and enforced for several years. As a result, they were more likely to have a robust compliance infrastructure already in place and could more easily adapt them to meet the demands of the GDPR.

This was also supported by findings in the eighth annual Advisen Information Security and Cyber Risk Management survey[56] (mainly of US businesses). It found that 49% of large companies made changes to their cyber security controls as a result of the GDPR, compared with just 28% of middle market companies. When asked the primary reason for purchasing cyber insurance, 7 times as many large companies as middle market companies cited regulatory interpretation or uncertainty (for example, the GDPR).[57]

Conclusion

Current research indicated that the impact of the GDPR has varied across industries, with some such as the finance and insurance industry having existing regulatory requirements that may have made it easier to comply. In addition, larger companies were more likely to be compliant due to having more resources and a greater infrastructure to support this.

2.3.6 Impact on Board level prioritisation of cyber security

Findings from the literature suggested that the GDPR had improved Board level prioritisation of cyber security. However, in some instances, governance and ownership of cyber security still resided with those in information technology and information security roles. This suggested that the organisation's response to cyber risks had grown from a technical perspective, rather than a strategic one.

The FTSE 350 Cyber Governance Health Check 2018[58] completed a survey with 94 UK companies[59] listed in the FTSE 350 and concluded that the GDPR had increased the attention Boards give to cyber risk. It found that 77% of businesses reported Board discussion and management of cyber risk had increased since the introduction of the GDPR, and more than half (55%) of these businesses had increased measures as a result. It also noted that businesses introducing increased measures

---

[55] Marsh and McLennan (2017) GDPR Preparedness: An Indicator of Cyber Risk Management
[56] Advisen (2018) Information Security and Cyber Risk Management: The eighth annual survey on the current state of and trends in information security and cyber risk management. Note: The majority of respondents to this survey were from the United States (79 percent), followed by Europe (10 percent), and North America outside the U.S. (4 percent).
[57] It should be noted that the US insurance market is more developed, which may also be a driver for uptake
[58] HM Government (2019) FTSE 350 Cyber Governance Health Check 2018
[59] The survey sample in 2018 is broadly representative of the population in terms of business activity sector, 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. The majority of respondents were Non-Executive Directors and member of the board

in response to the 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.

Research[60] on GDPR preparedness globally also highlighted that 'in many organisations, [the] GDPR has become a flashpoint, focusing senior leadership attention on a broader, more strategic view of cyber risk management.'

Following the introduction of the GDPR, a 2019 survey of senior business decision makers within enterprise financial organisations in the UK[61] highlighted that large fines had impacted on Board level prioritisation of cyber security. It noted that approximately a third of companies (32%) referenced the GDPR fines as being the primary reason for an increase in Board level involvement and/or provision for IT security spending.

Nevertheless, research completed by RSM[62] with companies across Europe suggested that there remained a gap in senior management engagement and prioritisation of cyber security. This research found that there was a lack of discussion around the risks at Board level, as well as ambiguity over who is responsible for cyber security in the organisation. It found that:

- 65% of businesses said cyber security needed to be discussed more at senior management level
- 59% of businesses stated that once they had experienced a breach, cyber security became more of a priority for senior management
- 54% of businesses noted that the threat of cyber crime and the need for increased security was only occasionally discussed at Board level

It also suggested that often senior management did not see the need for investment in cyber security, believing that, as they have yet to experience a breach (as far as they are aware), it will not happen.

Moreover, 2019 research by Grant Thornton[63] found that more than 60% of the companies it surveyed[64] stated no Board member had specific responsibility for cyber security. In approximately the same proportion of companies, the Board did not undertake a regular formal review of cyber security risks and management.

This is further supported by a 2019 global cyber risk perception survey[65] which found that while cyber risk ranks high among organisational priorities, 'the fact that IT is named as a primary owner nearly twice as often as risk management points to a continuing, mistaken view of cyber risk as primarily a technology issue, rather than a critical business risk that merits a strategic enterprise risk management approach'. This indicated that more research could be done to better understand how to change these mindsets at a senior management level.

Conclusion

There were mixed views on whether the GDPR has improved Board level prioritisation of cyber security. While there is research to suggest the GDPR has increased Board level focus on cyber risk, in part due to the large fines associated with non-compliance, many Boards do not yet undertake

---

[60] *Marsh and McLennan (2017) GDPR Preparedness: An Indicator of Cyber Risk Management*
[61] *HTTPS://WWW.CLEARSWIFT.COM/ABOUT-US/PR/PRESS-RELEASES/HIGH-PROFILE-GDPR-FINES-HAVING-GREATEST-IMPACT-ON-UK-CYBER%20SECURITY-SPEND (October 2019})*
[62] *RSM (2019) Catch 22: Digital transformation and its impact on cybersecurity*
[63] *Grant Thornton (2019) Cyber security: the board report. How boards can reduce the impact of cyber-attacks on business*
[64] *The research was undertaken as part of Grant Thornton's International Business Report, which surveys around 10,000 businesses annually across more than 30 economies. Fieldwork is undertaken on a biannual basis, and online and telephone interviews are conducted with board and senior leaders, not limited to but including: chief executive officers, managing directors and chief financial officers.*
[65] *Marsh and McLennan (2019) 2019 Global Cyber Risk Perception Survey*

regular reviews of cyber security as it is not viewed as business risk. Further work may be needed to identify if Board engagement on cyber security/data security increases or decreases in future.

2.3.7 Unintended/other consequences

Qualitative findings from the 2019 Cyber Security Breaches Survey [66] noted the GDPR has led some organisations to frame cyber security largely in terms of avoiding personal data breaches. As a result, it suggested that some organisations may be less focused on other kinds of breaches or attacks and have a narrower set of technical controls in place.

In addition, research by RSM[67] spanning 33 EU countries noted that pressure to meet complex requirements had resulted in 'GDPR fatigue' among some companies. It suggested that as companies became overwhelmed by information and demands on what they have to do, many reverted to previous working practices. This may also have resulted in businesses (especially those in unregulated industries) taking a more 'tick box' approach to 'getting the job done', resulting in less effective protection and a false sense of security.

This research[68] also highlighted that another potential issue with the GDPR is its 'one-size-fits-all approach'. As a result, many requirements have been left open and too broad, leaving businesses more vulnerable. Furthermore, this research[69] found that, while 62% of businesses invested more in cyber security in preparation for the GDPR, 49% did not believe it had made their business safer and 26% did not believe that, a year on from the GDPR deadline, their business was fully compliant.

However, research[70] has also noted that investment in data privacy created business value beyond compliance and has become an important competitive advantage for many companies. It found that GDPR-ready companies had benefited from their privacy investments in a number of tangible ways, including:

- shorter sales delays due to customers' privacy concerns (3.4 weeks vs. 5.4 weeks)
- being less likely to have experienced a breach in the last year (74% vs. 89%)
- when a breach occurred, fewer data records were impacted (79k vs. 212k records) and system downtime was shorter (6.4 hours vs. 9.4 hours) - this meant that the overall costs associated with these breaches were lower (only 37% of the GDPR-ready companies had a loss of over $500,000 last year vs. 64% of the least GDPR ready)

Research by Capgemini[71] has also found that organisations who identified as compliant with the GDPR experienced benefits beyond those directly linked to data privacy:

- 81% said that the GDPR has had a positive impact on the organisation's reputation/brand image, with one business noting 'customers do recognise and appreciate the level of effort and impact the GDPR compliance brings with it'
- 84% said trust had increased
- 76% had seen a revenue increase, with strong performance driving benefits such as greater customer loyalty and increases in online purchasing

---

[66] *DCMS, Ipsos Mori and University of Portsmouth (2019) Cyber Security Breaches Survey 2019*
[67] *RSM (2019) Catch 22: Digital transformation and its impact on cybersecurity*
[68] *Ibid*
[69] *Ibid*
[70] *CISCO (2019) Maximizing the value of your data privacy investments: Data Privacy Benchmark Study. Cisco's Data Privacy Benchmark Study utilises data from Cisco's Annual Cybersecurity Benchmark Study, a double-blind survey completed by more than 3200 security professionals in 18 countries and across all major industries and geographic regions*
[71] *Capgemini (2019) Championing Data Protection and Privacy: a source of competitive advantage in the digital century*

Research on cyber risk management and resilience[72] proposed that the introduction of the GDPR has had an impact on the cyber security practices of businesses outside of the European Union. It suggested that regulators in Asia have become more transparent about their growing cyber threats and malicious data breaches in response to the GDPR, to more accurately reflect the cyber threat level in the region. For example, it noted that Hong Kong issued a circular to inform the public of the possible impacts of a large-scale cyber-attack, while Singapore released a factsheet for organisations to highlight the implications of the GDPR on their businesses.[73,74]

Other Asian regulators had also embraced the GDPR to learn and reflect for reforms. Parts of the data protection regulations in Thailand, India and China are thought to have been modelled after the GDPR, while several legal terms were directly drawn from the GDPR, such as 'right to be forgotten' in Indonesia and 'data portability' in the Philippines.[75,76]

Conclusion

There have been both positive and negative unintended consequences of the GDPR. The research suggested compliance has had a positive impact on business reputation and has increased customer trust, improved customer satisfaction, strengthened employee morale and has had a positive impact on revenue. However, in some cases it has led to companies viewing cyber security solely in terms of personal data and information security. In addition, it is suggested that approximately only a quarter of businesses viewed themselves as compliant, as many businesses became indifferent and reverted to previous working practices.

2.3.8 NIS Regulations

Literature on the impact of the NIS Regulations in the public domain was extremely limited. The Post-Implementation Review of the NIS Regulations was published in May 2020, which was too late to be included in this literature review.

Research to date has highlighted how the GDPR and NIS Regulations could differ and/or complement each other in their aims to strengthen cyber security and safeguard data protection, as illustrated in Figure 2.1.

Organisations that were required to report under the NIS Regulations will mostly also have been subject to reporting requirements of the GDPR. However, the reporting regime of the NIS Regulations has a different focus to the requirement to notify personal data breaches under the GDPR. Importantly, the GDPR and NIS Regulations have used different criteria to establish what might be considered appropriate technical and organisational measures and so the possible impacts may differ.[77] In addition, the NIS directive has been implemented differently in different member states, unlike the GDPR which is in many ways uniform across the EU.

---

[72] *FireEye and Marsh & McLennan Insights (2019) Advancing Cyber Risk Management: From Security to Resilience*
[73] *Office of the Privacy Commissioner for Personal Data (May 25, 2018). EU General Data Protection Regulation (GDPR), as quoted in FireEye and Marsh & McLennan Insights (2019) Advancing Cyber Risk Management: From Security to Resilience*
[74] *Personal Data Protection Commission Singapore (2017). European Union General Data Protection Regulation Factsheet for Organisations, as quoted in FireEye and Marsh & McLennan Insights (2019) Advancing Cyber Risk Management: From Security to Resilience*
[75] *Mark Innis (January 25, 2017). Indonesia: New Regulation on Personal Data Protection, as quoted in FireEye and Marsh & McLennan Insights (2019) Advancing Cyber Risk Management: From Security to Resilience*
[76] *Damian Domingo O. Mapa (2018). Mapping the Philippine Data Privacy Act and GDPR: A White Paper from the EITSC, as quoted in FireEye and Marsh & McLennan Insights (2019) Advancing Cyber Risk Management: From Security to Resilience*
[77] *https://www.kemplittle.com/blog/interaction-between-the-gdpr-and-the-nis-directive/ (accessed November 2019)*

Figure 2.1: Comparison of the GDPR and NIS Regulations

GDPR	Area	NIS Directive
Personal Data Security Protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data	**Scope**	**Network Security** Achievement of high level of security of network and information systems within the Union to boost the overall level of cybersecurity for EU Member States
Applies to any person or entity processing personal data related to the offering of goods and services or to the monitoring of their behaviour	**Target**	Security and notification requirements apply to **operators of essential services** and **digital service providers**
Rights of the data subject Obligations of data controllers Rules for transferring personal data	**Highlights**	**Obligations on designated Operators of Essential Services (OES) and relevant Digital Service Provider (rDSP).** Obligation for Member States to define: a **national strategy** and to designate competent authorities, **single points of contact** and computer security incident response teams (**CSIRTs)** Establishment of **Cooperation Group** and **CSIRTs Network**
✔Report breaches to supervisory authority without delay ✔In some cases the data subjects (individuals) need to be informed too	**Notification Requirements**	Incident reporting to the Competent Authority by: ✔Operators of **essential services** (energy, transport, health, water, digital infrastructure) ✔Providers of **digital services** (online marketplaces, online search engines, cloud computing services)
Up to £17 million or 4% of annual global turnover	**Penalties**	Member States shall set penalties that are effective, proportionate and dissuasive

Source: European Court of Auditors (2019) Challenges to effective EU cybersecurity policy

3 CHANGES IN CYBER RISK MANAGEMENT

Summary

The majority of organisations have improved their cyber security measures. In the last 3 years, most organisations have increased the prioritisation of cyber security and investment in this area. They had also introduced new or improved data protection and cyber security policies, processes, procedures and technical controls. However, there appeared to be a greater focus on governance, risk management, data security and system security than other aspects of cyber security. This suggests that organisations could benefit from improving their cyber resilience and the 'non-preventative' aspects of cyber security. It is concerning, however, that a minority of organisations were not giving cyber security the strategic focus required. Raising awareness of the business benefits of improved cyber security could help to address this issue.

Most organisations said that the changes made as a result of the GDPR had been sustained (84%). Further research is required to determine whether these changes have resulted in a longer-term behaviour change or a cultural shift towards more robust practices.

The survey showed that organisations that had experienced a cyber security incident were more likely to have made improvements than those that had not experienced an incident. The same can be said for organisations that had conducted a DPIA or those that processed personal data. This indicates that more changes were made in organisations where the GDPR was applicable. It also suggests that organisations that are not in scope of the regulations, or those that think they are not in scope, could benefit from greater insights into real-life examples of the impact of a breach or encouraging the use of Business Impact Assessments and consideration of impact tolerances.

There was also some variation in response by industry - organisations in the finance and insurance industry were more likely than other respondents to have made positive changes to their cyber security in the last 3 years. Interviewees said this was due to the volume and nature of personal data that they hold. This highlights the benefit of tailoring guidance and interventions by industry, taking account of differences in motivation and influences.

Findings in relation to potentially detrimental consequences of the GDPR were mixed. The majority of respondents did not think that the GDPR had led to excessive investment in cyber security (60%) or excessive focus on data protection (54%). However, a substantial proportion of respondents did report these negative impacts (27% and 36% respectively). This suggests that organisations could benefit from further guidance on the appropriate balance between data protection and other aspects of cyber security.

3.1 Context

The GDPR became enforceable in the UK in May 2018. We have, therefore, gathered data on changes made by organisations in the last 3 years in order to compare what was happening in 2020 to what was in place before the GDPR came into effect. The quantitative survey focused on the changes organisations had made in relation to the NCSC guidance on the GDPR security

outcomes,[78] in order to understand whether organisations across the UK had taken the necessary measures to improve their cyber risk management following the introduction of the GDPR. We also considered changes in cyber security expenditure in the last 3 years and the extent to which changes had been made across all aspects of cyber security and were being sustained. The qualitative interviews focused on the reasons why changes had been made, or not made.

Note: While total responses can be generalised, survey findings by industry are indicative and should not be generalised to represent the wider population.

3.2 Manage security risk

Organisations have appropriate organisational structures, policies and processes in place to understand, assess and systematically manage security risks to personal data.
(Source: NCSC)

3.2.1 Governance

Organisations have appropriate data protection and information security policies and processes in place. If required, records of processing activities are maintained and a Data Protection Officer is appointed.
(Source: NCSC)

We explored changes in governance in relation to:

- prioritisation of cyber security
- cyber security policies
- cyber security strategies
- Board level awareness of cyber security
- use of the NCSC Board toolkit
- changes to Board updates on of cyber security
- staffing

Overall, based on the findings presented below, governance of cyber security appears to have improved in the last 3 years.

3.2.1.1 Prioritisation of cyber security

Board prioritisation

Approximately half of respondents to the Board survey (46%-54%) reported an increase in the Board's prioritisation of the various aspects of cyber security governance in the last 3 years (see Figure 3.1). However, between 38% and 47% said it had remained the same.

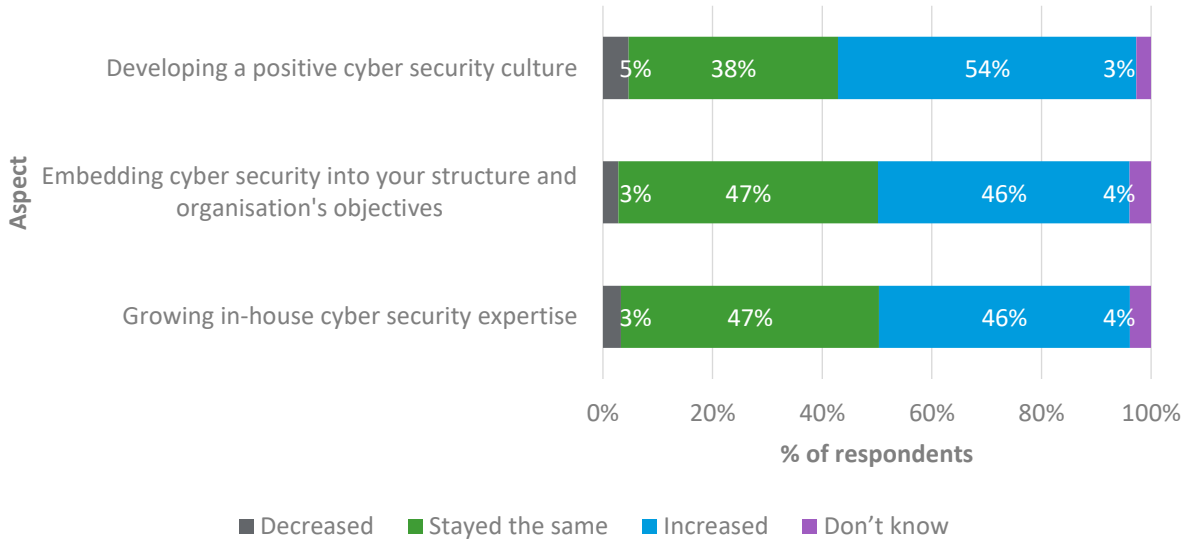
Due to the smaller number of responses within this group (104), responses to the Board member only survey questions have not been broken down by industry, experience of cyber security incident or whether they processed personal data or completed a DPIA.

In all cases, the qualitative interviewees reported that increases in Board prioritisation were driven by a desire to be compliant with the GDPR and to avoid financial penalties for non-compliance. The

[78] *NCSC guidance on GDPR security outcomes: HTTPS://WWW.NCSC.GOV.UK/GUIDANCE/GDPR-SECURITY-OUTCOMES (accessed May 2020)*

increasing awareness and prevalence of cyber attacks was also a factor. Interviewees said that the prevalence of cyber attacks had led to concern that their organisation would be targeted if they did not increase their prioritisation of cyber security. Some Board members reported that the reason for increasing their prioritisation of cyber security was because increasing awareness of cyber security risks had led to demands from their clients that their personal data be protected and stored safely. Some of the Board members interviewed reported that the prioritisation of cyber security in their organisation had not changed, because it was already high.

Figure 3.1: Changes in Boards' prioritisation of cyber security governance in the last 3 years

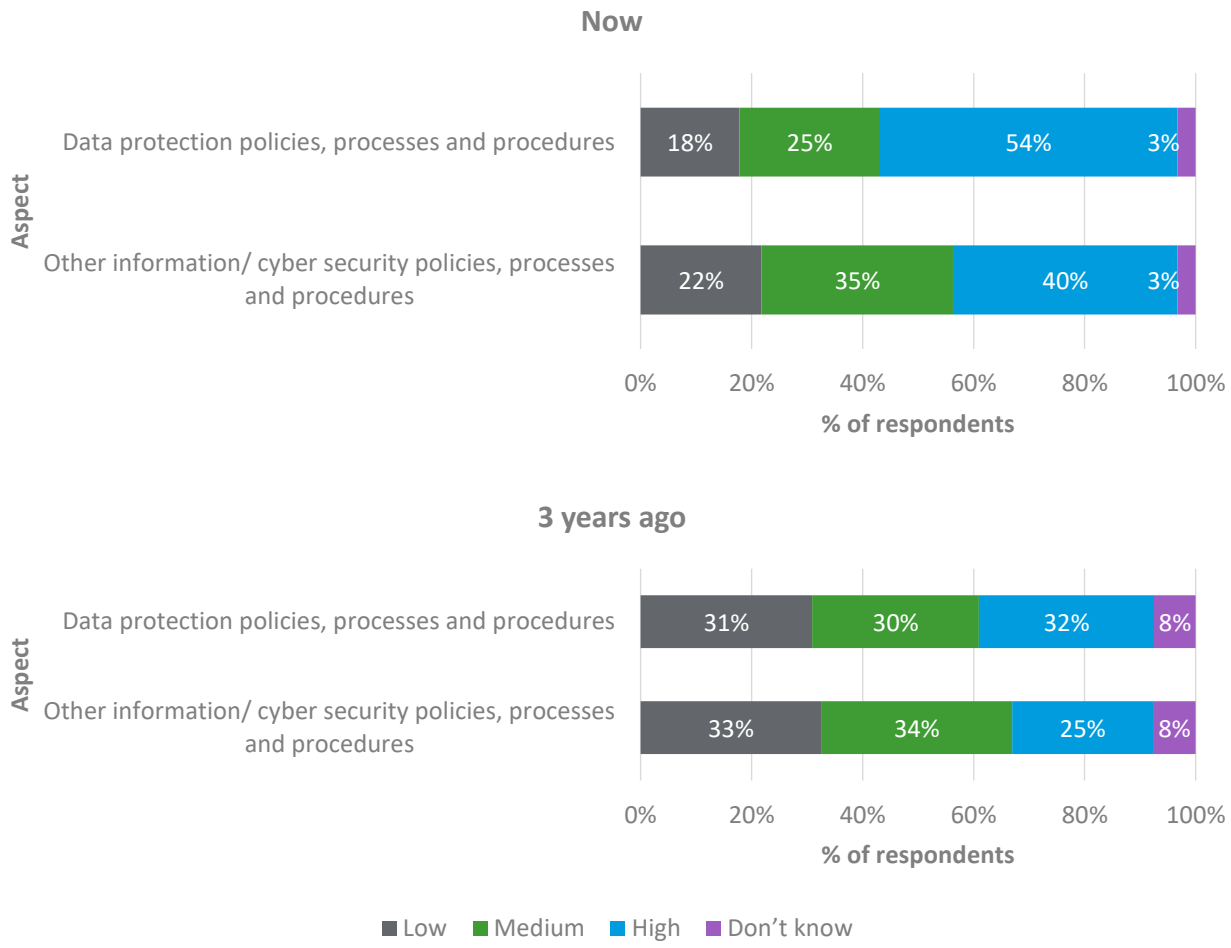


Source: Board survey BQ23abc. In the last 3 years, has the Board increased, decreased or given the same prioritisation to the following aspects of cyber security?
Weighted Base: 164
Unweighted Base: 104

Priority of policies, processes and procedures now compared to 3 years ago

More respondents to the staff survey rated cyber security policies, processes and procedures as a high priority within their organisation now compared to 3 years ago (see Figure 3.2). Fewer rated them as a low priority now compared to 3 years ago. The most common reason given by interviewees for this increase in priority was so that the organisation would be compliant with the GDPR. Another reason given by some interviewees was that it was clear that cyber security risks were increasing, as more cyber attacks were being reported. Therefore, increasing the priority of cyber security policies, processes and procedures was necessary to increase their organisations ability to protect themselves from a cyber attack. The interviewees that reported no change in priority felt that they were already mostly compliant with the GDPR.

Figure 3.2: Priority of cyber security policies, processes and procedures



Source: Staff survey Q24ab. Are the following aspects of cyber security a high, medium or low priority for your organisation...A. Now; B. 3 years ago.
Weighted Base: 1,069
Unweighted Base: 1,129

There was some variation in response by industry and by certain organisational characteristics. Where these variations were statistically significant, they are summarised below.

Organisations that had experienced a cyber security incident (62%) were more likely to rate data protection policies, processes and procedures as a high priority now than those that had not experienced an incident (52%). Organisations that had conducted a DPIA or processed personal data were more likely to rate both data protection and other information/cyber security policies, processes and procedures as a high priority now, as were respondents who were IT or cyber security professionals.

Box 1: Proportion of respondents that rated policies, processes and procedures as a high priority now by organisational characteristic

- 62% of respondents that had experienced a cyber security incident rated data protection policies, processes and procedures as a high priority now, compared to 52% of those that had not experienced an incident
- 64% of respondents that had conducted a DPIA rated data protection policies, processes and procedures as a high priority now, compared to 37% of those that had not conducted a DPIA
- 57% of respondents that processed personal data rated data protection policies, processes and procedures as a high priority now, compared to 37% of those that did not process personal data
- 61% of those who were IT or cyber security professionals rated data protection policies, processes and procedures as a high priority now, compared to 51% of those who were not IT or cyber security professionals
- 49% of those that had done a DPIA rated other information/cyber security policies, processes and procedures as a high priority now, compared to 29% of those that had not conducted a DPIA
- 45% of those that processed personal data rated other information/cyber security policies, processes and procedures as a high priority now, compared to 26% of those that did not process personal data
- 46% of those who were IT or cyber security professionals rated other information/cyber security policies, processes and procedures as a high priority now, compared to 39% of those not IT or cyber security professionals

When considered by industry, those in: finance and insurance; health; education; and arts, entertainment, recreation and other services were more likely than the average respondent to have rated data protection policies, processes and procedures as a high priority now (76%, 74%, 67% and 67% of respondents respectively, compared to 54% of all respondents to the staff survey). Those in the construction industry were less likely to have rated it as a high priority now than the average respondent (37%, compared to 54%). Those in property, as well as those in finance and insurance; education; and health were more likely to have rated other information/cyber security policies, processes and procedures as a high priority now than the average respondent (66%, 60%, 53% and 51% of respondents respectively, compared to 40% of respondents to the staff survey).

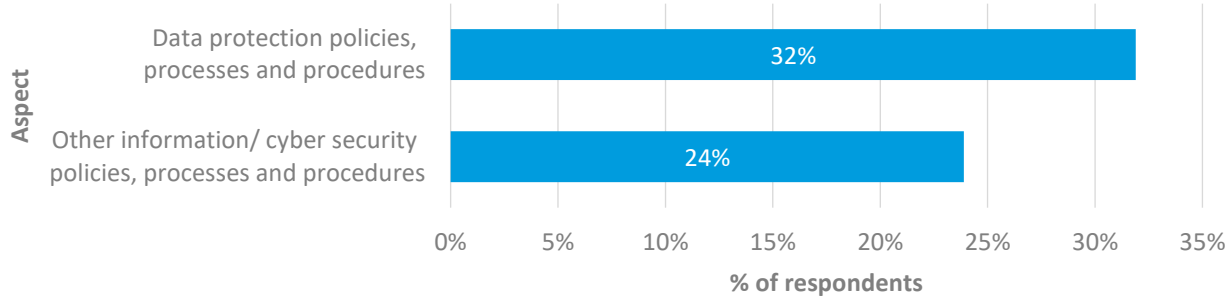
Change in priorities over the last 3 years

38% of respondents to the staff survey reported an increased prioritisation of at least one aspect of cyber security in the last 3 years, while 9% reported a decrease in the priority of one or more aspect of cyber security in the last 3 years. This included the priority of:

- data protection policies, processes and procedures (Figure 3.3 and Figure 3.4)
- other information/cyber security policies, processes and procedures (Figure 3.3 and Figure 3.4)
- technical controls for data protection (Figure 3.22and Figure 3.23)
- technical controls for other aspects of information/cyber security (Figure 3.22 and Figure 3.23)

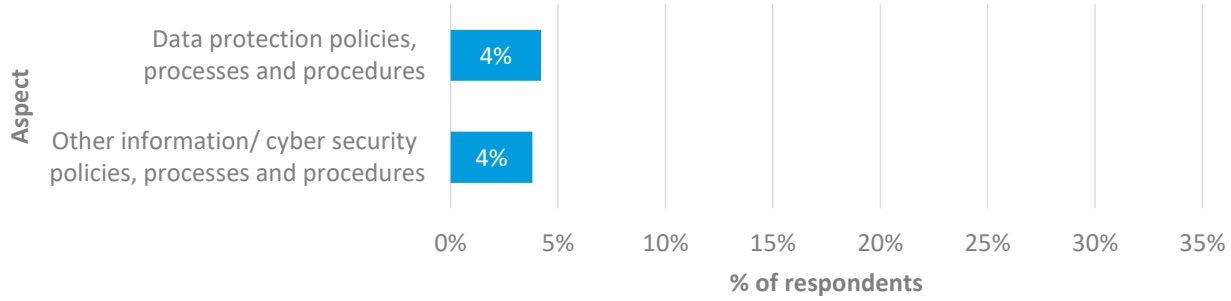
As Figure 3.3 and Figure 3.4 show, respondents were much more likely to report an increase in the priority of cyber policies, processes and procedures than a decrease.

Figure 3.3: Proportion of respondents reporting cyber security policies, processes and procedures as a higher priority now than 3 years ago



Source: Staff survey Q24ab. Proportion of respondents reporting aspects of cyber security higher priority now than 3 years ago
Weighted Base: 1,069
Unweighted Base: 1,129

Figure 3.4: Proportion of respondents reporting cyber security policies, processes and procedures as a lower priority now than 3 years ago



Source: Staff survey Q24ab. Proportion of respondents reporting aspects of cyber security lower priority now than 3 years ago
Weighted Base: 1,069
Unweighted Base: 1,129

There was some variation in response to these questions based on certain organisational characteristics. Organisations that experienced a cyber security incident, had completed a DPIA or processed personal data were more likely to rate both data and other information/cyber security policies, processes and procedures as a higher priority now than 3 years ago.

Box 2: Proportion of respondents that rated policies, processes and procedures as a higher priority now than 3 years ago by organisational characteristic

- 42% of those that experienced an incident rated data protection policies, processes and procedures as higher priority, compared to 30% of those that had not experienced an incident
- 40% of those that had completed a DPIA rated data protection policies, processes and procedures as higher priority, compared to 23% of those that had not completed a DPIA
- 34% of organisations that processed personal data rated data protection policies, processes and procedures as higher priority, compared to 21% of organisations that did not process personal data
- 33% of those that experienced an incident rated other information/cyber security policies, processes and procedures as higher priority, compared to 23% of those that had not experienced an incident
- 30% of those that had completed a DPIA rated other information/cyber security policies, processes and procedures as higher priority, compared to 20% of those that had not completed a DPIA
- 26% of organisations that processed personal data rated other information/cyber security policies, processes and procedures as higher priority, compared to 15% of organisations that did not process personal data

There was no statistically significant variation in how respondents who were IT or cyber security professionals answered these questions.

Some of the interviewees who had experienced a cyber incident explained their reasons for this increase in priority:

> *"We were the victims of a phishing attack, and we were very badly impacted as a result. It took us a long time to get the money back and because of this we had cashflow problems for several months after the incident. To ensure that this doesn't happen again, we have made our cyber security policies and processes a much higher priority." (Interviewee from a non-profit in the construction industry)*

> *"We experienced an incident a few years ago which led to a lot of sensitive data being stolen. This was a very difficult situation for us and our clients, and to ensure that our clients still felt safe using our services we prioritised our cyber security policies to reduce the likelihood of this happening again." (Interviewee from a large business with a complex and interconnected supply chain in the accommodation and food services industry)*

Some other interviewees reported that they were motivated to increase the priority of their data and other information/cyber security policies, processes and procedures because they were aware of the negative impact of other organisations experiencing cyber attacks. One interviewee reported:

> *"We have recently increased the priority of our cyber security process and policies because we know about the risks, and we don't want to be the victims of a cyber attack. There is another charity in our area who recently experienced a cyber attack, and from what we have heard they have been very heavily impacted by this. We don't want to have a similar experience, so we know that we need to make ourselves more secure." (Interviewee from an LA/non-profit providing important public services in the health industry)*

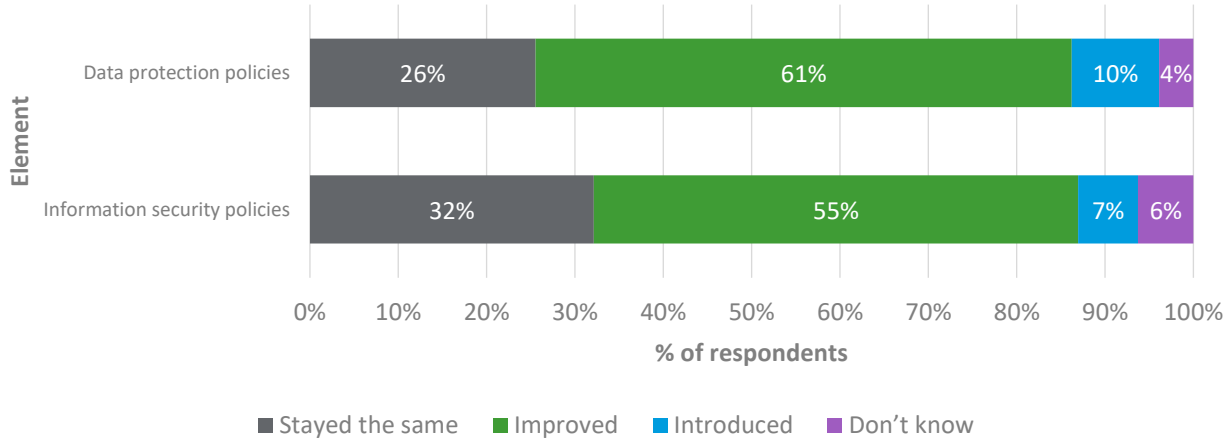
When considered by industry, respondents in arts, entertainment, recreation and other services; public administration and defence; and education were more likely to have rated these aspects of cyber security as a higher priority now, compared to 3 years ago (60%, 46% and 45% respectively rated data protection policies, processes and procedures as a higher priority and 48%, 42% and 38% respectively rated other information/cyber security policies, processes and procedures as a higher priority), especially compared to organisations in the information and communication industry (23% rated data protection policies, processes and procedures as a higher priority and 17% rated other information/cyber security policies, processes and procedures as a higher priority).

The qualitative interviews indicated that this was because these industries had relatively more changes to make to become compliant than those in information and communication, however, they did indicate that changes had been made. Finance and insurance respondents were also more likely to rate data protection policies, processes and procedures (48%) as a higher priority now than 3 years ago. Interviewees said this was because they store a large amount of personal data in comparison to organisations from other industries.

3.2.1.2 Cyber security policies

As Figure 3.5 shows, the majority of respondents said that their organisation had introduced and/or improved its data protection policies (71% of all respondents to both the staff and Board surveys introduced and/or improved) and information security policies in the last 3 years (62% of respondents introduced and/or improved).

Figure 3.5: Changes in cyber security policies in the last 3 years



Source: Staff/Board survey Q26ab/BQ25ab. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years?
Weighted Base: 1,233
Unweighted Base: 1,233
Note: Totals may not sum to 100% due to rounding.
Respondents were also allowed to select both introduced and improved where applicable

Board members were more likely to report changes to data protection policies in the last 3 years than staff (79% of Board members answered, 'introduced' and/or 'improved', compared to 69% of staff respondents). Respondents who were IT or cyber security professionals were more likely to report changes in their information security policies than non-IT or cyber security professionals (70%, compared to 57%). Respondents who were not IT or cyber security professionals were also less likely to report changes in their data protection policies than the average respondent (69%, compared to 71%).

Organisations that experienced a cyber security incident, had completed a DPIA or processed personal data, were more likely to have changed their data protection and information security policies in the last 3 years.

Box 3: Change in policies by organisational characteristic

- 84% of those that experienced an incident had introduced new and/or improved data protection policies, compared to 69% of organisations that had not experienced an incident
- 80% of those that had completed a DPIA had introduced new and/or improved data protection policies, compared to 55% of those that had not completed a DPIA
- 75% of organisations that processed personal data had introduced new and/or improved data protection policies, compared to 58% of organisations that did not process personal data
- 76% of those that experienced an incident had introduced new and/or improved information security policies, compared to 59% of organisations that had not experienced an incident
- 73% of those that had completed a DPIA had introduced new and/or improved information security policies, compared to 46% of those that had not completed a DPIA
- 66% of organisations that processed personal data had introduced new and/or improved information security policies, compared to 43% of organisations that did not process personal data

Organisations in the construction industry were less likely to have changed their data protection policies (57%) than those in arts, entertainment, recreation and other services (94%); public administration and defence (87%); health (86%); and education (81%).

Organisations in the wholesale and retail industry were less likely to have changed their information security policies (52%) than those in arts, entertainment, recreational and other services (81%); education (79%); finance and insurance (77%); health (76%); and public administration and defence (75%).

We used the qualitative interviews to understand what type of changes had been made, examples included:

> *"We didn't have any policies before, but we have introduced a whole suite of policies since the introduction of the GDPR. These policies relate to data protection and cyber security." (Interviewee from an LA/non-profit providing important public services in the health industry)*

> *"We introduced policies on what data should be retained, and policies on how to decide when data is no longer required. There is also a new policy on how the data is to be stored and who has access to it." (Interviewee from a non-profit in the construction industry)*

> *"We have introduced privacy and data policies and have introduced data retention policies which cover all paperwork and data held electronically." (Interviewee from a LA/non-profit providing important public services in the education industry)*

> *"We rewrote our data protection policies for employees, for website users and for our members. In some cases, these didn't exist previously, and in others they were greatly expanded to include all the information required by the GDPR." (Interviewee from a non-profit in the professional, scientific and technical industry)*

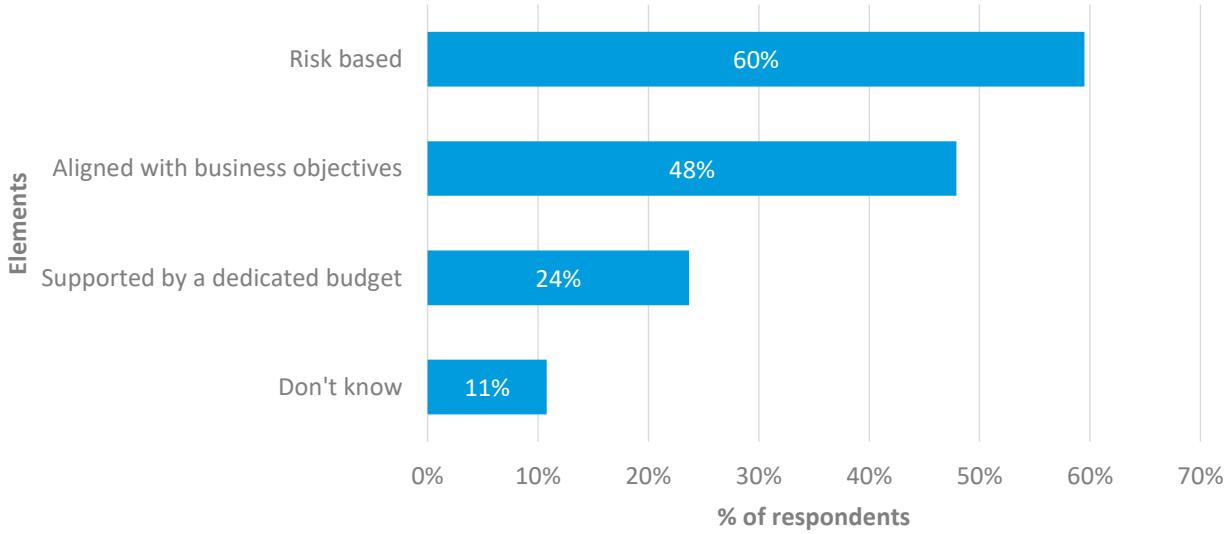
Interviewees from the information and communication industry and finance industry said they were less likely to have made changes to their data protection policies, as these were already compliant with the GDPR and, therefore, they felt further change was unnecessary.

3.2.1.3 Cyber security strategy

Approximately a fifth of Board members surveyed said that their organisation had a dedicated cyber security strategy (18%) and approximately half had a cyber security strategy as part of their IT strategy (52%). It is concerning, however, that almost a third (31%) reported having no formal cyber security strategy in place. We were unable to probe this further through the qualitative interviews as all interviewees were from organisations with a formal strategy in place. This is potentially an area for further research.

Most of the organisations that had a cyber security strategy in place had a risk-based strategy (60%) and approximately half (48%) had a strategy that was aligned with business needs. Less than a quarter (24%), however, had a strategy that was supported by a dedicated budget. It is concerning to note that 11% of Board members were unable to answer this question (said, 'Don't know').

Figure 3.6: Proportion of cyber security strategies with the following key elements

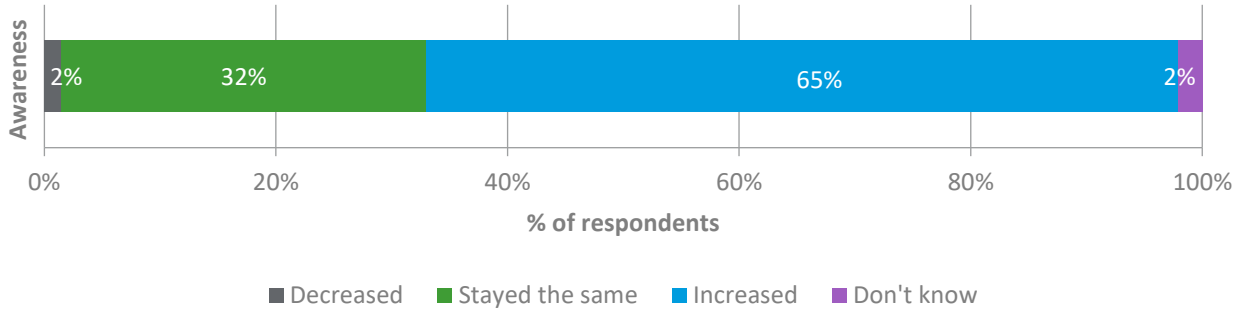


Source: Board survey BQ11. Where have a cyber security strategy for organisation, is it…?
Weighted Base: 114
Unweighted Base: 73
Note: Totals do not sum to 100% because respondents could choose more than one option.

3.2.1.4 Board level awareness

The majority of respondents to the Board survey (65%) said that their Board of Directors' awareness of cyber security had increased in the last 3 years, with a third (32%) reporting that it had stayed the same (Figure 3.7 overleaf).

Figure 3.7: Change in Board of Directors' awareness of cyber security in last 3 years

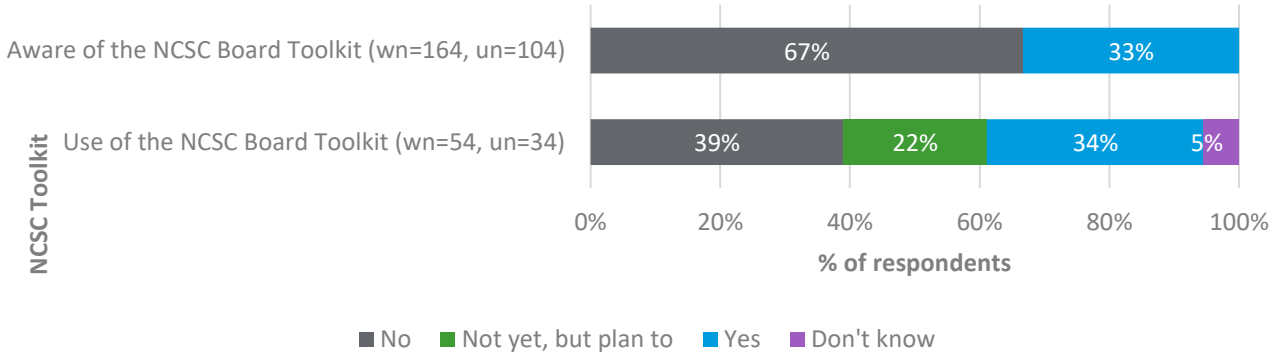


Source: Board survey BQ13. Has the Board of Director's awareness of cyber security increased, decreased or stayed the same in the last 3 years (since the introduction of the GDPR)?
Weighted Base: 164
Unweighted Base: 104

3.2.1.5 NCSC Board Toolkit

The majority of Board members surveyed were not aware of the NCSC Board Toolkit (67%). Where Board members were aware of it (33%), only a third had used it (34%), with a further fifth planning to use it in the future (22%).

Figure 3.8: NCSC Board Toolkit



Source: Board survey BQ15. Are you aware of the National Cyber Security Centre (NCSC) Board Toolkit? And BMQ16. Has your organisation used it?
wn = Weighted Base, un = Unweighted Base
Note: Only respondents who were aware of the NCSC toolkit were asked if they had used it, hence the lower base

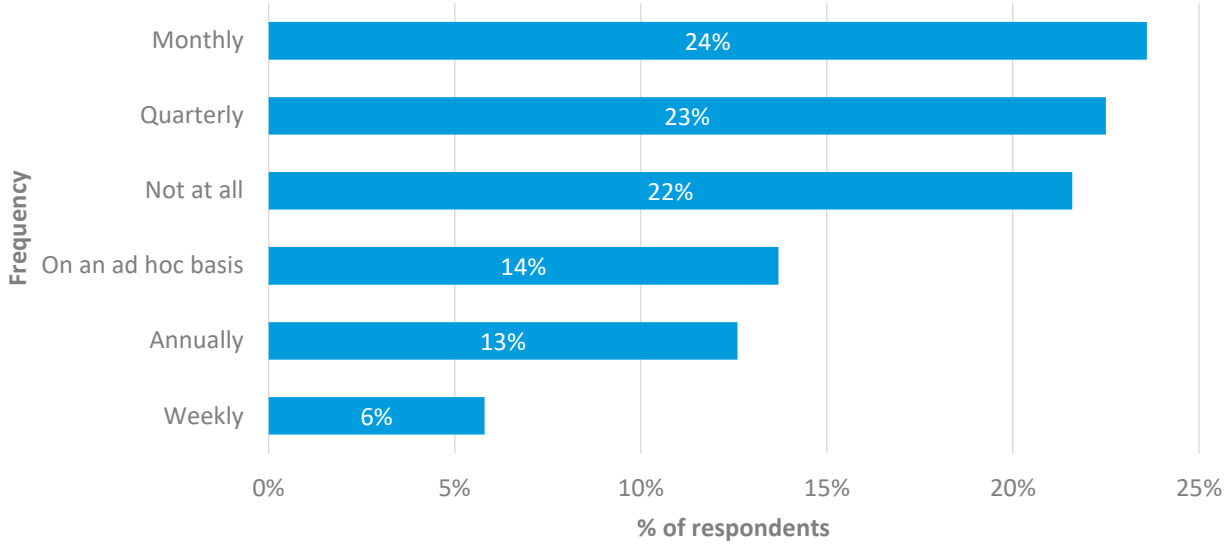
Board members who were aware of the NCSC Board Toolkit but had not used it and had no plans to do so (39%) were asked why not. Their reasons included that they had no need to or they had other providers/specialists advising them.

3.2.1.6 Changes to Board updates

Findings on the frequency of cyber security updates to the Board were mixed. Monthly or quarterly updates were the most common responses followed by 'not at all.' In most cases the frequency of these updates had stayed the same (63%). However, approximately a third (33%) reported that the

frequency of cyber security updates had increased in the last 3 years. The remaining 4% did not know.

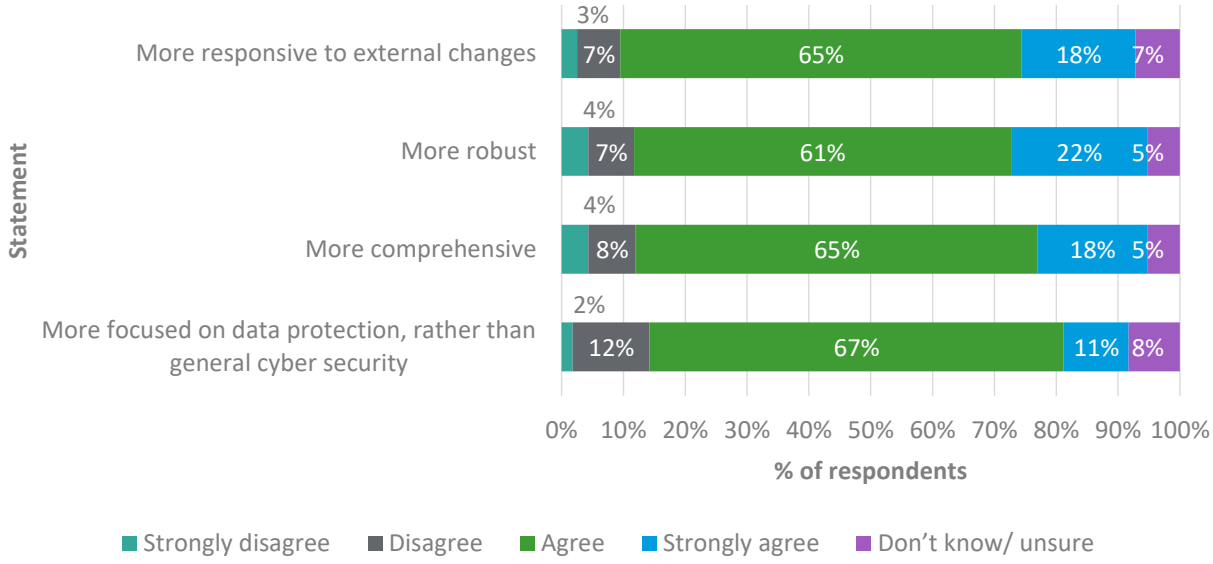
Figure 3.9: Frequency of cyber security updates to the Board



Source: Board survey BQ18. How often does the Board receive reported updates on cyber security?
Weighted Base: 164
Unweighted Base: 104
Note: 'Other' responses included every 2 months and every 6 months
** is an indicator that the proportion is negligible, but not zero (i.e. does not round up to 1%).*

Board members typically responded positively about changes to their cyber security updates over the last 3 years (see Figure 3.10).

Figure 3.10: Changes to cyber security updates in the last 3 years



Source: Board survey BQ21. To what extent do you agree or disagree with the following statements about updates on your organisations cyber security now, compared to 3 years ago?
Weighted Base: 164
Unweighted Base: 104

The vast majority of respondents agreed, or strongly agreed, that their cyber security updates were:

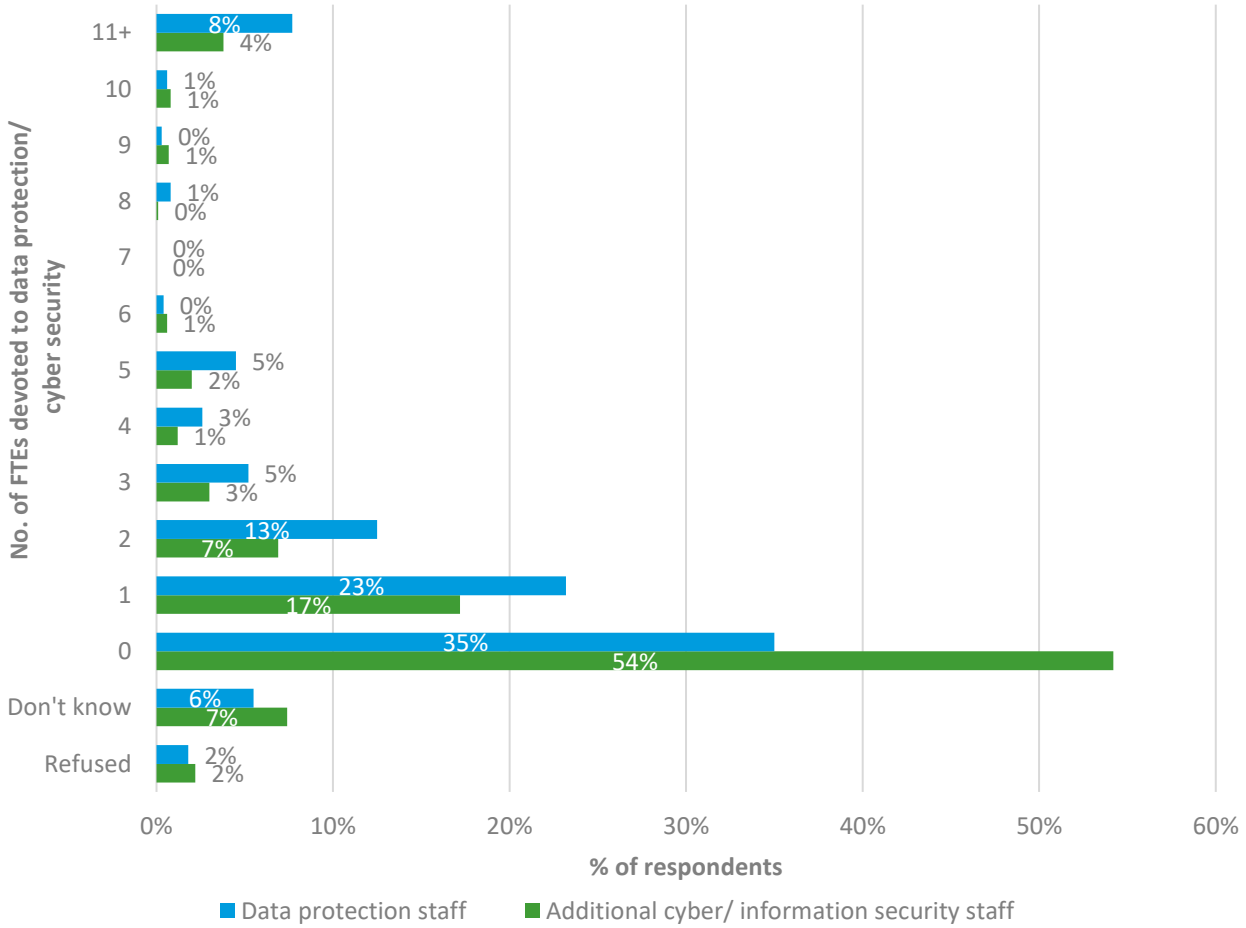
- more responsive to external changes (83% of respondents agreed or strongly agreed)
- more robust (83%)
- more comprehensive (83%)

However, the majority of respondents (78%) agreed or strongly agreed that their cyber security updates had also become more focused on data protection, rather than general cyber security, than they were 3 years ago.

3.2.1.7 Staffing

While most respondents to the staff survey said that their organisation had at least one employee that specialised in data protection (58%), over a third did not have any specialist data protection employees (35%) and more than half of respondents (54%) did not have any additional employees that specialised in cyber security or information security (such as an Information Officer, Security Architect, Engineer, Analysts etc) within their organisation (see Figure 3.11).

Figure 3.11: Number of Full-Time Equivalent (FTE) Data protection and cyber/information security staff in 2020

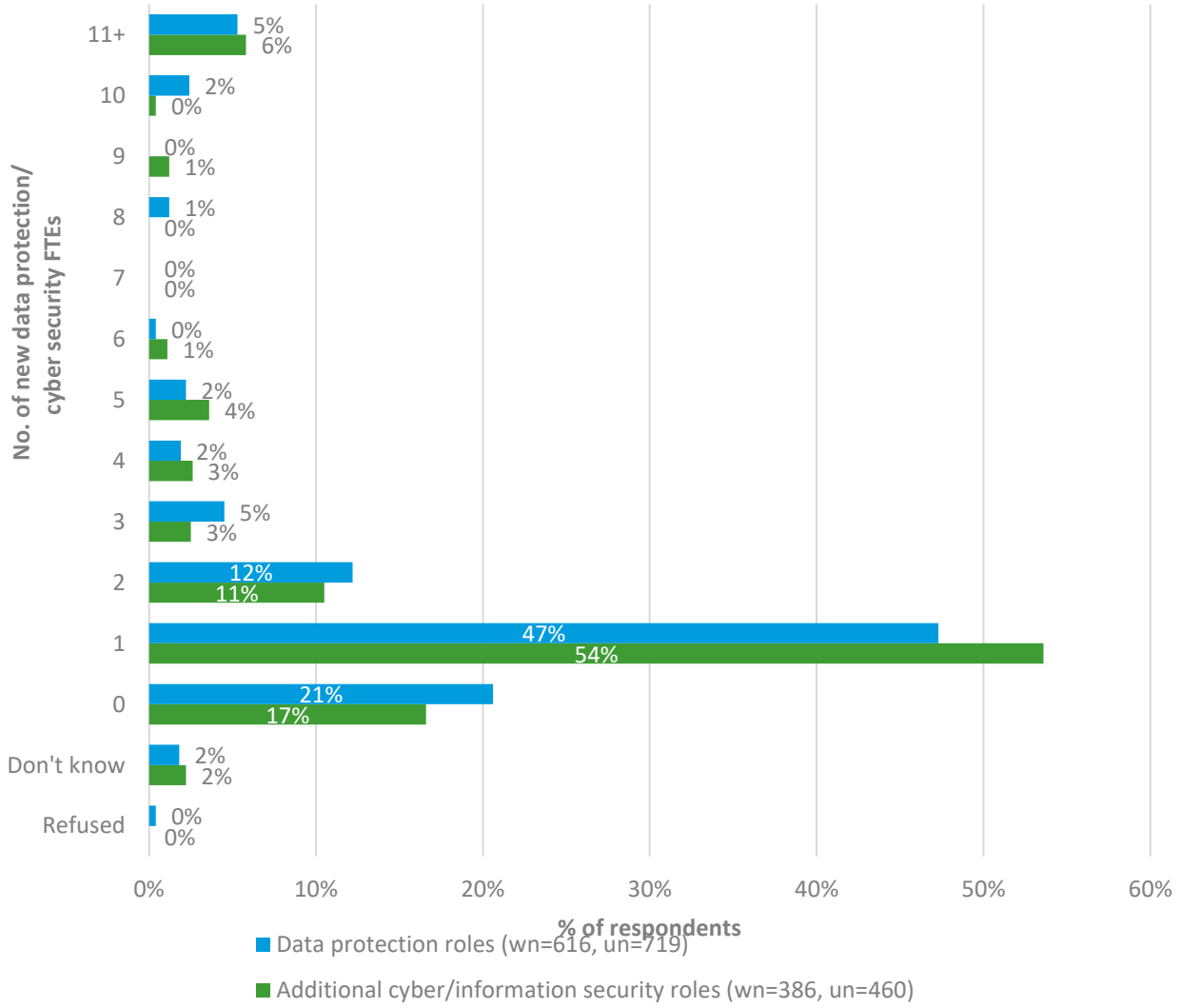


Source: Staff survey Q10. How many employees, in terms of FTEs, specialise in data protection within your organisation? (e.g. Chief Data Officer, Head of Compliance and data protection, Data Protection Officer, Privacy Officer, Data Protection Compliance Manager etc) and Q13. Excluding those who specialise in data protection, how many FTE employees specialise in cyber security or information security (e.g. Information Officer, Security Architect, Engineer, Analysts etc)
Weighted Base: 1,069
Unweighted Base: 1,129
Note: '' is an indicator that the proportion is negligible, but not zero (i.e. does not round up to 1%).*

As would be expected, organisations that had not done a DPIA, experienced a cyber security incident or that did not process personal data were more likely to have no employees that specialised in data protection (51%, 38% and 52% of respondents reported no data protection staff respectively) than organisations that had completed a DPIA, experienced an incident or processed personal data (21%, 25% and 31% respectively). This was the same for cyber or information security specialists (66% of organisations that had not done a DPIA had no cyber or information security staff, compared to 44% of those that had done a DPIA; 59% of those that had not experienced an incident, compared to 36% of those that had; 70% of organisations that did not process personal data, compared to 51% of those that did).

Where organisations had employees who specialised in data protection or cyber/information security, the majority had created one or more of these roles in the last 3 years (since GDPR was announced in April 2016) (see Figure 3.12).

Figure 3.12: Data protection and cyber/information security roles created in the last 3 years



Source: Staff survey Q11. How many of these [data protection] roles have been created in the last 3 years since GDPR was announced in April 2016? And Q14. How many of these [cyber/information security] roles have been created in the last 3 years?

Note: '' is an indicator that the proportion is negligible, but not zero (i.e. does not round up to 1%).*
Only respondents who had some data protection or cyber/information security staff were asked how many of these roles were created in the last 3 years

Where organisations had data protection or other cyber/information security staff, those organisations that had experienced a cyber security incident were more likely than those that had not experienced an incident to have created one or more of these roles in the last 3 years (84%% of those that had experienced an incident had created new data protection roles, compared to 76% of those that had not experienced an incident; 89% of organisations that had experienced a cyber security incident had created new cyber security roles, compared to 79% of those that had not experienced an incident).

The creation of new roles was more common among respondents from the wholesale and retail industry than those in information and communication, health or education.

Box 4: Creation of new roles by industry

- 93% of wholesale and retail respondents had created at least one new data protection role in the last 3 years, compared to 67% of respondents from the health industry, 66% from information and communication and 64% from education
- 90% of wholesale and retail respondents had created at least one new cyber/information security role in the last 3 years, compared to 72% in information and communication, 70% in health and 64% in education

We used our qualitative interviews to better understand why some organisations had increased their data protection and cyber security staff, while others had not. Where interviewees reported staff changes since the GDPR was introduced, the rationale was typically that they had lacked the in-house expertise to enable them to understand and meet the requirements of the GDPR:

> *"We just didn't have the expertise amongst our staff to understand how best to change our processes so that we would be compliant. It was necessary for us to hire someone with the right knowledge and skills to make us compliant and keep us protected." (Interviewee from a large business with a complex and interconnected supply chain in the accommodation and food services industry)*

Some interviewees stated that while they did not employ new members of staff, they did appoint someone within the organisation to take responsibility for ensuring their organisation was compliant with the GDPR.

3.2.2 Risk management

Appropriate steps are taken to identify, assess and understand security risks to personal data and the systems that process this data. The GDPR emphasises a risk-based approach to data protection and the security of processing systems and services. Steps must be taken to assess these risks and include appropriate organisational measures to make effective risk-based decisions based upon:

- the state of the art [technology]
- cost of implementation
- the nature, scope, context and purpose of processing
- the severity and likelihood of the risk being realised

Beyond this, where the processing is likely to result in a high risk to the rights and freedom of individuals, organisations must also undertake a Data Protection Impact Assessment (DPIA) to determine the impact of the intended processing on the protection of personal data. The DPIA should consider the technical and organisational measures necessary to mitigate that risk. Where such measures do not reduce the risk to an acceptable level, organisations need to have a process in place to consult with the ICO before you start the processing.
(Source: NCSC)

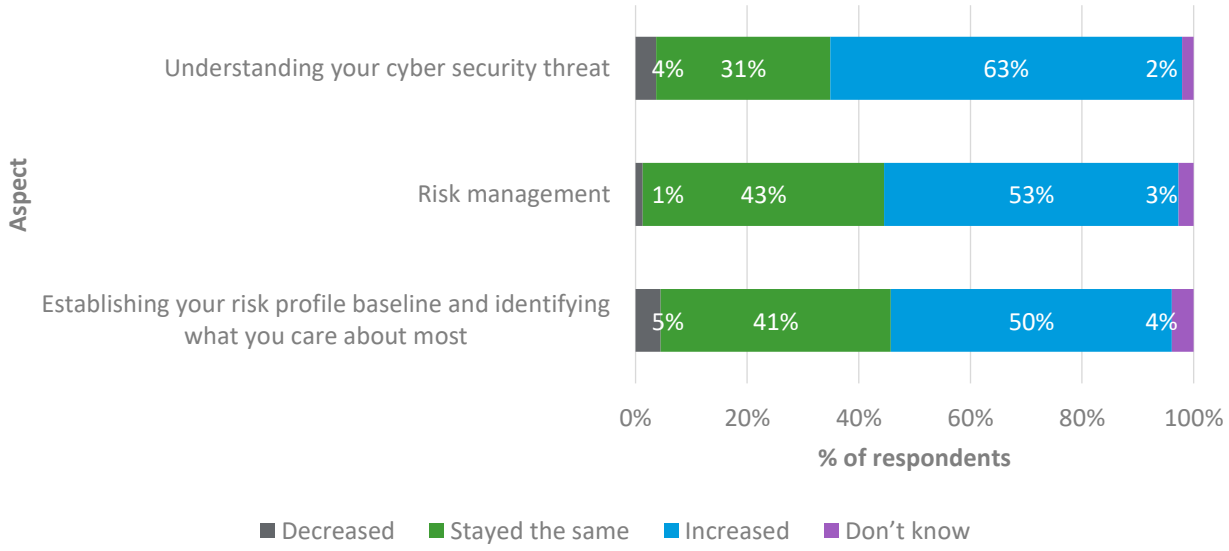
In addition to the findings on cyber security policies and resources reported above, we explored changes in cyber security risk management in relation to prioritisation of risk management and the use of DPIAs.

Overall, based on the findings presented below, most organisations appear to have improved their risk management in the last 3 years.

3.2.2.1 Prioritisation of risk management

Board members typically reported an increase in the Board's prioritisation of risk management aspects of cyber security in the last 3 years (see Figure 3.13).

Figure 3.13: Changes in Board prioritisation of cyber risk management in the last 3 years



Source: Board survey BQ23def. In the last 3 years, has the Board increased, decreased or given the same prioritisation to the following aspects of cyber security?
Weighted Base: 164
Unweighted Base: 104

Around half of respondents said that their organisation had introduced and/or improved its risk management (53% of all respondents to both surveys). Examples of specific changes reported by interviews included:

> *"Changing the composition of the risk committee." (Interviewee from a non-profit in the professional, scientific and technical industry)*

> *"Our risk management processes have changed since the GDPR was introduced, and we now have risk registers. This is talked about often at Board meetings as well as senior management team meetings. We are now more aware of the risks. We discuss the risks more and take action as and when we need to." (Interviewee from an LA/non-profit providing important public services in the health industry)*

3.2.2.2 Changes in risk management

Board members were more likely to report a change in their risk management than staff (64% of Board members reported a change, compared to 51% of staff). Organisations that had experienced a cyber security incident, conducted a DPIA or processed personal data were also more likely to have changed their risk management in the last 3 years.

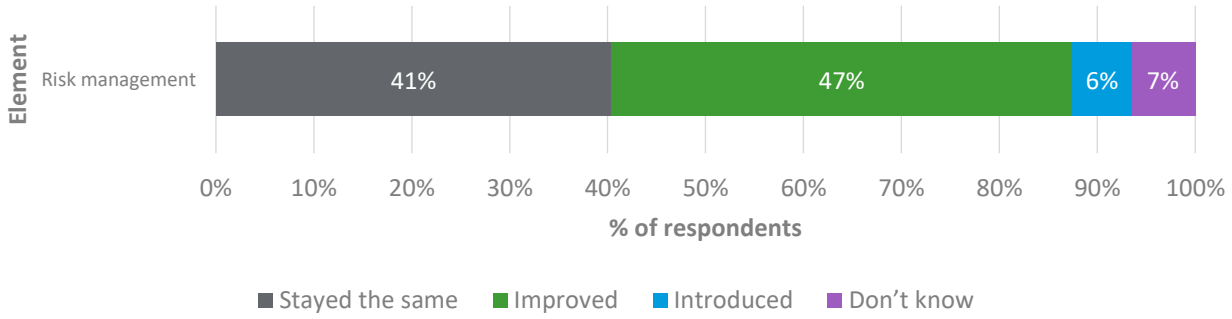
Box 5: Changes in risk management by organisational characteristic

- 62% of those that had experienced an incident answered, 'introduced' and/or 'improved', compared to 51% of those that had not experienced an incident
- 62% of those that had done a DPIA said, 'introduced' and/or 'improved', compared to 38% of those that had not done a DPIA
- 57% of those that processed personal data answered, introduced' and/or 'improved', compared to 36% of organisations that did not process personal data

Respondents who were IT or cyber security professionals were also more likely to report changes in their risk management (58%) than those who were not IT or cyber security professionals (49%).

Organisations in finance and insurance (83%), health (70%) and education (67%) were more likely to have changed their risk management in the last 3 years than organisations in the construction industry (43%).

Figure 3.14: Changes in risk management in the last 3 years



Source: Staff/Board survey Q26c/BQ25c. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years?
Weighted Base: 1,233
Unweighted Base: 1,233
Note: Totals may not sum to 100% due to rounding. Respondents were also allowed to select both introduced and improved where applicable

3.2.2.3 Data Protection Impact Assessment (DPIA)

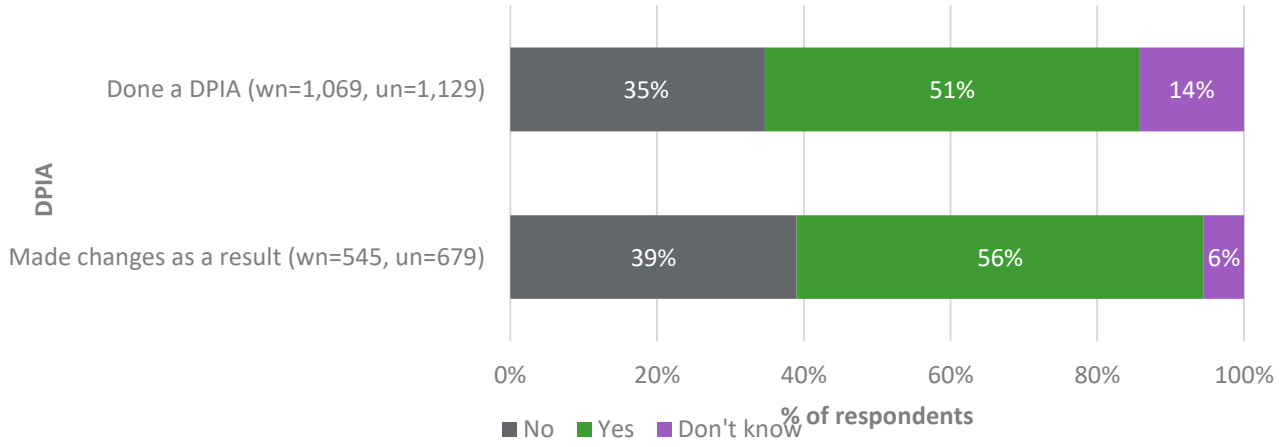
We also explored changes made as a result of having completed a DPIA as well as the rationale for not making changes. As Figure 3.15 shows, approximately half of respondents to the staff survey (51%), said their organisation had completed a DPIA, as required by the GDPR, where data processing was likely to result in a high risk to personal data.

As would be expected, organisations that processed personal data were more likely to have conducted a DPIA (53%) than organisations that did not process personal data (40%). It should be noted, however, that 75 of the 679 respondents that had completed a DPIA (11%) said that their organisation did not process personal data. This may be due to the way that the question was worded to identify organisations that processed personal data about consumers, service users, businesses or other organisations.

IT or cyber security professionals were also more likely to have said that their organisation completed a DPIA (63%) than non-IT/cyber security professionals (47%). There was no statistically significant variation in the responses of those that had experienced a cyber security incident and those that had not.

Organisations in education (75%), finance and insurance (72%), public administration and defence (66%) and health (60%) were more likely to have completed a DPIA than those in the professional, scientific and technical industry (34%).

Figure 3.15: Proportion of organisations who have completed a DPIA in the last 3 years and made changes as a result



Source: Staff survey Q29. Has your organisation done one or more Data Protection Impact Assessment (DPIA) (as required by the GDPR where data processing is likely to result in a high risk to personal data)?; and Q30. Have you made any changes to your cyber security arrangements as a result of doing a DPIA?

Note: Only respondents who had done a DPIA were asked if they had made changes as a result, hence the lower base for this question

As shown in Figure 3.15, just over half of the organisations that completed a DPIA made changes to their cyber security as a result of it (56% of all respondents who had completed a DPIA), which suggests that this risk management process is having an impact on cyber security practices. Figure 3.16 shows where this impact is being felt.

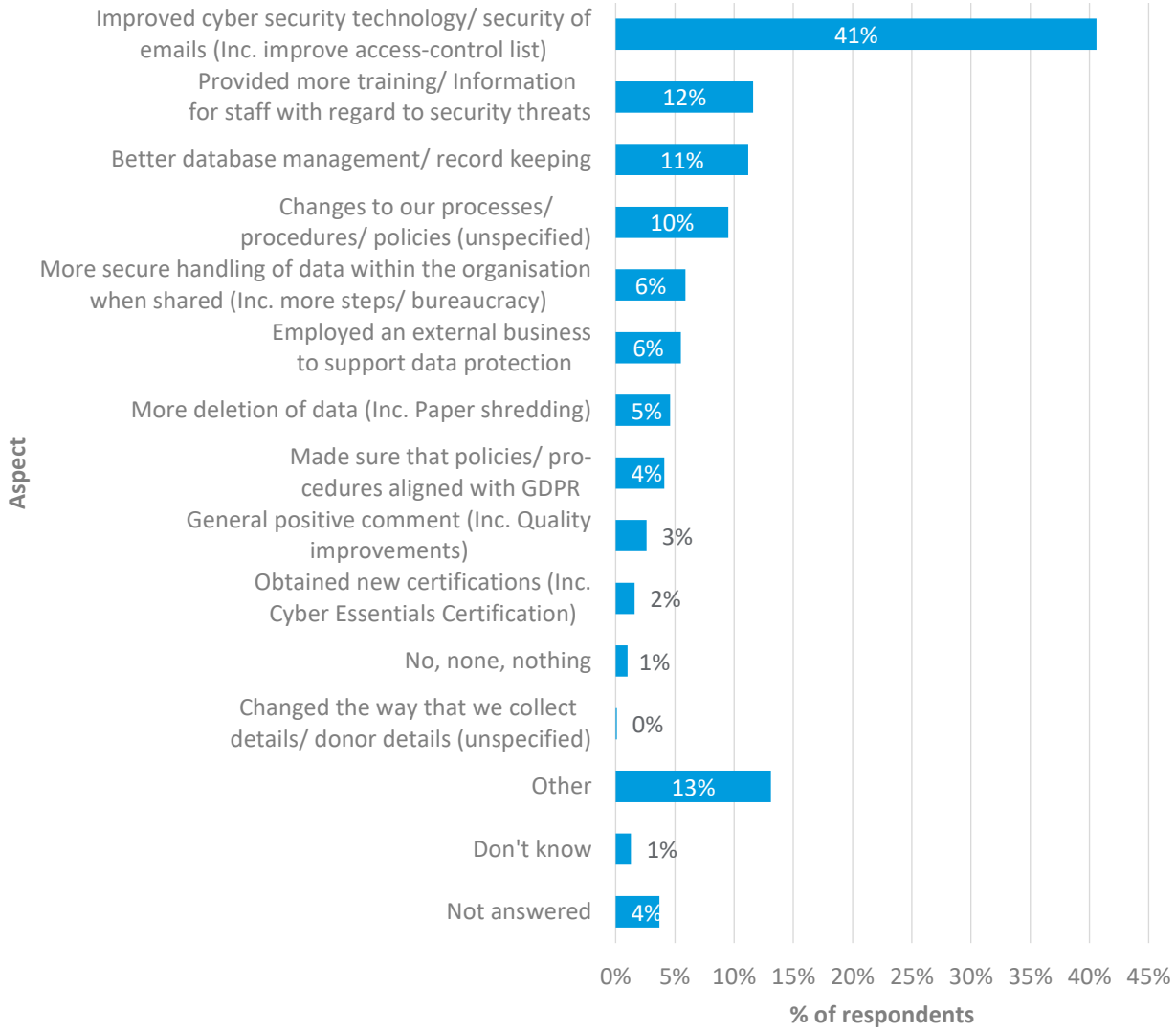
Organisations that had experienced a cyber security incident (81%) or processed personal data (60%) were more likely to have made changes than those that did not experience an incident (51%) or process personal data (35%). IT or cyber security professionals were also more likely to have reported changes (69%) compared to non-specialists (49%).

Organisations in the information and communication industry were more likely than the average respondent to have made changes to their cyber security as a result of a DPIA (69%, compared to 56% of all respondents who had completed a DPIA).

Respondents who said they had made changes as a result of completing a DPIA were asked what type of changes had been made. As Figure 3.16 shows, DPIAs appeared to drive a technical response from organisations. Improved cyber security technology, email security or improved access controls was the most common response, followed by providing more training/information for staff with regards to security threats and better database management/record keeping.

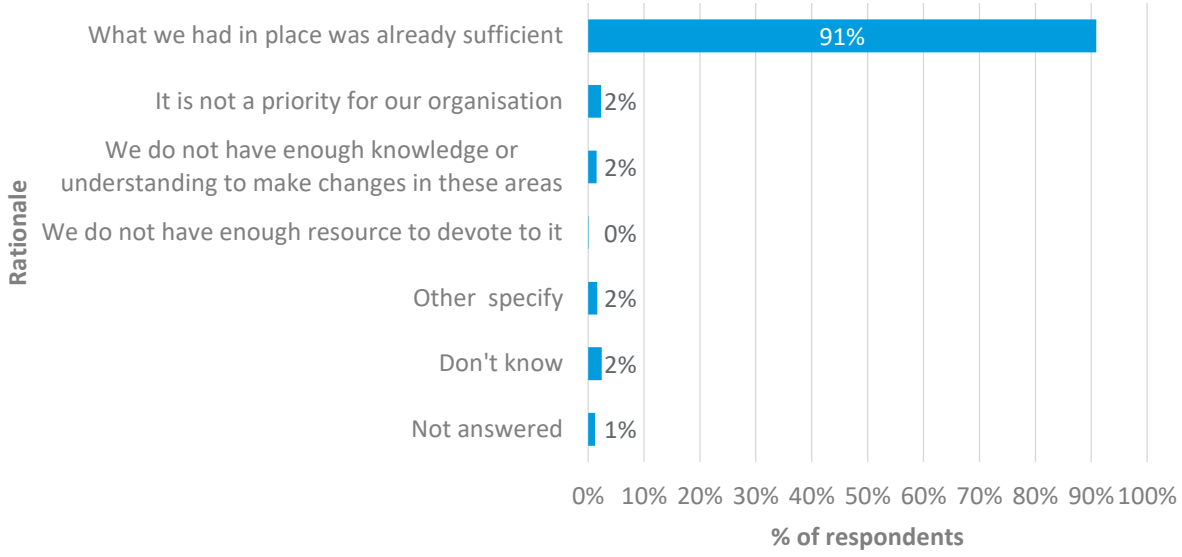
Where changes were not made, in the vast majority of cases this was because respondents felt the measures in place were already sufficient (see Figure 3.17). This was less common among respondents who were IT or cyber security specialists (82%) than those who were not (93%). There was no statistically significant variation in the responses given by those that had experienced a cyber incident or processed personal data and those that did not. Organisations in the public administration and defence industry were less likely to have said what was in place was sufficient (77%) than the average respondent (91%).

Figure 3.16: Changes made as a result of a DPIA



Source: Staff survey Q31. What type of changes have you made as a result of doing a DPIA?
Weighted Base: 238
Unweighted Base: 321
Note: Totals do not sum to 100% because respondents could give multiple responses.
Respondents who answered, 'Other' were asked to specify. Examples of their responses included password protection, multi-authentication, email/file encryption, better data management, access controls, improved software and policies, and more firewalls.

Figure 3.17: Rationale for not making changes as a result of doing a DPIA



Source: Staff survey Q32. What is the main reason you haven't made any changes as a result of doing a DPIA?
Weighted Base: 202
Unweighted Base: 227

Respondents who answered, 'Other' were asked to specify. Examples of their responses included measures in place are already appropriate, cost, low risk, no changes needed, not necessary/not required to/no changes needed.

Most interviewees were confident that the changes they had made as a result of the GDPR had improved their ability to manage security risk:

> *"The changes we made when the GDPR was enforced have made us much better at managing cyber security risks. Initially we weren't sure what we needed to do to be compliant, so we hired cyber security experts to look into this for us. They gave us advice and told us what changes we needed to make to our policies and processes. Because of this we are more aware of the risks, and how to mitigate them." (Interviewee from a non-profit in the arts, entertainment, recreation and other services industry)*

However, some interviewees did not think that the changes they made as a result of the GDPR had led to improvements to their organisation's ability to manage cyber security risks:

> *"The changes haven't made us better at managing cyber security risks. We only made changes to be compliant with the GDPR, and that is just about data protection. Our cyber security was already robust, the GDPR encouraged us to tweak the data protection aspect of cyber security." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

3.2.3 Asset management

Organisations understand and catalogue the personal data they process and can describe the purpose for processing it. They also understand the risks posed to individuals of any unauthorised or unlawful processing, accidental loss, destruction or damage to that data.

The personal data processed should be adequate, relevant and limited to what is necessary for the purpose of the processing. It should not be kept for longer than is necessary.
(Source: NCSC)

In addition to the findings on cyber security processes and resources reported above, we explored changes in the management of data as an asset, and the tracking and recording of all assets that process personal data.

Overall, based on the findings presented below, there has been some improvement in asset management in the last 3 years.

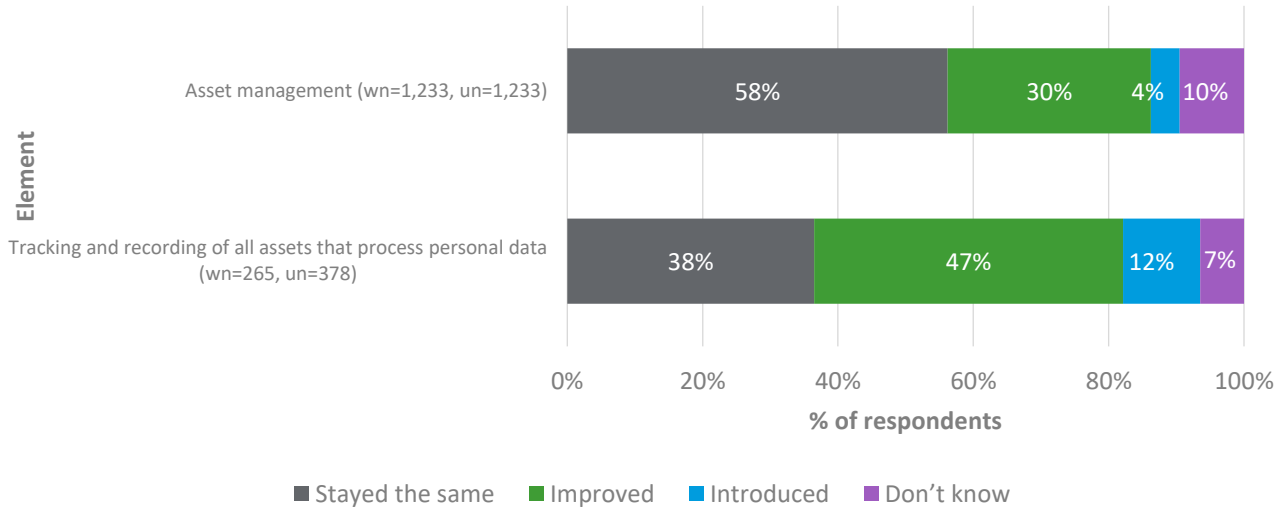
Changes in asset management

Over half of all respondents said that their asset management had stayed the same in the last 3 years (56%). Organisations that had experienced a cyber security incident, conducted a DPIA or processed personal data were more likely to have changed their asset management (53%, 43% and 36% respectively, answered 'introduced' and/or 'improved'), than to those that had not experienced an incident (31%), had not done a DPIA (23%) or did not process personal data (27%). The majority of interviewees in organisations that had experienced an incident said that they had changed their asset management to minimise the risk of a future incidents, as opposed to enforcement of the GDPR.

Respondents who were IT or cyber security professionals were more likely to have reported a change in their asset management than non-professionals (50%, compared to 28%).

Compared to the average respondent (34%), organisations in the finance and insurance industry (53%) and the information and communication industry (43%) were more likely to have introduced and/or improved asset management in the last 3 years.

Figure 3.18: Changes in asset management and tracking and recording all of assets that process personal data in the last 3 years



Source: Staff survey Q26l. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years? and Staff/Board survey Q26d/BQ25d. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years?

Notes: wn= Weighted Base, un= Unweighted Base

Only respondents who considered themselves to be either an IT or cyber security professional were asked question Q26l

Totals may not sum to 100% due to rounding. Respondents were also allowed to select both introduced and improved where applicable

Tracking and recording assets that process personal data

Respondents who were IT or cyber security professionals (378 respondents or 33% of respondents to the staff survey) were asked additional questions about more technical changes to their cyber security, including tracking and recording of all assets that process personal data. The bases for these responses are, therefore, lower than the total survey responses. The majority of technical respondents said that their organisation had introduced and/or improved their tracking and recording of all assets that process personal data (56%).[79]

Organisations that had completed a DPIA, experienced a cyber security incident or processed personal data were more likely to have changed their tracking and recording of assets in the last 3 years than those that had not completed a DPIA, experienced a cyber security incident or processed personal data.

Box 6: Changes in tracking and recording assets by organisational characteristic

- 68% of those that had done a DPIA answered, 'introduced' and/or 'improved', compared to 36% of those that had not done a DPIA
- 65% of organisation that experienced an incident, compared to 50% of those that had not experienced an incident
- 60% of organisations that processed personal data, compared to 19% of those that did not process personal data - note small base for the latter on this particular question (28 respondents)

There was no statistically significant variation in response to this question by industry.

3.2.4 Data processors and the supply chain

Organisations understand and manage security risks to their processing operations that may arise as a result of dependencies on third parties such as data processors. This includes ensuring that they employ appropriate security measures.

In the case of data processors, organisations are required to choose those that provide sufficient guarantees about their technical and organisational measures. The GDPR includes provisions where processors are used, including specific stipulations that must feature in contracts.
(Source: NCSC)

In addition to the findings on cyber security processes and resources reported above, we explored changes in data processors and the supply chain in relation to working with suppliers and partners to manage supply chain risks and procurement or supply chain risk management.

Overall, based on the finding presented below, less change was evident in relation to procurement and the supply chain.

Working with suppliers and partners to manage supply chain risks

The supply chain plays an important part in many of the most famous cyber security incidents over the past decade, for example the Target incident.[80] However, the majority of Board members said there had been no change in how they worked with their suppliers and partners to manage supply

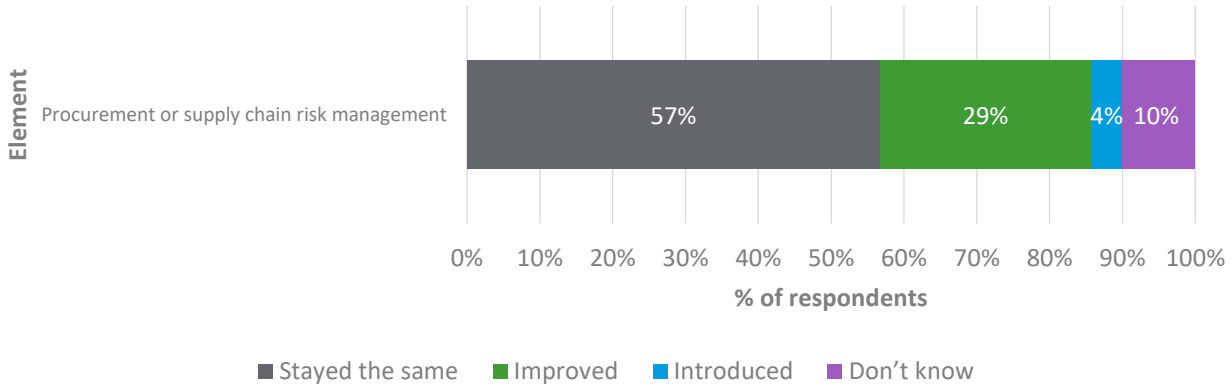
[79] *This does not match Figure 3.18 because respondents could select both introduced and improved where applicable*
[80] *Plachkinova and Maurer (2018) Teaching Case Security Breach at Target, Journal of Information Systems Education, Vol. 29(1) Winter 2018*

chain risks in the last 3 years (54%), 37% reported an increase and 8% didn't know.[81] This is potentially linked to the view, expressed in existing research, that many organisations are still treating cyber security as a technical issue.

Procurement or supply chain risk management

A minority of respondents said that their organisation had introduced and/or improved its procurement or supply chain risk management (33%).

Figure 3.19: Changes in procurement or supply chain risk management in the last 3 years



Source: Staff/Board survey Q26e/BQ25e. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years?
Weighted Base: 1233
Unweighted Base: 1233
Notes: Totals may not sum to 100% due to rounding.
Respondents were also allowed to select both introduced and improved where applicable

Respondents were also more likely to have changed their procurement or supply chain risk management if they had experienced a cyber security incident, completed a DPIA or processed personal data than those that did not.

Box 7: Changes in procurement or supply chain risk management by organisational characteristic

- 53% of organisations that experienced an incident answered, 'introduced' and/or 'improved', compared to 30% of those that had not
- 45% of organisations that had done a DPIA, compared to 23% of those that had not
- 38% of organisations that processed personal data, compared to 15% of those that did not process personal data

Respondents that were IT or cyber security professionals were more likely to have reported changes in procurement or supply chain risk management than those who were not IT or cyber security professionals (52%, compared to 27%).

Organisations in the finance and insurance industry (57%) and information and communication industry (43%) were more likely to have changed their procurement or supply chain risk management than the average respondent (33%).

[81] *Totals do not sum to 100% due to rounding*

Examples of changes in supply chain risk management included:

> *"More checks with suppliers to ensure that they are compliant with the GDPR and only working with those that are compliant. This is because if they are compliant, then it makes it easier for us to be compliant with the GDPR. Another change we made is to have risk management logs and make sure those are up to date." (Interviewee from an SME in the finance and insurance industry)*

3.3 Protect personal data against cyber attack

Proportionate security measures are in place to protect against cyber attack which cover the personal data processed and the systems that process such data.
(Source: NCSC)

3.3.1 Service protection policies and processes

Appropriate policies and processes that direct the overall approach to securing systems involved in the processing of personal data should be defined, implemented, communicated and enforced. Organisations should also consider assessing your systems and implementing specific technical controls as laid out in appropriate frameworks (such as Cyber Essentials).
(Source: NCSC)

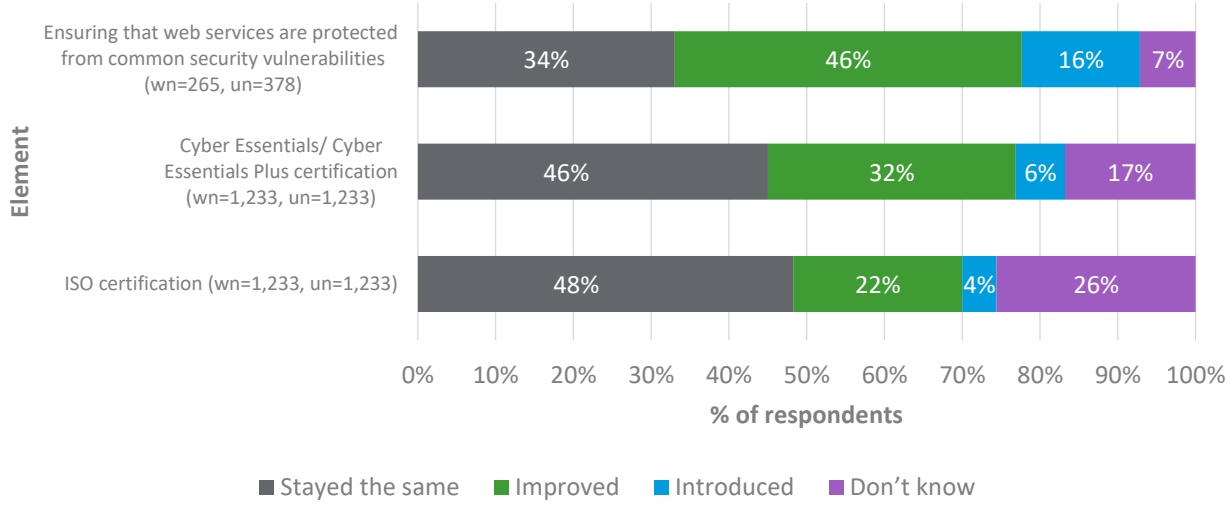
In addition to the findings on the policies and processes above, we explored changes in service protection policies and processes, such as ensuring that web services are protected from common vulnerabilities, as well as changes in Cyber Essentials/Cyber Essentials Plus certification and ISO certification.

Overall, based on the findings presented below, there was some improvement in relation to service protection policies and processes.

Ensuring web services are protected from common vulnerabilities

Respondents who were IT or cyber security professionals were asked additional questions about more technical changes to their cyber security, including how they ensure that web services are protected from common vulnerabilities. The majority of technical respondents reported that their organisations had introduced and/or improved processes for ensuring that web services are protected in the last 3 years (see Figure 3.20). There was no statistically significant variation in the response by industry.

Figure 3.20: Changes in certification and service protection in the last 3 years



Source: Staff/Board survey Q26fg/BQ25fg. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years? and Staff survey technical question Q26q. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years?

Notes: '' is an indicator that the proportion is negligible, but not zero (i.e. does not round up to 1%).*
Respondents who answered, 'Other' were asked to specify. Examples of their responses included measures in place are already appropriate, cost, low risk, no changes needed, not necessary/not required to/no changes needed.

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed how they ensure that web services are protected in the last 3 years (78%, 70% and 63% respectively answered, 'introduced' and/or 'improved') than those that had not experienced an incident (51%), completed a DPIA (42%) or did not process personal data (39% - note small base of 28 respondents).

The majority of interviewees were confident that the changes they have made as a result of the GDPR have improved their ability to protect themselves from a cyber attack:

> *"Becoming GDPR compliant means that we now have something specific in place to manage our cyber security and this has definitely improved our ability to protect against attacks." (Interviewee from a large business with a complex and interconnected supply chain in the property industry)*

Changes in certification

A minority of respondents said that their organisation had introduced and/or improved its Cyber Essentials/Cyber Essentials Plus certification (38%) and ISO certification (26%). This included becoming certified for the first time, getting recertified and upgrading their certification. The proportion of respondents that answered 'don't know' to these questions suggested more could be done to raise awareness of the benefits of certification. Some interviewees reported that the introduction of the GDPR had motivated them to obtain Cyber Essentials/Cyber Essential Plus certification or ISO certification. These interviewees reported that this was because the GDPR made them more aware of cyber risks and they were keen to ensure that they had appropriate measures in place to protect themselves from these risks. Another way in which the GDPR motivated the interviewees to introduce new or improved accreditation was because they wanted to ensure that they would be compliant with the GDPR. One interviewee said that obtaining ISO certification was very helpful in becoming compliant with the GDPR:

"It helps that we had done ISO beforehand, so we already had done a lot of what was needed anyway. We were Cyber Essentials accredited already as well, and we had to make some other changes whilst obtaining this accreditation. This made it much easier for us when the GDPR was enforced, as because we had these accreditations, we were already compliant with the GDPR." (Interviewee from a large business with a complex and interconnected supply chain in the finance and insurance industry)

Organisations were also more likely to have to have changed their Cyber Essentials/Cyber Essentials Plus certification in the last 3 years if they experienced a cyber security incident, completed a DPIA or processed personal data (61%, 48% and 43% reported a change respectively, compared to 34% of organisations that had not experienced an incident, 23% of those that had not done a DPIA and 19% of those that did not process personal data).

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were also more likely to have changed their ISO certification (44%, 34% and 29% respectively) than those that had not experienced an incident (23%), conducted a DPIA (17%) or processed personal data (14%).

IT or cyber security respondents were more likely to report changes in their Cyber Essentials/Cyber Essentials Plus certification in the last 3 years (58%, compared to 30% of respondents who were not IT or cyber security professionals). They were also more likely to report changes in their ISO certification (45%, compared to 19% of respondents who were not IT or cyber security professionals).

Organisations in the production industry and information and communication industry were more likely to have changed their Cyber Essentials/Cyber Essentials Plus certification in the last 3 years than the average respondent (52% and 45% reported changes respectively, compared to the average respondent 38%).

Organisations in the finance and insurance industry (47%), production industry (43%) and information and communication industry (36%) were also more likely to have introduced or improved their ISO certification than the average respondent (26%).

3.3.2 Identity and access control

Access to personal data and systems that process this data must be understood, documented and managed. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. Organisations should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.

Organisations should appropriately authenticate and authorise users (or automated functions) that can access personal data. Organisations should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures.

Organisations should prevent users from downloading, transferring, altering or deleting personal data where there is no legitimate organisational reason to do so. Organisations should appropriately constrain legitimate access ensure there is an appropriate audit trail.

There should be a robust password policy in place which avoids users having weak passwords, such as those trivially guessable. All default passwords are removed, and unused accounts are suspended.
(Source: NCSC)

In addition to the findings on the policies, processes and procedures above, we explored changes in identity and access controls.

Overall, based on the findings below, there was some improvement in relation to identity and access controls in the last 3 years.

As noted in Section 3.2.2.3, improved cyber security technology/security of emails, including improved access control was the most common change made in response to doing a DPIA (41%).

Responses in relation to changes in identity and access controls were mixed. Around half of respondents said that their organisation had introduced (4%) and/or improved (43%) its identity and access controls, while 43% said they had stayed the same (11% didn't know).[82]

Board members were more likely to report changes to identity and access controls in the last 3 years than staff (59%, compared to 44%).

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed identity and access controls (64%, 53% and 50% respectively) than those that had not experienced a cyber security incident (43%), did not conduct a DPIA (31%) or did not process personal data (28%). IT or cyber security professionals were more likely to report changes in their identity and access controls (57%) than non-IT or cyber security professionals (40%). Similarly, organisations in finance and insurance, education and arts, entertainment, recreation and other services were more likely than to have changed their identity and access controls than the average respondent (67%, 62% and 60% respectively, compared to 46%).[83]

Examples of changes to identity and access controls, reported by interviewees, included:

> *"We introduced password protection procedures for personal data, so that we could ensure that only certain employees had access to our data." (Interviewee from an SME in the health industry)*

3.3.3 Data security

Technical controls (such as appropriate encryption) should be implemented to prevent unauthorised or unlawful processing of personal data, whether through unauthorised access to user devices or storage media, backups, interception of data in transit or at rest or accessing of data that might remain in memory when technology is sent for repair or disposal.
(Source: NCSC)

The increased prioritisation of data protection and other cyber security policies, processes and procedures, combined with survey findings on increased spending on cyber security in general (see Figure 3.29), and hardware and software in particular (Figure 3.28), indicates a focus on the security of data and the systems that process it. We also explored changes in technical controls, including their prioritisation, in the last 3 years and encryption of personal data (Figure 3.24).

Overall, based on the findings presented below, data security appears to have improved in the last 3 years.

[82] *Totals may not sum to 100% due to rounding. Respondents were also allowed to select both introduced and improved where applicable*
[83] *Totals do not match because respondents could select both introduced and improved where applicable*

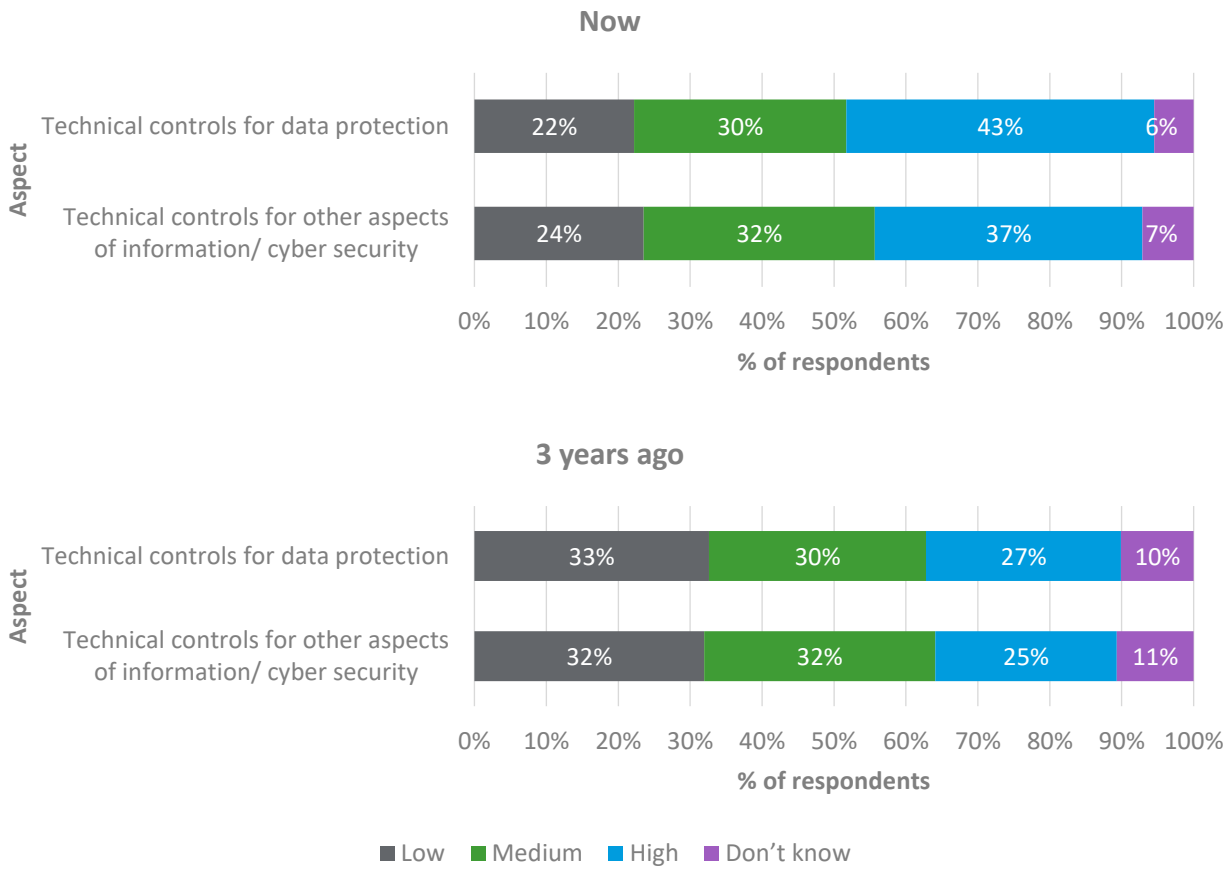
Board prioritisation

Most Board members (57%) reported an increase in the prioritisation given to implementing effective technical cyber security measures - 37% reported no change and 1% reported a decrease (5% didn't know).

Priority of technical controls now compared to 3 years ago

As Figure 3.21 shows, more respondents to the staff survey said that technical controls were a high priority, and fewer said they were a low priority now, compared to 3 years ago - especially those relating to data protection.

Figure 3.21: Priority of technical controls for cyber security



Source: Staff survey Q24cd. Are the following aspects of cyber security a high, medium or low priority for your organisation...A. Now; B. 3 years ago.
Weighted Base: 1,069
Unweighted Base: 1,129

There was some variation in response to these questions based on certain organisational characteristics. Organisations that had conducted a DPIA or processed personal data were more likely to rate technical controls for data protection and other aspects of cyber security as a high priority now than those that had not done a DPIA or did not process personal data.

Box 8: Proportion of respondents that rated technical controls as a high priority now by organisational characteristic

- 49% of respondents from organisations that had conducted a DPIA and 46% of those that processed personal data rated technical controls for data protection as a high priority now, compared to 34% of those that had not done a DPIA and 26% of those that did not process personal data
- 45% of those that had conducted a DPIA and 41% of those that processed personal data rated technical controls for other aspects of information/cyber security as a high priority now, compared to 28% of those that had not done a DPIA and 22% that did not process personal data

IT or cyber security professionals were more likely to rate technical controls for data protection (50%) and technical controls for other aspects of information/cyber security (46%) as a high priority now, than respondents who were not IT or cyber security professionals (40% and 34% respectively).

Respondents in the finance and insurance, education and health industries were more likely to rate technical controls for data protection and other aspects of cyber security as a high priority now, than those in construction.

Box 9: Proportion of respondents that rated technical controls as a high priority now by industry

- 72% of respondents the finance and insurance, 60% in education and 60% in health rated technical controls for data protection as 'high' now, compared to 26% in construction
- 64% of respondents the finance and insurance, 60% in education and 48% in health rated technical controls for other aspects of information/ cyber security 'high' now, compared to 26% in construction
- information and communication (46%) and property (55%) industries were also more likely than the average respondent (25%) to report technical controls for other aspects of information/ cyber security as high priority now

Change in priorities over the last 3 years

As Figure 3.22 and Figure 3.23 show, the proportion of respondents that reported technical controls as a higher priority was much larger than those who said it was a lower priority now compared to 3 years ago.

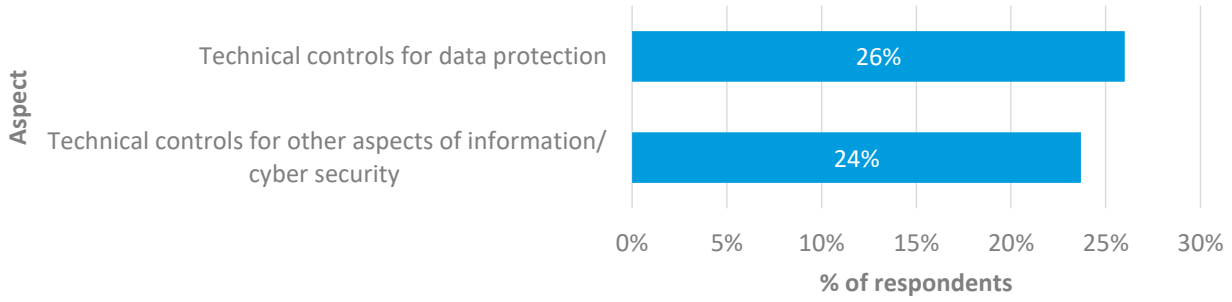
Organisations that had completed a DPIA or processed personal data were more likely to rate technical controls as higher priority now than 3 years ago, when compared to those that had not conducted a DPIA or did not process personal data.

Box 10: Proportion of respondents that rated technical controls as a higher priority now than 3 years ago by organisational characteristic

- 31% of organisations that had done a DPIA and 28% of those that processed personal data rated technical controls for data protection as a higher priority now, compared to 22% of those that had not conducted a DPIA and 17% of those that did not process personal data - there was no statistically significant variation in the responses of those that had or had not experienced an incident in relation to their prioritisation of technical controls for data protection
- 30% of organisations that had done a DPIA, 26% of those that processed personal data and 34% of organisations that experienced a cyber security rated technical controls for other aspects of information/cyber security as a higher priority now, compared to 19% of those that had not conducted a DPIA, 15% of those that did not process personal data and 22% of those that did not experience an incident

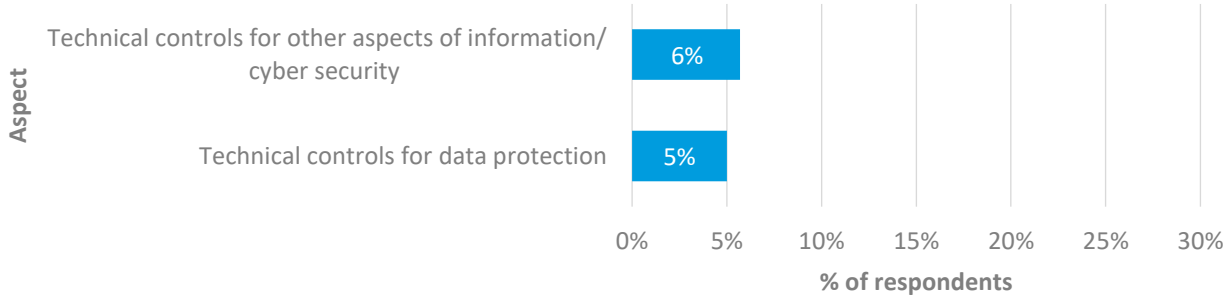
There was no statistically significant variation in how respondents who were IT or cyber security professionals answered these questions.

Figure 3.22: Proportion of respondents reporting technical controls as a higher priority now than 3 years ago



Source: Staff survey Q24cd. Proportion of respondents reporting aspects of cyber security higher priority now than 3 years ago
Weighted Base: 1,069
Unweighted Base: 1,129

Figure 3.23: Proportion of respondents reporting technical controls as a lower priority now than 3 years ago



Source: Staff survey Q24cd. Proportion of respondents reporting aspects of cyber security lower priority now than 3 years ago
Weighted Base: 1,069
Unweighted Base: 1,129

When considered by industry, respondents in arts, entertainment, recreation and other services; finance and insurance; education; and public administration and defence were more likely to have rated these aspects of cyber security as a higher priority now, compared to 3 years ago.

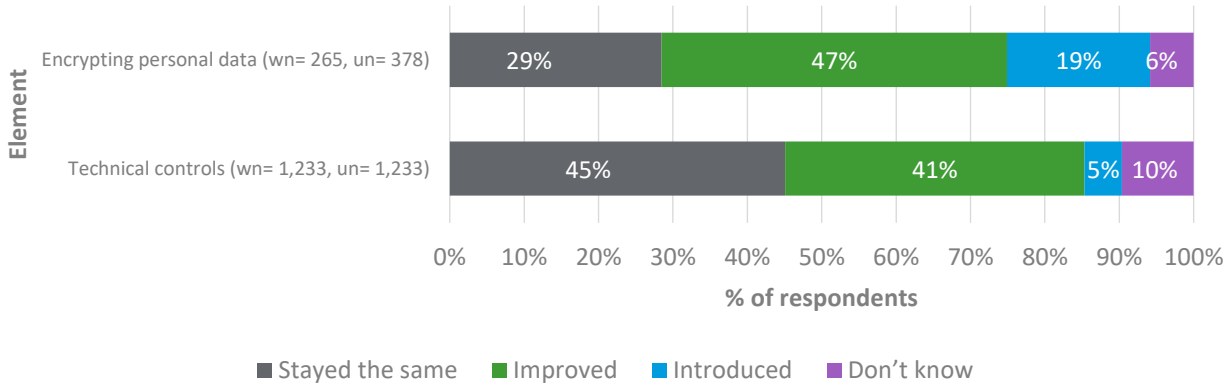
Box 11: Proportion of respondents that rated technical controls as a higher priority now than 3 years ago by industry

- 56% of respondents in arts, entertainment, recreation and other services, 48% in finance and insurance, 41% in education and 39% in public administration and defence rated technical controls for data protection a higher priority now, compared to 16% of respondents in information and communication
- 40% of respondents in arts, entertainment, recreation and other services, 44% in finance and insurance, 41% in education and 36% in public administration and defence rated technical controls for other aspects of information/cyber security a higher priority now than 3 years ago, compared to 24% of respondents to the staff survey

Encryption of personal data

As shown in Figure 3.24, most technical respondents said that their organisation had introduced and/or improved its encryption of personal data.

Figure 3.24: Changes in technical controls and encryption in the last 3 years



Source: Staff/Board survey Q26i/BQ25i. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years? And technical questions Q26p/BQ25p. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years?

Notes: wn= Weighted Base, un= Unweighted Base
Only respondents who considered themselves to be either an IT or cyber security professional were asked the technical question.
Totals may not sum to 100% due to rounding.
Respondents were also allowed to select both introduced and improved where applicable

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed how they encrypt personal data than those that had not experienced an incident or done a DPIA.

Box 12: Changes in encryption of personal data by organisational characteristic

- 80% of organisations that experienced an incident answered, 'introduced' and/or 'improved', compared to 58% of organisations that had not experienced an incident
- 75% of those that had done a DPIA, compared to 48% of organisations that had not
- 68% of those that processed personal data, compared to 51% of those that did not – note small base of 28 respondents for the latter

Organisations in the wholesale and retail industry and production industry were more likely to have changed how they encrypt personal data than the average respondent (83% and 80%, compared to 65%).[84]

Changes in technical controls

Around half of respondents said that their organisation had introduced and/or improved its technical controls (45%).[85] Board members were more likely to report changes to technical controls in the last 3 years than staff (62% of Board members reported changes, compared to 42% of staff).

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed their technical controls.

[84] *Totals do not match Figure 3.24 because respondents could select both introduced and improved where applicable*
[85] *As above, totals do not match Figure 3.24 because respondents could select both introduced and improved where applicable*

Box 13: Changes in technical controls by organisational characteristic

- 65% of organisation that experienced an incident answered 'introduced' and/or 'improved', compared to 42% that had not experienced an incident
- 52% of organisations that had done a DPIA, compared to 31% of those that did not conduct a DPIA
- 49% of organisations that processed personal data, compared to 29% of those that did not process personal data

IT or cyber security professionals were also more likely to report changes in their technical controls (59%) than those who were not IT or cyber security professionals (37%).

Organisations in the finance and insurance (77%); arts, entertainment recreation and other services (60%); education (56%); and information and communication industries (55%) were more likely to have introduced and/or improved technical controls than the average respondent (45%).[86]

[86] *As above, totals do not match Figure 3.24 because respondents could select both introduced and improved where applicable*

3.3.4 System security

Appropriate technical and organisation measures are implemented to protect systems, technologies and digital devices that process personal data from cyber attack. Whilst the GDPR requires a risk-based approach, typical expected examples of security measures that organisations can undertake include:

- tracking and recording of all assets that process personal data, including end user devices and removable media
- minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity
- actively managing software vulnerabilities, including using in-support software and the application of software update policies (patching) and taking other mitigating steps, where patches can't be applied
- managing end user devices (laptops and smartphones etc) so that organisational controls over software or applications that interact with or access personal data can be applied.
- encrypting personal data at rest on devices (laptops, smartphones, and removable media) that are not subject to strong physical controls
- encrypting personal data when transmitted electronically
- ensuring that web services are protected from common security vulnerabilities such as sql injection and others described in widely-used publications such as the owasp top 10.
- ensuring your processing environment remains secure throughout its lifecycle

Regular testing is also undertaken to evaluate the effectiveness of organisational security measures, including virus and malware scanning, vulnerability scanning and penetration testing as appropriate. Results of any testing and their remediating action plans are recorded.

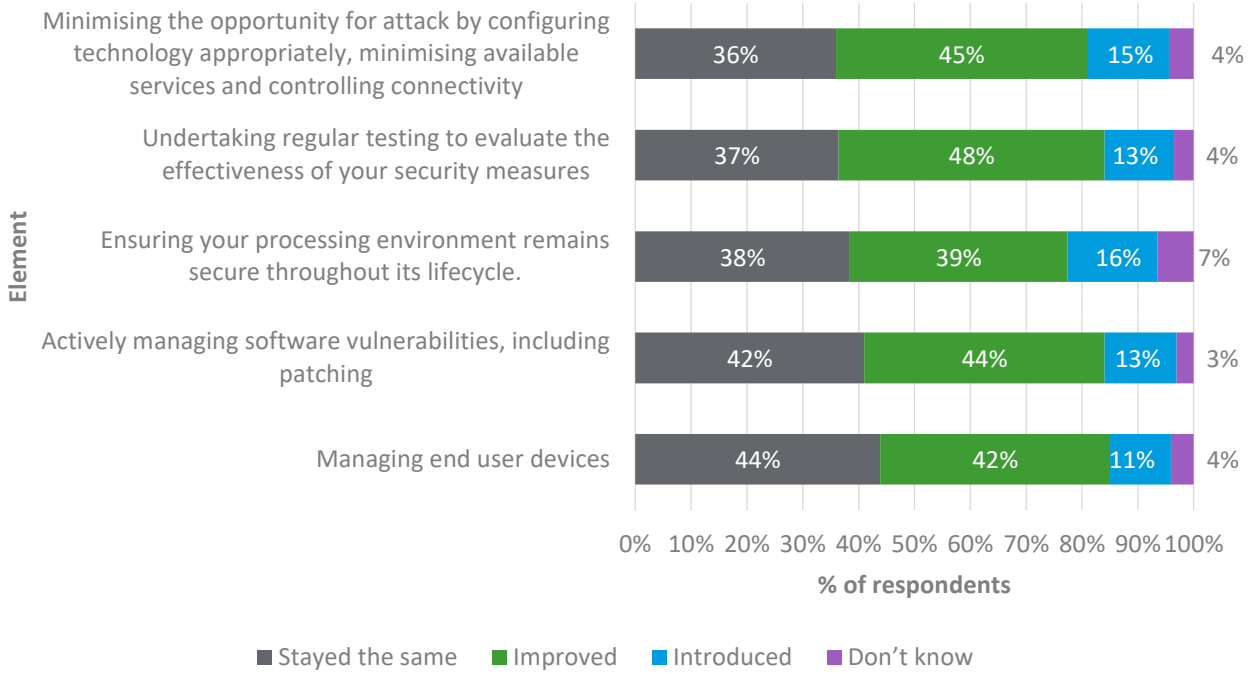
Whatever security measures are put in place, whether these are an organisation's own or whether through a third party service such as a cloud provider, organisations remain responsible both for the processing itself, and also in respect of any devices they operate.
(Source: NCSC)

In addition to findings presented in relation to data security (Section 3.3.3), tracking of assets (Figure 3.18) and service protection (Section 3.3.1), respondents who were IT or cyber security professionals were also asked about more technical changes to their system security.

Overall, based on the findings presented below, system security appears to have improved in the last 3 years.

As Figure 3.25 shows, the majority of respondents reported that these elements of their system security had been introduced and/or improved in the last 3 years.

Figure 3.25: Changes in system security in the last 3 years



Source: Staff survey, technical questions Q26. m,n,o,r and s. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years?
Weighted Base: 265
Unweighted Base: 378
Notes: Only respondents who considered themselves to be either an IT or cyber security professional were asked this question.
Totals may not sum to 100% due to rounding.
Respondents were also allowed to select both introduced and improved where applicable

3.3.4.1 Minimising the opportunity for attack

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed how they minimise the opportunity for attack than those who had not (75%, 69% and 63% respectively answered 'introduced' and/or 'improved', compared to 52% of organisations that had not experienced an incident, 69% of those that had not done a DPIA and 34% of those that did not process personal data – note the small base of 28 respondents for the latter group).

Organisations in health and production were more likely to have changed how they minimise the opportunity for attack than the average respondent (80% and 75% respectively, compared to 60%).

3.3.4.2 Undertaking regular testing to evaluate the effectiveness of security measures

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were also more likely to have changed how they undertake regular testing to evaluate the effectiveness of their security measures than those that had not experienced an incident, done a DPIA or processed personal data.

Box 14: Changes in testing to evaluate the effectiveness by organisational characteristic

- 76% of organisations that experienced an incident answered, 'introduced' and/or 'improved', compared to 53% of organisations that had not experienced an incident
- 70% of those that had done a DPIA, compared to 43% of those that had not done a DPIA
- 66% of those that processed personal data, compared to 23% of those that did not process personal data – note the small base of 28 respondents for the latter group

There was no statistically significant variation in response to this question by industry.

3.3.4.3 Ensuring the processing environment remains secure throughout its lifecycle

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed how they ensure their processing environment remains secure throughout its lifecycle than those that had not experienced an incident, done a DPIA or processed personal data.

Box 15: Changes in ensuring a secure processing environment by organisational characteristic

- 73% of organisations that experienced an incident answered, 'introduced' and/or 'improved', compared to 47% of those that had not experienced an incident
- 67% of organisations that had done a DPIA, compared to 34% of those that had not done a DPIA
- 60% of organisations that processed personal data, compared to 30% of those that did not process personal data – note small base of 28 respondents for the latter group

Organisations in the production industry were more likely than average to have changed how they ensure their processing environment remains secure throughout its lifecycle (70% answered 'introduced' and/or 'improved', compared to 55%).

3.3.4.4 Actively managing software vulnerabilities

Organisations that experienced a cyber security incident or had completed a DPIA were more likely to have changed how they were actively managing software vulnerabilities in the last 3 years.

Box 16: Changes in managing software vulnerabilities by organisational characteristic

- 77% of organisations that had experienced an incident answered, 'introduced' and/or 'improved', compared to 43% of organisations that had not experienced an incident
- 63% of those that had done a DPIA, compared to 38% of organisations that had not done a DPIA

There was no statistically significant variation in the responses of organisations that processed personal data and those that did not.

Technical respondents in the production industry were more likely to report changes in how they were actively managing software vulnerabilities than the average technical respondent (70% answered 'introduced' and/or 'improved', compared to 55%).[87]

3.3.4.5 Managing end user devices

Organisations that experienced a cyber security incident were more likely to have changed how they managed end user devices than those that had not experienced an incident or organisations that had not completed a DPIA (68% answered, 'introduced' and/or 'improved', compared to 43% and 44% respectively). There was no statistically significant variation in response to this question by whether or not the organisation processed personal data.

Organisations in the production industry were more likely to have changed how they managed end user devices than the average respondent (70% answered, 'introduced' and/or 'improved', compared to 52%).[88]

[87] *This does not match Figure 3.25 as respondents could select both introduced and improved where applicable*
[88] *As above, this does not match Figure 3.25 as respondents could select both introduced and improved where applicable*

3.3.5 Staff awareness and training

Staff are given appropriate support to help them manage personal data securely, including the technology they use. This includes relevant training and awareness as well as provision of the tools they need to effectively undertake their duties in ways that support the security of personal data. Staff should be provided with support to ensure that they do not inadvertently process personal data (for example, by sending it to the incorrect recipient).
(Source: NCSC)

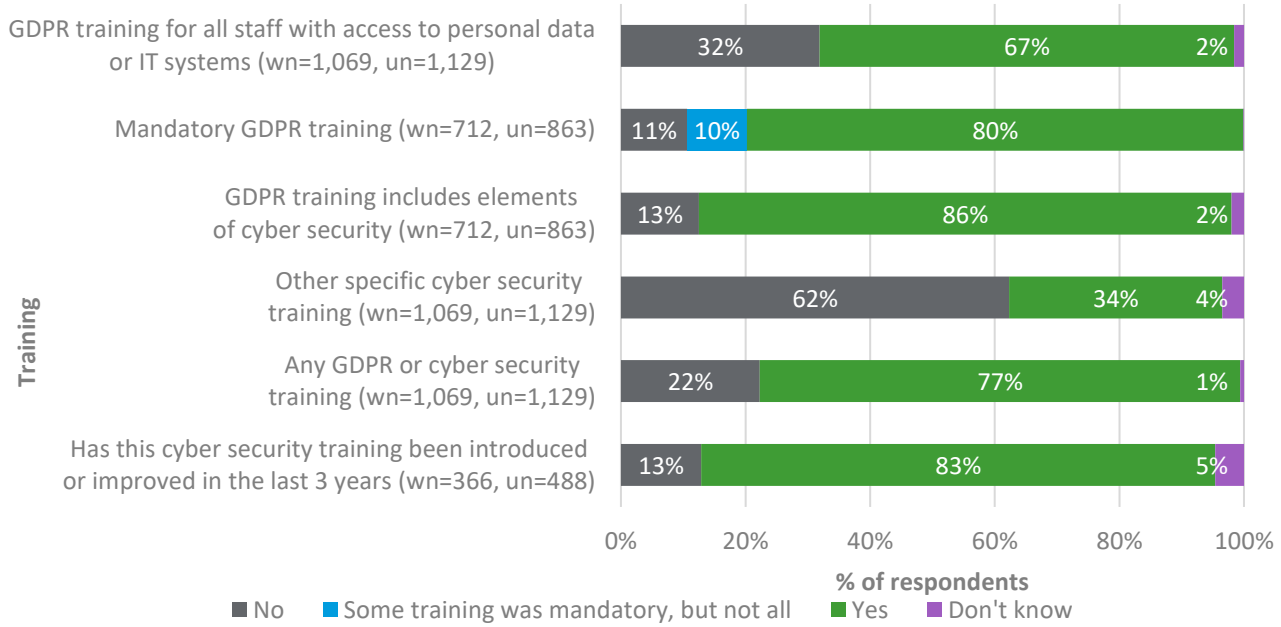
Many of the findings presented thus far indicate a focus on equipping staff with the appropriate knowledge and tools to manage data securely. These include: the creation of new data protection or cyber/information security roles (Figure 3.12); increased spending on cyber security in general (see Figure 3.29) and hardware and software in particular (Figure 3.28); increased prioritisation of growing in-house expertise; and increased prioritisation of data protection and other cyber security policies, processes, procedures and technical controls. We also explored changes in training provision in the last 3 years.

Overall, based on the findings presented below, there was some change in relation to staff awareness and training in the last 3 years.

3.3.5.1 GDPR training

While 67% of respondents to the staff survey said their organisation provided training on the GDPR for all staff who had access to personal data or IT systems, almost a third (32%) did not.

Figure 3.26: Training provided



Source: This chart is based on staff survey questions on the GDPR and cyber security training:
Q16. Do you provide GDPR training for all staff in your organisation who have access to personal data or IT systems?
Q17. Is any of this training mandatory?
Q18. Does this training include elements of cyber security (i.e. password protection, access control, patching, avoiding phishing etc.)?
Q19. Excluding other types of training that cover elements of cyber security only, do any staff within your organisation receive specific cyber security training (i.e. password protection, access control, patching, avoiding phishing etc.)? Q20. Has this training been introduced or improved in the last 3 years?
wn= Weighted Base, un= Unweighted Base
Notes: Totals do not sum to 100% as this Figure is based on responses to multiple questions
Only respondents who said they provided training were asked if it was mandatory, if it included elements of cyber security and if it had been introduced or improved in the last 3 years, hence smaller bases for these questions.

Where GDPR training was provided it was typically mandatory (80%) and generally included elements of cyber security (86%). For example, password protection, access control, patching and avoiding phishing (see Figure 3.26). Most interviewees in the qualitative interviews said that they provided training on the GDPR to all staff. This typically covered what the GDPR meant for them as an organisation and how they could be compliant:

> *"The reason that we provide compulsory training for all staff is to ensure that they know what their responsibilities are and what the GDPR means for them." (Interviewee from an MSP in the professional, scientific and technical industry)*

Unsurprisingly, organisations that completed a DPIA (82%), experienced a cyber security incident (79%) or processed personal data (71%) were also more likely than average to provide training on the GDPR. Provision of the GDPR training for all staff was more common in organisations in education (89%); arts, entertainment, recreation and other services (87%); health (85%); finance and insurance (80%); and public administration and defence (80%), compared to the average (67%).

Interviewees in organisations that had experienced a cyber security incident said that the reason they introduced GDPR training for all staff was to raise awareness of the risks:

> *"We experienced a cyber attack a couple of years ago and it had a huge impact on our organisation. Our cash flow in particular was severely affected. The attack happened when a member of staff was sent a phishing email and they clicked on the link as they were unaware that this was suspicious. We never want to be in this situation again, and you hear a lot of stories on the news about how these incidents are becoming more and more frequent. Looking back on it, if there was better awareness of phishing emails then this could have been avoided. This is probably the main reason for us introducing compulsory GDPR and cyber security training for all members of staff, so that they are more aware of the risks." (Interviewee from an LA/non-profit providing important public services in the health industry)*

3.3.5.2 Mandatory GDPR training

Where mandatory GDPR training was provided, most interviewees said it was provided to all staff to ensure they understood what the GDPR would mean for them, and how they could be compliant. A minority of interviewees, all from small organisations, said that they only provided training on the GDPR for staff members who handled data. They felt that this approach was necessary because they lacked the resources to offer mandatory GDPR training to all staff members.

One interviewee provided different levels of training depending on the responsibilities of the employee. They explained:

> *"The level of the GDPR and data protection training that we provide depends on how relevant [it is to the role of the employee] and how involved they would be with client data. Therefore, staff that have the most involvement received the most detailed training which we feel is a more efficient way of utilising the resources that we allocate to staff training". (Interviewee from an MSP in the production industry)*

Where training was provided, organisations that had completed a DPIA were more likely to provide mandatory GDPR training (82%) than those that had not (74%). There was also variation by industry- organisations in the finance and insurance (95%) and health industries (89%) were more likely to have provided mandatory GDPR training than those in production (63%) and public administration and defence (70%).

3.3.5.3 GDPR training included elements of cyber security

Interestingly, organisations that did not process personal data were more likely to have cyber security elements in their GDPR training (93%) than those that did process personal data (84%). This may be because those that processed personal data were more likely to have provided separate cyber security training (see below).

Organisations that had experienced a cyber security incident (91%) and those that had completed a DPIA (90%) were more likely than the average respondent to provide cyber security elements in their GDPR training (86%).

IT or cyber security professionals in organisations where GDPR training was provided for all staff were more likely to have said that this training included cyber security elements (92%) than respondents who were not IT or cyber security professionals (83%).

Organisations in the wholesale and retail industry were more likely to include elements of cyber security in their GDPR training (100%) than those in production (75%) and arts, entertainment, recreation and other services (76%).

3.3.5.4 Cyber security training

As shown in Figure 3.26, approximately a third of respondents (34%) said that staff within their organisation received specific cyber security training, for example password protection, access control, patching and avoiding phishing. This excluded training courses that only covered elements of cyber security (such as GDPR training).

Organisations that experienced a cyber security incident (57%), completed a DPIA (45%) or processed personal data (38%), were more likely than the average respondent to have provided specific cyber security training.

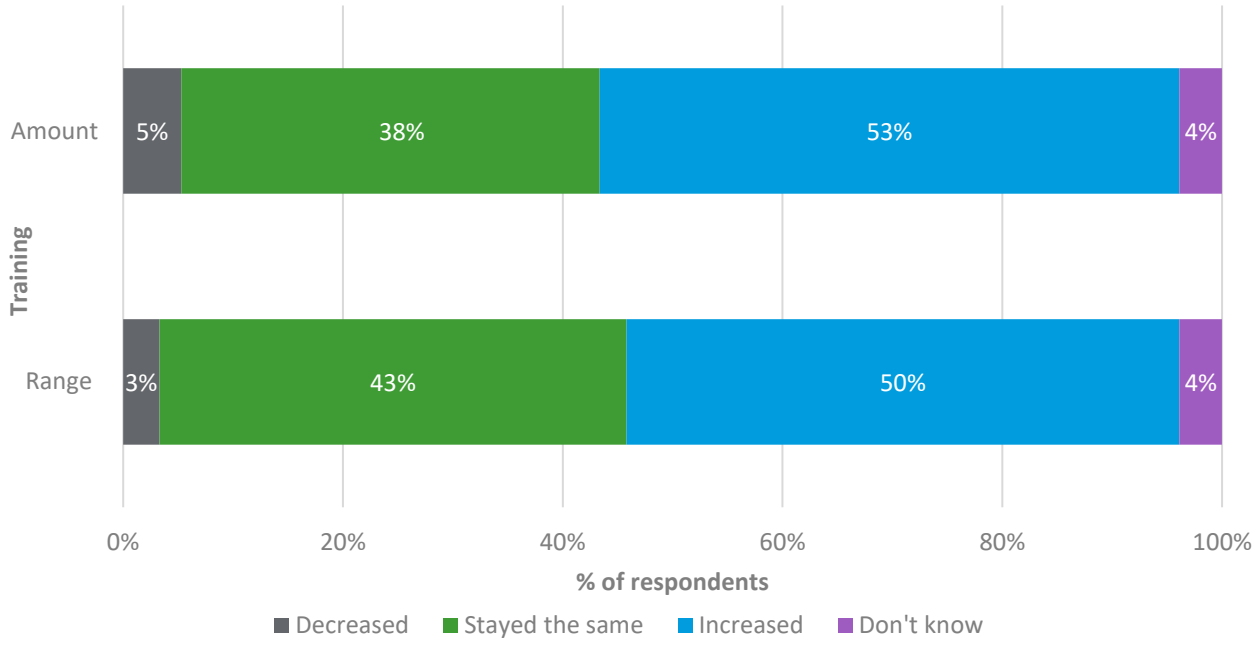
As Figure 3.26 also shows, where organisations provided specific cyber security training, this had typically been introduced or improved in the last 3 years (83%). Organisations that processed personal data (86%) and those that had completed a DPIA (85%) were also more likely to have introduced or improved this training in the last 3 years than the average respondent (83%).

This was more common among those working in the health industry (98%, compared to 83% of all respondents to the staff survey, had introduced/improved this).

When considered by industry, organisations in the production industry (61%), information and communication industry (51%) and finance and insurance industry (48%) were more likely to have provided specific cyber security training than organisations in the construction industry (23%) and public administration and defence (24%).

As previously mentioned in relation to staffing, 46% of Board members reported an increased prioritisation of growing in-house cyber security expertise. Similarly, approximately half of Board members reported an increase in their organisation's investment in the amount (53%) and range (50%) of cyber security training provided in the last 3 years (see Figure 3.27).

Figure 3.27: Change in cyber security training provided in the last 3 years



Source: Board survey BQ8cd. Has your organisation's investment in the following areas increased, decreased or stayed the same in the last 3 years since GDPR was announced in April 2016? Range of cyber security training provided; Amount of cyber security training provided.
Weighted Base: 164
Unweighted Base: 104

3.4 Detect security threats

Organisations can detect security events that affect the systems that process personal data and monitor authorised user access to that data.
(Source: NCSC)

3.4.1 Security monitoring

Organisations can detect security events that affect the systems that process personal data and monitor authorised user access to that data, including anomalous user activity.

Organisations record user access to personal data. Where unexpected events or indications of a personal data breach are detected, organisations have processes in place to act upon those events as necessary in an appropriate timeframe.
(Source: NCSC)

In addition to the improvements in tracking and recording assets (Figure 3.18), we explored changes in monitoring and review processes, including audit processes in the last 3 years.

Overall, based on the findings presented below, there was some change in relation to security monitoring in the last 3 years.

Half of respondents to both the staff and Board surveys (50%) said that their organisation had introduced and/or improved its monitoring and review processes in the last 3 years, including audit processes:[89]

- 42% of respondents answered 'stayed the same'
- 44% answered 'improved'
- 7% answered 'introduced'
- 8% answered 'don't know'

The types of changes reported by interviewees included:

> *"The changes we made to our monitoring processes involved putting in place new monitoring procedures. As a result of this we are now more diligent with our paperwork for new clients and new jobs." (Interviewee from an SME in the accommodation and food services industry)*

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed their monitoring and review processes, including audit processes than those that had not experienced an incident, completed a DPIA or processed personal data.

Box 17: Changes monitoring and review processes by organisational characteristic

- 69% of organisations that had experienced an incident answered, 'introduced' and/or 'improved', compared to 48% of those that had not experienced an incident
- 63% of those that had done a DPIA, compared to 32% of those that had not done a DPIA
- 55% of those that processed personal data, compared to 32% of those that did not process personal data

IT or cyber security professionals were more likely to report changes to monitoring and review, including audit processes (63%) than non-IT or cyber security professionals (44%).

Organisations in the finance and insurance industry, arts, entertainment, recreation and other services industry, education industry and health industry were more likely to have changed their monitoring and review processes than the average respondent (80%, 67%, 65% and 59% answered, 'introduced' and/or 'improved', respectively, compared to 50% of all respondents to both surveys).

The majority of interviewees reported that the changes they have made as a result of the GDPR have improved their ability to detect security threats:

> *"We changed our processes and it is now a requirement for us to monitor our systems so we can identify any weak points and could identify any signs that indicate that we may be about to experience a cyber attack. We now have the right procedures in place to identify current threats and would be able to quickly put measures in place to prevent an attack." (Interviewee from an MSP in the information and communication industry)*

> *"Before the GDPR was enforced we weren't very secure, simply because we didn't know how to be and what the risks were. As a result of the GDPR we made changes, because we wanted to be compliant and also because it made us more aware of the importance of being secure. We installed firewalls and anti-virus software on all our machines, and this has made us much better at detecting cyber security threats than we were before." (Interviewee from an LA/non-profit providing important public services in the health industry)*

[89] *Totals do not sum to because respondents were allowed to select both introduced and improved where applicable*

3.5 Minimising the impact

Organisations can:

- minimise the impact of a personal data breach
- restore their systems and services
- manage the incident appropriately
- learn lessons for the future

(Source: NCSC)

3.5.1 Response and recovery

Organisations have well-defined and tested incident management processes in place in case of personal data breaches. Mitigation processes are in place that are designed to contain or limit the range of personal data breach that could be compromised following a personal data breach.

Where the loss of availability of personal data could cause harm, measures are in place to ensure appropriate recovery. This should include maintaining (and securing) appropriate backups.
(Source: NCSC)

We explored changes in the Board's prioritisation of planning their response to cyber incidents and incident management or recovery processes in the last 3 years.

Overall, based on the findings presented below, there was some change in relation to response and recovery in the last 3 years.

The majority of Board members (54%) reported an increase in the Board's prioritisation of planning their response to cyber incidents in the last 3 years. 33% said that it stayed the same, while 8% reported a decrease in the prioritisation of this aspect of cyber security (6% did not know).[90]

Findings in relation to incident management or recovery processes were mixed. Almost half of respondents to both surveys (45%) said that their organisation had introduced and/or improved its incident management or recovery processes in the last 3 years. However, almost half of respondents (46%) said these had stayed the same. The remaining 9% did not know. [91]

While most of the interviewees who took part in the qualitative interviews reported making changes to their incident management and recovery processes as a result of the GDPR, those that did not make changes said this was because the incident management processes they had in place were already compliant with the GDPR.

[90] *Totals do not sum to 100% due to rounding*
[91] *Totals do not sum to 100% because respondents were allowed to select both introduced and improved where applicable*

Organisations that experienced a cyber security incident, completed a DPIA or processed personal data were more likely to have changed their incident management or recovery processes.

Box 18: Changes in incident management or recovery processes by organisational characteristic

- 66% of organisations that experienced an incident answered 'introduced' and/or 'improved', compared to 42% of those that had not experienced an incident
- 54% of those that had done a DPIA, compared to 30% of those that had not done a DPIA
- 50% of those that processed personal data, compared to 26% of those that did not process personal data

IT or cyber security professionals were more likely to report changes in their incident management or recovery processes than non-IT/cyber security professionals (58% and 39% answered 'introduced' and/or 'improved', respectively).

Organisations in finance and insurance, production and health were more likely to have changed their incident management or recovery processes than the average respondent (77%, 60% and 55% answered 'introduced' and/or 'improved', respectively, compared to 45% on average).

Some interviewees reported that the changes they have made as a result of the GDPR have improved their ability to minimise the impact and respond to and recover from a cyber security incident. This was mainly because they now have back-ups of their data, so if data was lost or stolen then they would be able to retrieve this. However, most interviewees reported that they were not sure if the changes they had made as a result of the GDPR had helped to minimise the impact. This was because these organisations had not experienced a cyber security incident and, although they would like to think they could respond to and recover from an incident, they could not definitively say if this was the case or if it had improved as a result of changes made.

3.5.2 Improvements

When a personal data breach occurs, steps are taken to:

- understand the root cause
- report the break to the Information Commissioner and where appropriate, affected individuals
- where appropriate or required, report other relevant bodies (for example, other regulators, the NCSC and/or law enforcement)
- take appropriate remediating action

(Source: NCSC)

Improvements in monitoring and review processes indicate that some organisations may be better equipped to identify and report a breach. The increased prioritisation of planning their response to cyber incidents and changes in incident management and recovery processes in some organisations also suggest that they may be better placed to take remediating action. The findings presented above also indicate that organisations that had experienced a cyber security incident were more likely to have made changes in line with the NCSC cyber security outcomes in the last 3 years than those that had not experienced an incident.

All of the cyber security incidents reported by those who took part in the qualitative interviews were phishing attacks where a member of staff had received a fraudulent email. The impacts of these incidents on the organisations varied in severity, ranging from a systems failure that lasted 24 hours

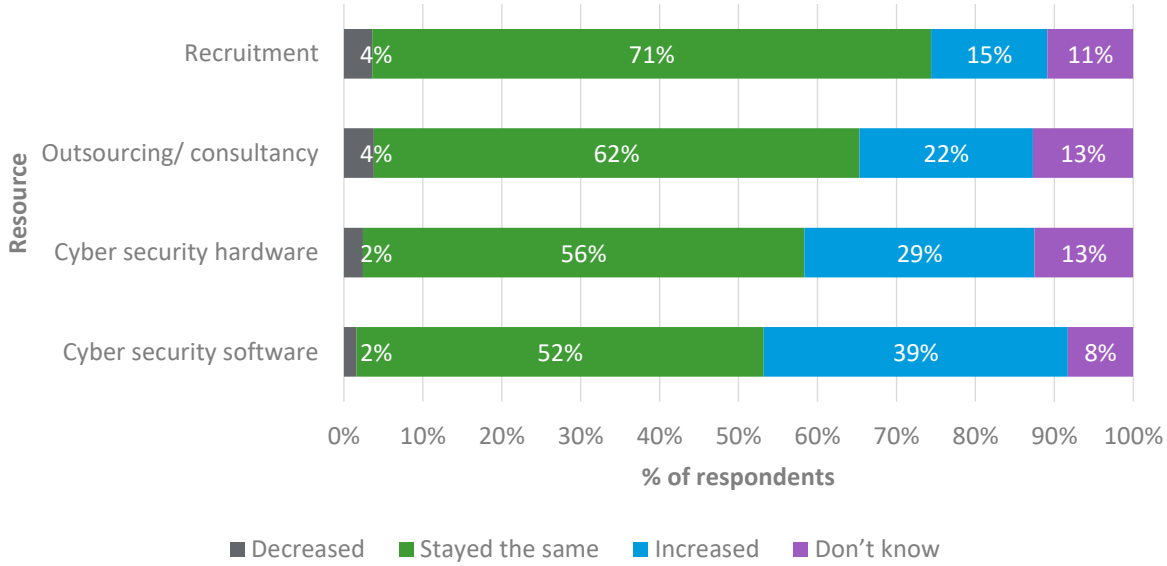
to cashflow problems that lasted several months. All affected interviewees reported that they responded by thoroughly checking their cyber security measures so they could understand how the breach occurred and reduce the chances that it would happen again. The interviewees also reported that they now provided mandatory staff training on phishing emails. Some organisations went further and introduced policies that required any suspected phishing emails to be reported so they could be investigated.

3.6 Cyber security expenditure

Staff survey

As Figure 3.28 shows, while a minority of respondents to the staff survey reported an increase in their organisation's expenditure on cyber security resources in the last 3 years (e.g. software, hardware, outsourcing/consultancy and recruitment), in most organisations it stayed the same.

Figure 3.28: Change in expenditure over the last 3 years



Source: Staff survey Q22. Has your organisation's expenditure on the following cyber security resources increased, decreased or stayed the same in the last 3 years?
Weighted Base: 1,069
Unweighted Base: 1,129

Some interviewees said that their organisation had increased expenditure on cyber security resources, including anti-virus software and cloud software such as Microsoft Azure. These interviewees reported that the increase in expenditure gave them more confidence in their cyber risk management and ability to store personal data securely, but that it was too early to definitively say if it this investment had reduced their risk from cyber attacks. This increase in expenditure indicates an increased focus on cyber security in some organisations, but it is not evidence of improvements in cyber security outcomes.

Where interviewees reported that their expenditure on cyber security resources had stayed the same, this was because what was already in place was considered sufficient to be compliant with the GDPR. These interviewees were confident in their ability to protect themselves from a cyber attack, so they felt it was not necessary to increase expenditure on cyber security resources.

Organisations that had experienced a cyber security incident, done a DPIA or processed personal data or were more likely to have increased expenditure on all cyber security resources.

Box 19: Increase in expenditure by organisational characteristic

- recruitment - 27% of respondents that had experienced a cyber security incident, 15% of those that had done a DPIA and 17% of those that processed personal data reported an increase in expenditure, compared to 13% of those that had not experienced an incident, 11% of those that had not done a DPIA and 5% of those that did not process personal data
- outsourcing/consultancy - 45% of those that had experienced an incident, 28% of those that had done a DPIA and 25% of those that processed personal data reported an increase in expenditure, compared to 18% of those that had not experienced an incident, 15% of those that had not done a DPIA and 8% of those that did not process personal data
- hardware – 45% of those that had experienced an incident, 36% of those that had done a DPIA and 32% of those that processed personal data reported an increase in expenditure, compared to 26% of those that had not experienced an incident, 21% of those that had not done a DPIA and 19% of those that did not process personal data
- software - 60% of those that had experienced an incident, 45% of those that had done a DPIA and 42% of those that processed personal data reported an increase in expenditure, compared to 35% of those that had not experienced an incident, 28% of those that had not done a DPIA and 25% of those that did not process personal data

Box 20: Increase in expenditure by industry

- organisations from the finance and insurance industry were more likely than the average respondent to have increased expenditure on all cyber security resources (36% reported increased expenditure on recruitment, 44% on outsourcing/consultancy, 60% on hardware and 60% software)
- organisations in the information and communication industry were more likely than average to have increased expenditure on recruitment (21%)
- health organisations were more likely than average to have increased expenditure on outsourcing/consultancy (34%) and software (47%)
- organisations in public administration and defence were more likely than average to have increased expenditure on outsourcing/consultancy (37%)

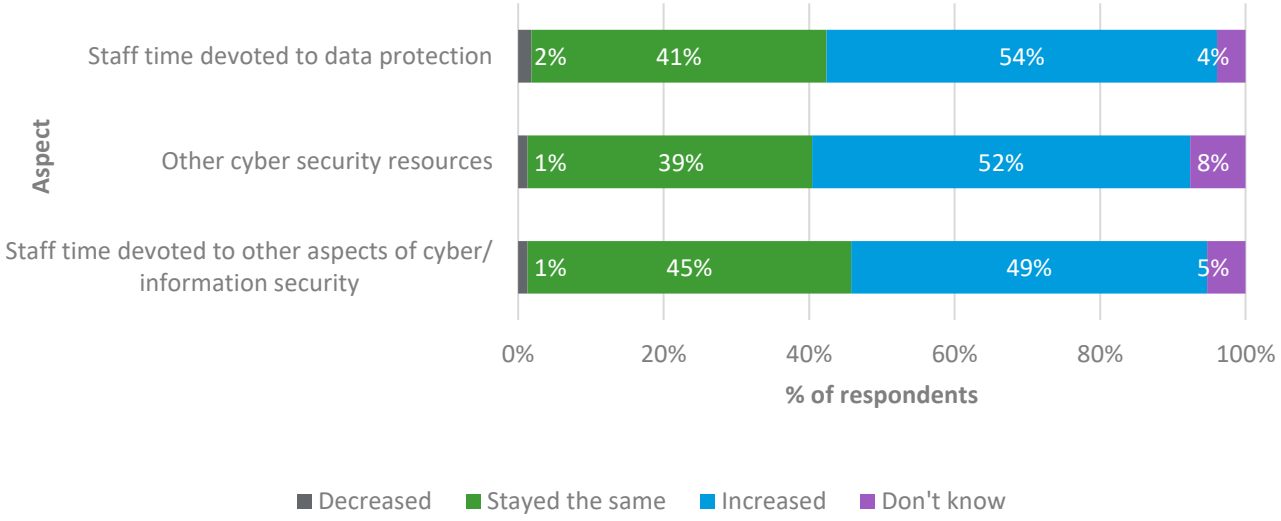
Overall, across the 4 categories of expenditure:

- 8% of respondents to the staff survey said that their organisation's expenditure had decreased in at least one of these areas in the last 3 years (software, hardware, outsourcing/consultancy and recruitment)
- 83% of respondents said that at least one area of expenditure had stayed the same
- 49% of respondents reported that they had increased expenditure in at least one area

Board survey

In contrast, as shown in Figure 3.29, approximately half of Board members (49%-54%) reported an increase in their organisation's spend on staff and other cyber security resources in the last 3 years (such as cyber security hardware, software, awareness raising, outsourcing/consultancy, recruitment). Where the Board members interviewed reported that expenditure on cyber security resources had stayed the same, this was because they felt that what they had in place was sufficient to be compliant with the GDPR.

Figure 3.29: Change in cyber security investment in the last 3 years



Source: Board survey BQ8abe. Has your organisation's spend on other cyber security resources increased decrease or stayed the same in the last 3 years?
Weighted Base: 164
Unweighted Base: 104

3.7 Breadth and duration of impact

Figure 3.30 shows that the vast majority of respondents agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas within their organisation (74%) and the changes that their organisation had implemented due to the GDPR have been sustained (84%).[92]

Breadth

Most interviewees agreed that the impact of the GDPR had been felt equally across all aspects of cyber security in their organisation. However, some interviewees disagreed and felt that as result of the GDPR, they were focusing too much on data protection:

> *"The GDPR has led to data security being prioritised over other areas of cyber security in our organisation. The changes that we made were more to do with managing data as opposed to improving our cyber security measures. For this reason, I don't think the GDPR has made us safer from a cyber attack, but our data is better protected than before." (Interviewee from an SME in the construction industry)*

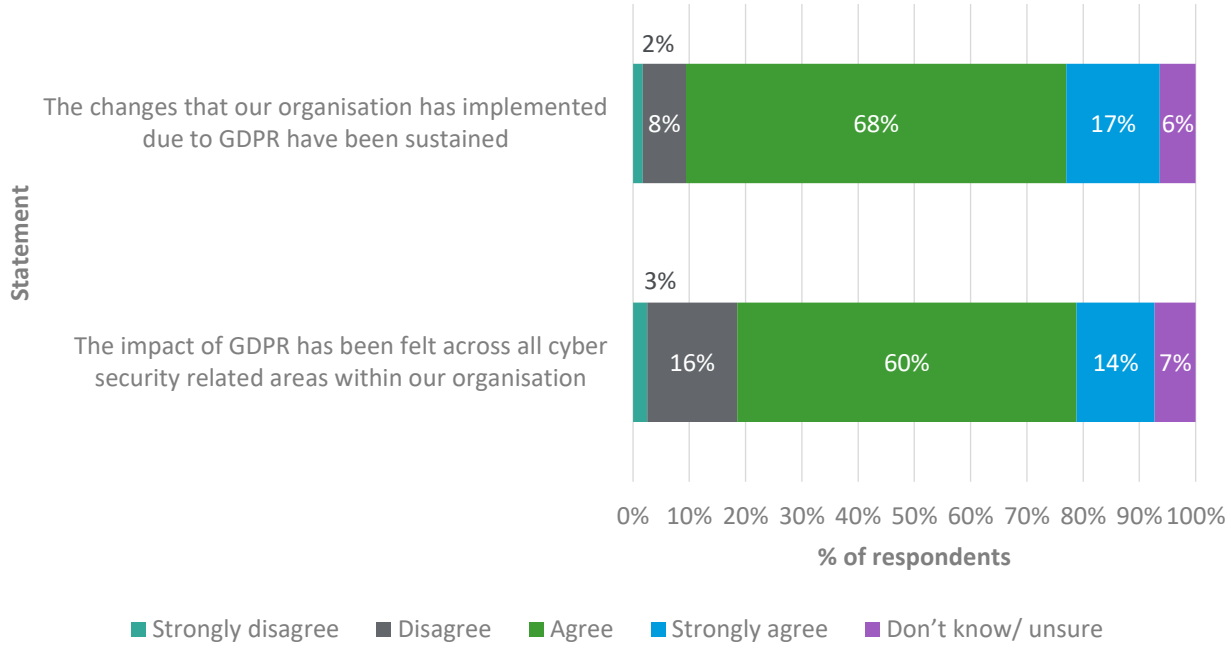
Board members were more likely than staff to have agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas within their organisation (91% of Board members agreed or strongly agreed, compared to 72% of staff). The Board members interviewed said that they ensured that all aspects of cyber security received equal amounts of resourcing and felt that all aspects of cyber security were focused on equally as a result. This contrasted with the opinions of most staff members interviewed who felt that in fact, data protection was being prioritised over other aspects of cyber security.

Those that processed personal data were more likely to have agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas in their organisation (78%), than those that did not process personal data (60%). Cyber security and IT professionals were also

[92] *Totals do not sum due to rounding*

more likely to agree or strongly agree with this statement (85%) than non cyber security and IT professionals (67%).

Figure 3.30: Breadth and duration of impact



Source: Staff and Board survey Q36/BQ31. To what extent do you agree or disagree with the following statements?
Weighted Base: 1,233
Unweighted Base: 1,233

Respondents in wholesale and retail were less likely than respondents in other industries to have agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas in their organisation.

Box 21: Proportion of respondents that agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas by industry

- education (94%)
- finance and insurance (93%)
- health (90%)
- arts, entertainment, recreation and other services (89%)
- production (86%)
- information and communication (83%)
- wholesale and retail (66%)

Interviewees from information and communication organisations felt that this was because they were already mostly compliant with the GDPR and, therefore, not many changes were required:

> *"As we are an IT company, we already knew a lot about cyber security, so we didn't have much to do to be compliant with the GDPR. I think because of this, we only had to make minimal changes to all aspects of cyber security, so I think the impact of the GDPR has been very equal." (Interviewee from an MSP in the professional, scientific and technical industry)*

It is also important to note that, although there was evidence that most organisations had improved their cyber risk management in the last 3 years, more improvements were reported in relation to preventative aspects such as governance, risk management, data security and system security.

Duration

While most interviewees reported that the changes they had made to their cyber security had been sustained, some interviewees said they were finding it challenging to sustain the changes made. These were typically SMEs or LAs/non-profits providing important services that had fewer resources and had more changes to make in order to become compliant. They were, therefore, incurring substantial additional ongoing expenses as a result of the GDPR. Another factor reported by interviewees as making it difficult to sustain changes was staff awareness that the GDPR is an ongoing issue and not a 'one-off':

> *"The main challenge for us is getting staff to realise that this isn't a 'one-off' and something that they no longer need to worry about, but it is ongoing and there needs to be a sustained level of investment to ensure that we don't go backwards and cease to be compliant with the GDPR." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

Board members were less likely than staff members to have disagreed or strongly disagreed that the changes made as a result of the GDPR had be sustained (4%, compared to 10%). Whereas, organisations that processed personal data (88%) and those that had not experienced a cyber security incident (86%) were more likely to have agreed or strongly agreed than those that did not process personal data (71%) or had experienced an incident (79%) that the changes made were sustained. Respondents who were IT or cyber security professionals were more likely to have disagreed or strongly disagreed that changes were sustained (14%) than other respondents (9%).

Respondents from the public administration and defence (95%), education (94%), health (97%), and arts, entertainment, recreation and other services (96%) industries were more likely than respondents in production (72%) to have agreed or strongly agreed that the changes made had been sustained.

It may be too soon to determine whether these changes have resulted in a longer-term behaviour change or a cultural shift towards more robust practices. This is a potential area for further research in the future.

3.8 Unintended consequences

Despite a very small proportion of respondents reporting a decrease in the priority of various aspects of cyber security in the last 3 years (see Figure 3.4 and Figure 3.23), findings in relation to the potentially detrimental consequences of the GDPR were mixed (see Figure 3.31).

The majority of respondents disagreed or strongly disagreed that the GDPR had led to:

- excessive investment in cyber security, significantly beyond what is necessary (60%)[93]
- excessive focus on data protection to the detriment of other aspects of cyber security (54%)

However, a substantial proportion of respondents agreed or strongly agreed with these statements (27% and 36% respectively). The proportion of respondents who agreed and disagreed that the GDPR had led to excessive caution amongst staff in the handling of data was approximately 50:50 (including those who strongly agreed or strongly disagreed). Some interviewees reported that the

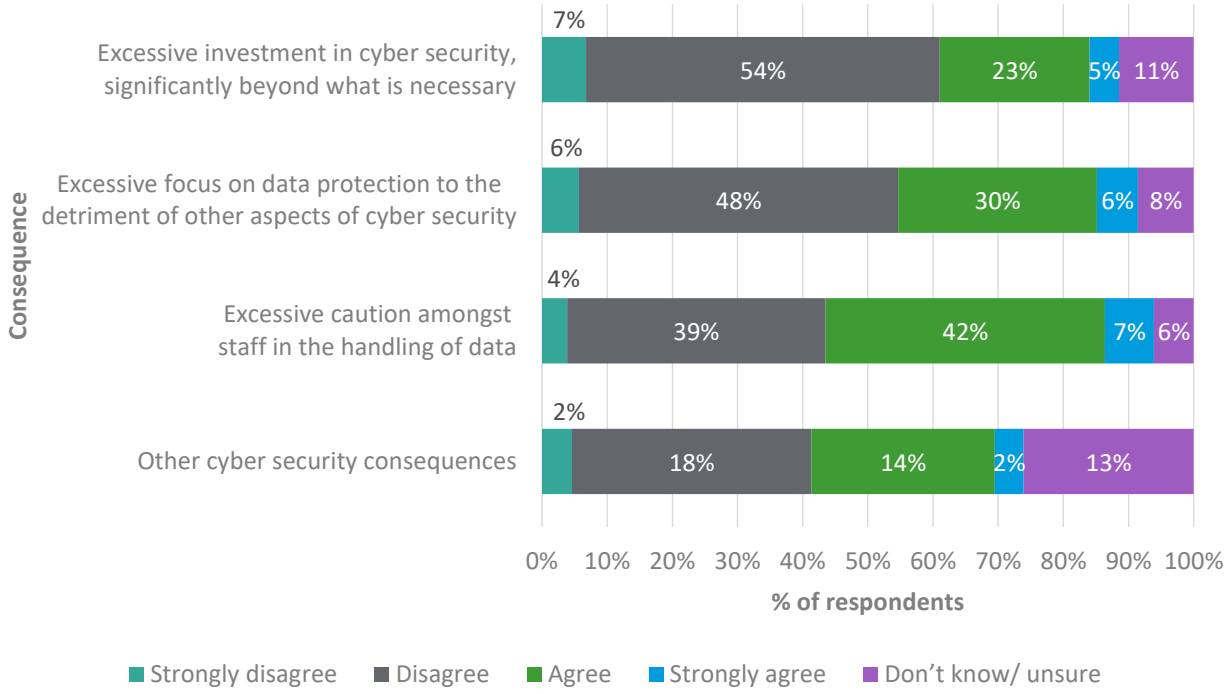
[93] *Does not match sum of percentages in Figure 3.31 due to rounding*

changes made as a result of the GDPR had not improved their organisation's ability to protect themselves against a cyber attack. One interviewee explained that this was because:

> *"The GDPR and cyber security are different things. The GDPR is about data protection and so has not had an impact on our ability to protect ourselves against a cyber breach." (Interviewee from an MSP in the professional, scientific and technical industry)*

This suggests organisations may benefit from further consideration and guidance on the appropriate balance between data protection and other aspects of cyber security when developing any future cyber security regulations and incentives.

Figure 3.31: Other consequences of the GDPR



Source: Staff and Board survey Q37/BQ32. To what extent do you agree or disagree that the GDPR has led to the following consequences in your organisation?
Weighted Base: 1,233
Unweighted Base: 1,233
Note: Respondents who answered, 'Other' were asked to specify. Examples of their responses included advice from ICO and ISO, protecting users.

The majority of organisations interviewed in our qualitative research stated that the amount of time and the cost of implementing changes to become compliant with the GDPR had a negative impact on their organisation, in particular interviewees stated:

> *"Lots of time was required to get everything sorted and implement the changes. Privacy impact assessments take time to do and this has resulted in delays on getting the new software that we need." (Interviewee from an LA/non-profit providing important public services in the education industry)*

> *"It has been very expensive to implement the changes, and it has probably cost more than they needed to spend. Lots of time spent implementing the changes that could have been spent*

doing other things." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)

"GDPR is an additional thing to constantly consider and maintain. It's extremely expensive for smaller organisations like us to implement GDPR compliant procedures." (Interviewee from an MSP in the information and communication industry)

Several interviewees felt that they were spending a disproportionate amount of time on data security, and not enough time on other aspects of cyber security, for example:

"As an organisation, we have become very focussed on IT controls, and on the cyber side of data protection. But risks are also high in terms of physical security as we often handle data physically. Since the GDPR was enforced, resources have been taken away from physical security in order to comply with the GDPR. We're concerned that physical security has essentially been side-lined as a result of implementation." (Interviewee from an LA/non-profit providing important public services in the health industry)

"People have become too focused on small areas of the GDPR. The risk of a cyber attack is low, but people have tied themselves into knots on what they should and shouldn't be saying and can and can't do. They often pick up one sentence in the legislation and get very worked up about it. Staff time has therefore been disproportionately concerned about elements of cyber security that are at such low risk of being breached and are likely to never be breached." (Interviewee from an LA/non-profit providing important public services in the health industry)

Excessive focus on data protection

Organisations that had not experienced a cyber security incident (58%) were more likely than those that had (36%) to have disagreed or strongly disagreed that the GDPR had led to excessive focus on data protection to the detriment of other aspects of cyber security. Respondents who were not IT or cyber security professionals were also more likely to have disagreed or strongly disagreed (60%) than IT or cyber security professionals (38%).

Respondents in public administration and defence (69%) and arts, entertainment, recreation and other services (81%) were more likely to have disagreed or strongly disagreed that the GDPR had led to excessive focus on data protection to the detriment of other aspects of cyber security, than those in the production industry (36%).

Excessive caution when handling data

Organisations that had not experienced a cyber security incident were more likely to have disagreed or strongly disagreed that the GDPR had led to excessive caution amongst staff in the handling of data (46%), than those that had experienced an incident (31%). Respondents who were IT or cyber security specialists were less likely to have disagreed or strongly disagreed with this statement (37%) than non-IT or cyber security specialists (46%). There was no statistically significant variation in the responses of those that processed personal data and those who did not.

Organisations in the professional, science and technical industry (58%) and the arts, entertainment, recreations and other services industry (58%) were also more likely to have disagreed or strongly disagreed that the GPDR had led to excessive caution amongst staff in the handling of data, than those in the finance and insurance industry (27%) and business administration and support service industry (30%).

Excessive investment in cyber security

Board members were more likely to have agreed or strongly agreed that the GDPR had led to excessive investment in cyber security than staff (36%, compared to 26%). Whereas organisations that processed personal data were more likely to have disagreed or strongly disagreed with this statement (62%). Organisations in public administration and defence (80%), health (77%) and arts, entertainment, recreations and other services (79%) were also more likely to have disagreed or strongly disagreed with this statement than other respondents (60%).

Other consequences

When asked if there was anything else they would like to add in relation to the impact of the GDPR on cyber security, the majority of respondents said no/nothing (85% of all respondents to both surveys), however, a number of respondents did provide comments which have been coded as follows:

- it has been good for the industry (3% of respondents)
- it has increased awareness of data handling/threats of cyber security (2% of respondents)
- the procedures have been unnecessary for small businesses (2% of respondents)
- there has been a lack of guidance/help (1% of respondents)
- it has increased workload/excessive amount of time spent on the GDPR (1% of respondents)
- it has not been enforced properly/people are ignoring procedures (1% of respondents)
- enforcing the GDPR is very important for cyber security (<1% of respondents)
- it was not as difficult as [they] thought it would be (<1% of respondents)
- it has been costly to implement the GDPR (<1% of respondents)

3.9 Aggregate picture

In most cases, organisations appear to have made some progress towards the NCSC GDPR security outcomes[94] in the last 3 years, as summarised below. However, there appeared to be greater focus on governance, risk management, data security and systems security. Less change was evident in relation to procurement and supply chain risk management. Most organisations had:

- improved data protection policies and information security policies (71% and 62% of all respondents to both surveys respectively)
- a cyber security strategy (69% of respondents to the Board survey)
- increased the Board of Directors' awareness of cyber security (65% of respondents to the Board survey)
- improved cyber security updates to the Board (83% of respondents to the Board survey said these had become more comprehensive, robust and responsive to external changes)
- increased Board prioritisation of understanding the threat (63% of respondents to the Board survey)
- improved encryption of personal data (65% of technical respondents to the staff survey)

[94] *NCSC guidance on GDPR security outcomes: HTTPS://WWW.NCSC.GOV.UK/GUIDANCE/GDPR-SECURITY-OUTCOMES (accessed May 2020)*

- improved their system security:
  - 60% of technical respondents to the staff survey changed how they minimise the opportunity for attack
  - 60% changed how they undertake regular testing to evaluate security measures
- provided training on the GDPR (67% of respondents to the staff survey)

Around half of the organisations surveyed had:

- had improved monitoring and review processes (50% of all respondents to both surveys)
- increased the Board's prioritisation of planning their response to cyber incidents (54% of respondents to the Board survey)
- improved incident management or recovery processes (45% of all respondents to both surveys)

This suggests that, in some cases, further change is required in order to improve cyber security, particularly in relation to improving cyber resilience and the 'non-preventative' aspects of cyber security.

The survey findings indicated that organisations that had experienced a cyber security incident were more likely to have made changes against the NCSC cyber security outcomes in the last 3 years than those that had not experienced an incident. As were organisations that had conducted a DPIA or those that processed personal data. It is important to note, however, that there was some overlap between these 3 groups. Organisations that processed personal data about consumers, service users or businesses or other organisations were more likely to have completed a DPIA (53%) or experienced a cyber security incident (16%) than those that did not process personal data (40% and 9% respectively).

This suggests that the GDPR has successfully encouraged improvement in cyber risk management for organisations that are within the scope of the regulation. It also indicates that organisations that are not in scope of the regulations, or those that think they are not in scope, could benefit from greater insight into the changing nature of cyber risks and the damage they can do to an organisation, without them having to undergo the trauma of an incident - as experience of an incident also appeared to encourage organisations to take action. Alternatively encouraging greater use of Business Impact Assessments and consideration of impact tolerances could help organisations to understand the specific impact of a potential breach and accept that it could happen to them.

3.9.1 Manage security risk

Most organisations had changed their organisational structures, policies and processes in the last 3 years to better enable them to understand, assess and systematically manage security risks to personal data. This is particularly true in relation to governance and risk management. Less change was evident in relation to supply chain risk management. However, it is concerning that a minority of organisations were not giving cyber security the strategic focus required:

- 31% of Board members surveyed said they had no formal cyber security strategy
- a substantial proportion of respondents still had no data protection or cyber/information security staff (35% and 54% respectively)
- only 33% of Board members were aware of the NCSC Board Toolkit and, of those who were aware of it only 34% had actually used it. This suggests that the Toolkit could be more widely publicised to Boards to increase their awareness of both the Toolkit and the benefits of using it
- over a third of Board members said they only received cyber security updates on an ad hoc basis (14%) or not at all (22% of respondents to the Board survey)

This suggests that more could be done to change this mindset in a minority of organisations. Potential interventions could include raising awareness of the business benefits of improving cyber security.

3.9.2 Protect personal data against cyber attack

The increased prioritisation of data protection and other cyber security policies, processes, and procedures, indicates a focus on the security of data and systems. Most organisations had changed security measures to protect personal data, and the systems that processed it, against cyber attack, especially in relation to data security (57% of Board members had increased the prioritisation of implementing effective technical cyber security measures and 65% of technical respondents to the staff survey had improved encryption of personal data) and system security (60% of technical respondents to the staff survey changed how they minimise the opportunity for attack, 60% changed how they undertake regular testing to evaluate security measures, 55% changed how they ensure the processing environment remains secure, 55% changed how they actively manage software vulnerabilities and 52% changed how they manage end user devices). Findings were mixed in relation to service protection policies and processes, identity and access control, and staff awareness and training.

3.9.3 Detect security threats

In addition to introducing new or improved tracking and recording of assets that process personal data (56% of technical respondents to the staff survey), half of organisations had introduced and/or improved their monitoring and review processes (50% of all respondents to both surveys) so that they can detect security events that affect the systems that process personal data and monitor authorised user access to that data.

3.9.4 Minimising the impact

Findings in relation to response and recovery were mixed. While most organisations reported an increase in the Board's prioritisation of planning their response to cyber incidents in the last 3 years (54% of respondents to the Board survey), 33% said that it stayed the same and 8% reported a decrease in the prioritisation of this aspect of cyber security. Similarly, while almost half of organisations had introduced and/or improved their incident management or recovery processes in the last 3 years (45% of all respondents to both surveys), almost half of respondents said these had stayed the same (46%).

3.9.5 Cyber security expenditure

The increased spending on cyber security in general (52% of Board members reported an increased investment in cyber security resources), and hardware and software in particular (29% and 39% of respondents to the staff survey respectively), indicates a greater prioritisation of cyber security. However, this cannot be assumed to equate to better cyber security outcomes.

3.9.6 Breadth and duration of impact

While most organisations said that the impact of the GDPR had been felt across all cyber security related areas within their organisation (74% of all respondents to both surveys), more improvements were reported in relation to governance, risk management, data security and system security. We also found that organisations were more likely to have made changes to data protection than other aspects of cyber security (see unintended consequences).

Most organisations said the changes that their organisation had implemented due to the GDPR have been sustained (84%). Challenges to sustainability mainly related to the ongoing costs associated

with maintaining compliance and staff awareness that the GDPR was an ongoing issue, not a 'one-off'.

3.9.7 Unintended consequences

Some organisations felt that the GDPR had resulted in detrimental impacts, particularly in relation to excessive caution amongst staff in the handling of data (50% of all respondents to both surveys). The majority of Board members (78% of respondents to the Board survey) said that the cyber security updates received by the Board had become more focused on data protection than general cyber security in the last 3 years. As noted above, organisations were also more likely to have made changes to data protection than other aspects of cyber security:

- 58% of respondents to the staff survey had at least 1 FTE devoted to data protection, while only 36% had at least 1 additional cyber security FTE
- 54% of respondents to the Board member survey said that the staff time devoted to data protection had increased in the last 3 years, while only 49% said that the staff time devoted to other aspects of cyber security had increased in during that time
- 67% of respondents to the staff survey provided training on the GDPR, in most cases this training included aspects of cyber security (86%), however, only 34% provided specific cyber security training
- respondents to the staff survey were also more likely to report an increase in the priority of policies, processes, procedures and technical controls for data protection than for other aspects of cyber security

This suggests that organisations would benefit from further consideration and guidance on the appropriate balance between data protection and other aspects of cyber security when developing any future cyber security regulations and incentives.

3.9.8 Variation by industry

At an industry level, organisations in the finance and insurance industry were more likely than other respondents to have made positive changes to their cyber security in the last 3 years. Interviewees attributed this to the volume and nature of personal data that they hold, which could be more valuable to a potential attacker. The finance and insurance industry is a heavily regulated industry, which may also have influenced the changes made. Organisations in the finance and insurance industry were more likely than other respondents to have:

- at least one employee who specialised in data protection and cyber security
- completed a DPIA
- rated all cyber security aspects as high priority now
- said these were a higher priority now, compared to 3 years ago
- changed more aspects of their cyber security
- provided training on the GDPR
- provided specific cyber security training
- increased their expenditure on all cyber security resources – for example software, hardware, outsourcing/consultancy and recruitment
- said that the impact of the GDPR had been felt across all aspects of cyber security
- felt that the GDPR had led to excessive caution amongst staff in the handling of data

4 FACTORS DRIVING CHANGE

Summary

GDPR was considered the most important factor driving change in cyber security in the last 3 years:

- 23% of all respondents to both surveys named the introduction of the GDPR the most important factor
- 19% said desire to comply and avoid penalties

This was supported by the findings of the qualitative interviews. Increased awareness of the financial (5%) and reputational (5%) costs of cyber attacks were the next most popular responses.

Respondents that had experienced an incident were more likely than those that had not to have stated that 'perceived, heightened external threat of cyber attacks in their industry' had influenced changes in their cyber security in the last 3 years (34%, compared to 27%). While respondents that had completed a DPIA or that processed personal data were more likely than those that had not done a DPIA or did not process personal data to have cited a range of factors, indicating a higher level of awareness of the diverse range of factors.

The vast majority of respondents also said that the GDPR had influenced all of the changes in their organisation's cyber security over the last 3 years, at least to a small extent (82%). This was more common amongst respondents that had completed a DPIA, experienced a cyber security incident or processed personal data than those that had not.

Where respondents had not made changes to a particular aspect of their cyber security practices (79% of respondents) they were asked why not. The main reason given was that they felt existing measures were sufficient (61%). Organisations that did not process personal data (69%), had not experienced an incident (66%) or had not completed a DPIA (55%) were more likely to give this reason than those that had experienced an incident (37%). It is possible, however, that in some cases organisations may benefit from assistance in assessing their risk posture and the appropriateness of the measures they have taken, for example, by making organisations more aware of the:

- changing nature of cyber security threats
- full extent of the cyber security implications of the GDPR
- benefits to their business of improving their cyber security

4.1 Context

As discussed in Section 2 of this report, the prior literature and research indicated a wide range of factors impacting change in organisations' cyber security. The 2016 Cyber Security Regulation and Incentives Review[95] identified the GDPR as a potential driver for improvements. We sought to investigate this through our primary research.

[95] *HM Government (2016) Cyber Security Regulation and Incentives Review*

Note: While total responses can be generalised, survey findings by industry are indicative and should not be generalised to represent the wider population.

4.2 Range of factors

As shown in Figure 4.1, when asked what factors had specifically influenced cyber security changes made in the last 3 years, the majority of respondents chose those linked to the GDPR. Desire to comply with the GDPR and avoid penalties was the most popular response (66%), followed by the introduction of the GDPR generally (63%). Increased or greater awareness of the financial cost (51%) and reputational cost (49%) of potential data breaches or cyber-attacks were also popular responses.

The vast majority of interviewees said that they were motivated to make changes to their cyber security by the GDPR, as well as other factors. This highlights that regulation played a key part in the multiple factors that influence organisations' behaviour. The other factor cited by most interviewees was awareness of the increasing prevalence of cyber attacks.

Other factors mentioned by interviewees included:

- regular reviews of their cyber security which highlighted areas for improvements
- new technology to support and enable that change, for example Cloud storage, which made it easier for them to store personal data securely
- outsourced cyber professionals highlighting the need to improve cyber security policies and processes
- increasing client base/increase in the number of clients who expected compliance with the GDPR
- previous experience of a cyber incident
- increased frequency of flexible and remote working

Most interviewees reported that the GDPR was the most powerful factor influencing the changes made. The most common reason for this was that organisations wanted to be compliant with the GDPR, either because they wanted to avoid financial penalties for non-compliance or because their clients expected them to be compliant.

The majority of interviewees reported that their reaction to the GDPR was driven by a desire to be compliant with the regulations:

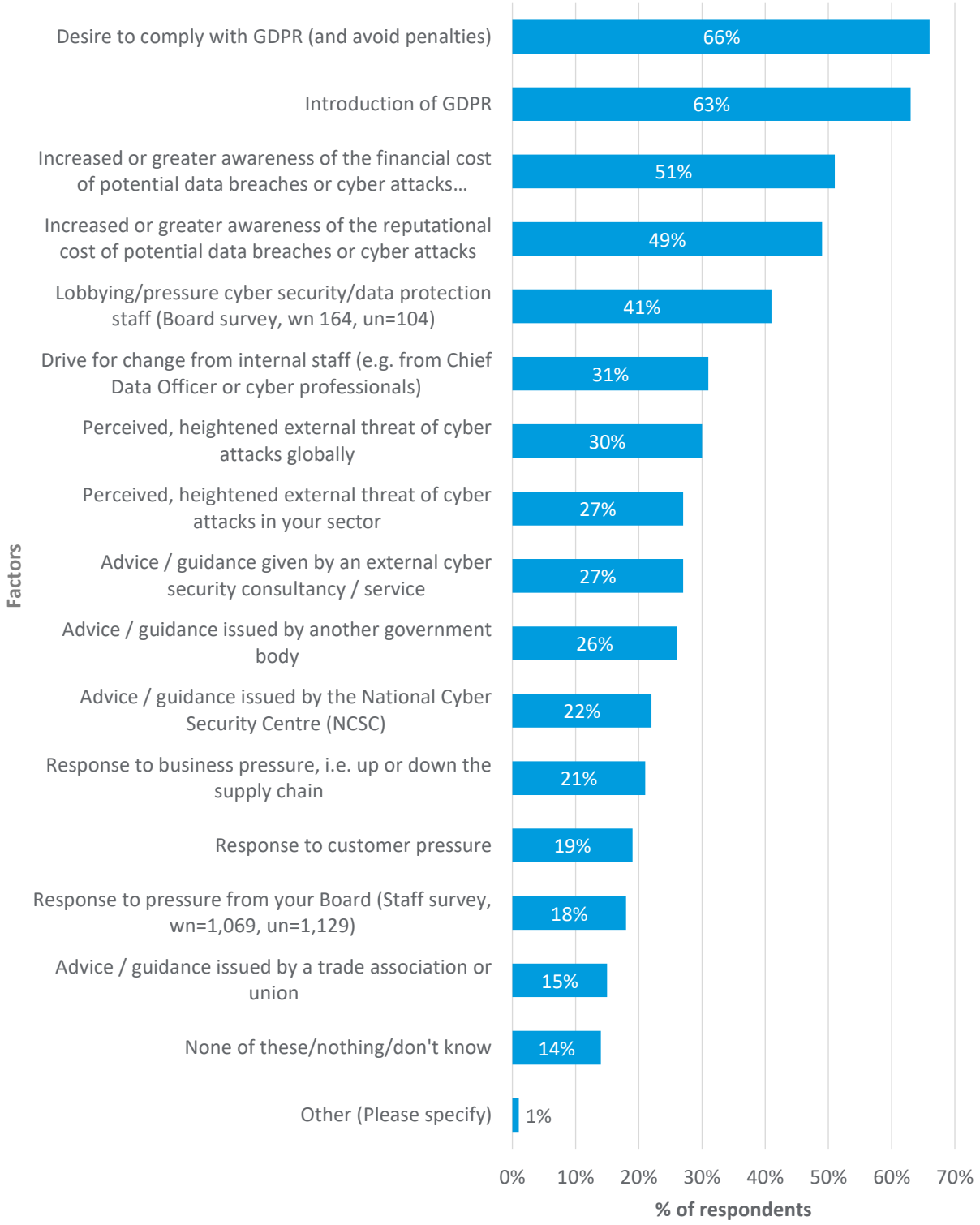
> *"It was mainly a compliance issue, it's a regulation and the law and it was important to comply with it." (Interviewee from an LA/non-profit providing important public services in the health industry)*

> *"It is important for us to be compliant with regulations, and to ensure that personal data is handled correctly." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

> *"We want to be looked upon as being the leaders of the sector and as being compliant with the GDPR, so we took this very seriously." (Interviewee from an SME in the health industry)*

Some of the interviewees reported that they reacted in the way that they did in order to avoid financial penalties for non-compliance. This response was more likely from SMEs and LAs/non-profits providing important public services, who said they would have severe financial issues and may be unable to continue operating if they had to pay a fine for non-compliance.

Figure 4.1: Factors that have influenced these changes



Source: Staff and Board survey Q33/BQ28. Reflecting on your answers to these questions, where you have made changes to your organisation's cyber security personnel, training, resources, priorities and activities, which of the following factors, if any, have influenced these changes?
Weighted Base: 1,233
Unweighted Base: 1,233
Note: Totals do not sum to 100% because respondents could choose more than one option.
Respondents who answered, 'Other' were asked to specify. Examples of their responses included advice from ICO, ISO, and advice from a variety of organisations.

Some interviewees stated that they reacted in this way because they were driven by customers and clients:

> *"Our client base has grown over the last few years and our new clients required the organisation to be GDPR compliant and to treat cyber security as a high priority." (Interviewee from a non-profit in the information and communication industry)*
>
> *"Due to many high-profile stories in the news over the last few years about cyber attacks, our customers are obviously concerned about what might happen to their personal data if we were to suffer a breach. This is what motivated us to ensure that we had robust measures in place, and part of that was to ensure that we were compliant with the GDPR." (Interviewee from a non-profit in the professional, scientific and technical industry)*

There was some variation in response to this question by industry and type of respondent. Where these variations were statistically significant, they are summarised below.

Board members were more likely than staff to have said that changes in their organisation were influenced by factors other than the GDPR.

Box 22: Factors influencing change by type of respondent

- 63% of Board members cited increased or greater awareness of the financial cost of potential data breaches or cyber attacks (excluding penalties), compared to 49% of staff
- 63% of Board members cited increased or greater awareness of the reputational cost of potential data breaches or cyber attacks, compared to 47% of staff
- 39% of Board members cited advice/guidance given by an external cyber security consultancy/service, compared to 25% of staff
- 21% of Board members cited advice/guidance issued by a trade association or union, compared to 14% of staff
- 43% of Board members cited perceived, heightened external threat of cyber attacks in their industry, compared to 25% of staff
- 46% of Board members cited perceived, heightened external threat of cyber attacks globally, compared to 28% of staff
- 49% of Board members cited drive for change from internal staff, compared to 28% of staff
- 40% of Board members cited response to business pressure (i.e. up or down the supply chain), compared to 18% of staff
- 33% of Board members cited response to customer pressure, compared to 17% of staff

As previously noted, the survey findings indicated that organisations that had experienced a cyber security incident were more likely to have made changes against the NCSC cyber security outcomes in the last 3 years than those that had not experienced an incident. It is not surprising, therefore, that respondents that had experienced an incident were more likely than those that had not to have stated that 'perceived, heightened external threat of cyber attacks in their industry' had influenced changes in their cyber security in the last 3 years (34%, compared to 27%). Interviewees from organisations that had experienced a cyber attack said that they made changes to ensure that the risk of another cyber attack was reduced. However, those that had not experienced a cyber security incident were more likely to have attributed changes made to almost every other factor, with the exception of: 'advice/guidance issued by a trade association or union'; 'perceived, heightened external threat of cyber attacks globally'; 'response to business pressure'; and 'response to customer pressure' – for which there was no significant variation in how both groups responded.

Respondents that had completed a DPIA were more likely than those that had not to have cited every factor as an influence, indicating a higher level of awareness of the diverse range of factors.[96] Similarly, respondents from organisations that processed personal data were more likely than those that did not to have given each response option, with the exceptions of 'advice/guidance issued by a trade association or union' and 'lobbying or pressure from staff responsible for cyber security/data protection' for which there was no significant variation in the proportion of respondents.

Respondents who were cyber security or IT professionals were more likely than average to have cited a range of external factors, such as 'advice/guidance issued by the NCSC' (27%), 'response to business pressure' (27%) as well as 'response to pressure from the Board' (23%) (compared to 22%, 21% and 16% of all respondents to both surveys, respectively).

When variation in response was considered by industry, those providing public services, (such as respondents in public administration and defence, education and health) were more likely than the average respondent to have cited a combination of factors relating to the GDPR and external advice whereas, respondents in finance and insurance and the information and communication industries were more likely than the average respondent to have cited external factors, other than the GDPR.

Box 23: Factors influencing change by industry[97]

Note: While total responses can be generalised, survey findings by industry are indicative and should not be generalised to represent the wider population.

- agriculture, forestry and fishing respondents were more likely to have reported 'desire to comply with the GDPR and avoid penalties' when compared to the average respondent (82% of agriculture, forestry and fishing respondents, compared to 66% of all respondents to both surveys)
- public administration and defence respondents were more likely to have said:
  - 'introduction of the GDPR' (77%, compared to 63%)
  - 'advice/guidance issued by another government body' (48%, compared to 26%)
  - 'advice/guidance issued by a trade association or union' (24%, compared to 15%)
- education respondents were more likely to have answered:
  - 'desire to comply with the GDPR and avoid penalties' (82%, compared to 66%)
  - 'introduction of the GDPR' (80%, compared to 63%)
  - 'increased or greater awareness of the financial cost of potential data breaches or cyber attacks, excluding penalties' (63%, compared to 51%)
  - 'increased or greater awareness of the reputational cost of potential data breaches or cyber attacks' (64%, compared to 49%)
  - 'advice/guidance given by an external cyber security consultancy/service' (38%, compared to 27%)
  - 'drive for change from internal staff' (43%, compared to 31%)
  - 'response to pressure from the Board' (26%, compared to 16%)

[96] *With the exception of lobbying or pressure from staff responsible for cyber security/data protection, which was only asked on the Board survey*

[97] *Note: this analysis focuses on identifying any significant variation by industry rather than presenting the most popular answer by industry*

- respondents in the health industry were more likely to have answered:
  - ‘desire to comply with the GDPR and avoid penalties’ (81%, compared to 66%)
  - ‘introduction of the GDPR’ (81%, compared to 63%)
  - ‘increased or greater awareness of the reputational cost of potential data breaches or cyber attacks’ (62%, compared to 49%)
  - ‘advice/guidance issued by another government body’ (46%, compared to 26%)
  - ‘response to pressure from the Board’ (30%, compared to 16%)
- wholesale and retail respondents (including repair of motor vehicles) were more likely to have answered, ‘advice/guidance issued by the NCSC’ than the average respondent (29%, compared to 22%)
- respondents in the property industry were more likely to have answered ‘advice/guidance given by an external cyber security consultancy/service’ (41%, compared to 27%)
- production respondents were more likely to have cited ‘response to business pressure, i.e. up or down the supply chain’ than the average respondent (31%, compared to 21%)
- respondents from finance and insurance organisations were more likely than average to have cited other external factors:
  - ‘increased or greater awareness of the reputational cost of potential data breaches or cyber attacks’ (63%, compared to 49%)
  - ‘advice/guidance issued by another government body’ (43%, compared to 26%)
  - ‘perceived, heightened external threat of cyber attacks in their industry’ (40%, compared to 27%)
  - ‘drive for change from internal staff’ (43%, compared to 31%)
  - ‘response to pressure from their Board’ (27%, compared to 16%)
- respondents in the information and communication industry were more likely, than the average respondent to have cited external factors, other than the GDPR, as well as pressure from their Board:
  - ‘advice/guidance issued by another government body’ (34%, compared to 26%)
  - ‘perceived, heightened external threat of cyber attacks in their industry’ (35%, compared to 27%)
  - ‘response to business pressure, i.e. up or down the supply chain’ (34%, compared to 21%)
  - ‘response to customer pressure’ (35%%, compared to 19%)
  - ‘response to pressure from the Board’ (23%, compared to 16%).
- respondents from the professional, scientific and technical industry were more likely to have cited ‘lobbying or pressure from staff responsible for cyber security/data protection’ (10%, compared to 6%)
- respondents in the arts, entertainment, recreation and other services were more likely than the average respondent to have given almost every response option:
  - ‘desire to comply with the GDPR and avoid penalties’ (87%, compared to 66%)
  - ‘introduction of the GDPR’ (89%, compared to 63%)

- ‘increased or greater awareness of the financial cost of potential data breaches or cyber attacks (excluding penalties)’ (73%, compared to 51%)
- ‘increased or greater awareness of the reputational cost of potential data breaches or cyber attacks’ (79%, compared to 49%)
- ‘advice/guidance given by an external cyber security consultancy/service’ (41%, compared to 27%)
- ‘advice/guidance issued by another government body’ (50%, compared to 26%)
- ‘advice/guidance issued by the NCSC’ (33%, compared to 22%)
- ‘advice/guidance issued by a trade association or union’ (29%, compared to 15%)
- ‘perceived, heightened external threat of cyber attacks globally’ (42%, compared to 30%)
- ‘perceived, heightened external threat of cyber attacks in their industry’ (42%, compared to 27%)
- ‘drive for change from internal staff’ (50%, compared to 31%)
- ‘response to pressure from the Board’ (46%, compared to 16%)

Most important factor

When asked what the most important factor was, introduction of the GDPR (23%) and the desire to comply with it and avoid financial penalties (19%) came top. Over a quarter of respondents said that all factors were important and they were unable to choose (26%).

Staff were more likely than Board members to rank ‘introduction of the GDPR’ as the most important factor influencing cyber security changes (24% of staff, compared to 14% of Board members). While Board members were more likely than staff to have said that they were unable to choose one factor as the most important factor (39% of Board members compared to 24% of staff).

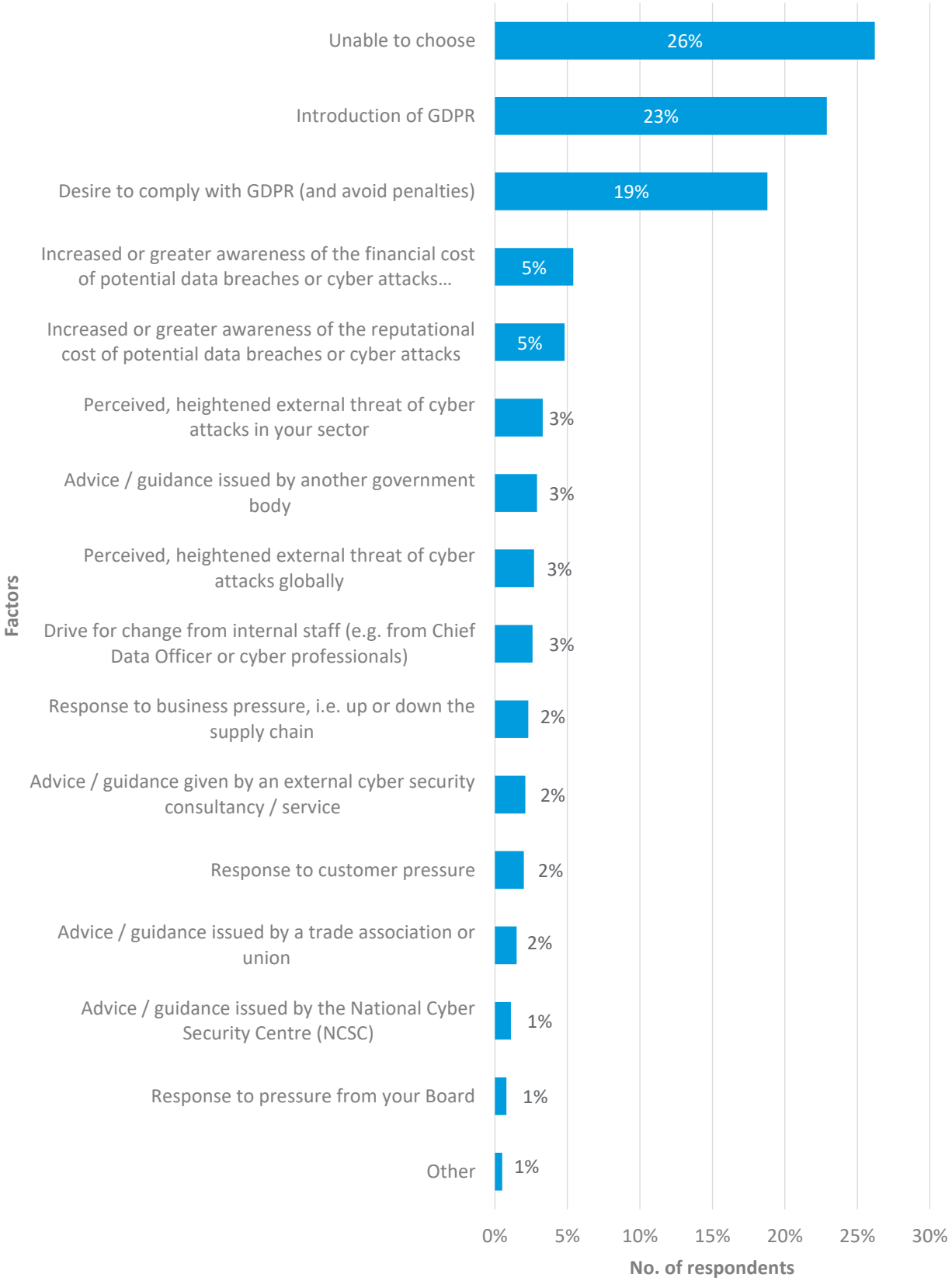
Respondents that had done a DPIA were more likely to have said ‘introduction of the GDPR’ was the most important factor influencing changes to cyber security than the average respondent (26%, compared to 23% of respondents, respectively).

Respondents who were cyber security or IT professionals were less likely to have said that either ‘introduction of the GDPR’ (18%) or ‘desire to comply with the GDPR and avoid penalties’ (12%) were the most important factors influencing cyber security changes than those who were not cyber security or IT professionals (27% and 21% respectively), possibly because they were more likely to have cited a range of other external factors as drivers.

Respondents who had not experienced a cyber security incident (21%) were more likely than those who had (10%) to have cited ‘desire to comply with the GDPR and avoid penalties’ as the most important factor. They were also more likely to have said that they could not choose one factor as the most important (28%, compared to 17%).

When considered by industry, respondents in public administration and defence (36%) and the health industry (32%) were more likely than other respondents (23%) to have cited ‘introduction of the GDPR’ as the most important factor. Respondents in the information and communication industry (9%) were less likely than the average respondent (19%) to have stated that ‘desire to comply with the GDPR and avoid penalties’ was the most important factor.

Figure 4.2: Factors ranked as most important in influencing these changes



Source: Staff and Board survey: Q34/BQ29. Please rank the factors you identified in terms of their importance, where one is the most important factor
Weighted Base: 1,062
Unweighted Base: 1,107

4.3 Influence of the GDPR

When asked to what extent all of the changes in their organisation's cyber security had been as a result of the introduction of the GDPR as opposed to other factors:

- the majority of respondents answered to a small or some extent (56%)
- a further quarter said to a great or very great extent (26%)
- only 15% of respondents said that the changes made were not a result of the introduction of the GDPR

There was some variation in response by industry and type of respondent. Where these variations were statistically significant, they are summarised below.

Respondents that completed a DPIA, experienced a cyber security incident or processed personal data were more likely to have attributed all changes to the GDPR than those that had not completed a DPIA or processed personal data (90%, 90% and 87% answered at least 'to a small extent,' compared to 72% and 62% respectively). Respondents who were cyber security or IT professionals were also more likely to attribute all changes to the GDPR than non-cyber security or IT professionals (86% at least 'to a small extent,' compared to 80%).

Respondents in: finance and insurance; arts, entertainment, recreation and other services; wholesale and retail; education; health; and public administration and defence were more likely than the average respondent to have attributed all of the changes in their cyber security over the last 3 years to the GDPR (100%,[98] 94%, 90%, 89%, 89% and 89% answered at least 'to a small extent,' respectively, compared to 82% of all respondents to both surveys).

We also explored the extent to which the GDPR had influenced changes to individual aspects of cyber security.

The majority of respondents reported that the introduction of the GDPR had influenced the changes reported in their cyber security in the last 3 years, to at least a small extent (see Figure 4.3).

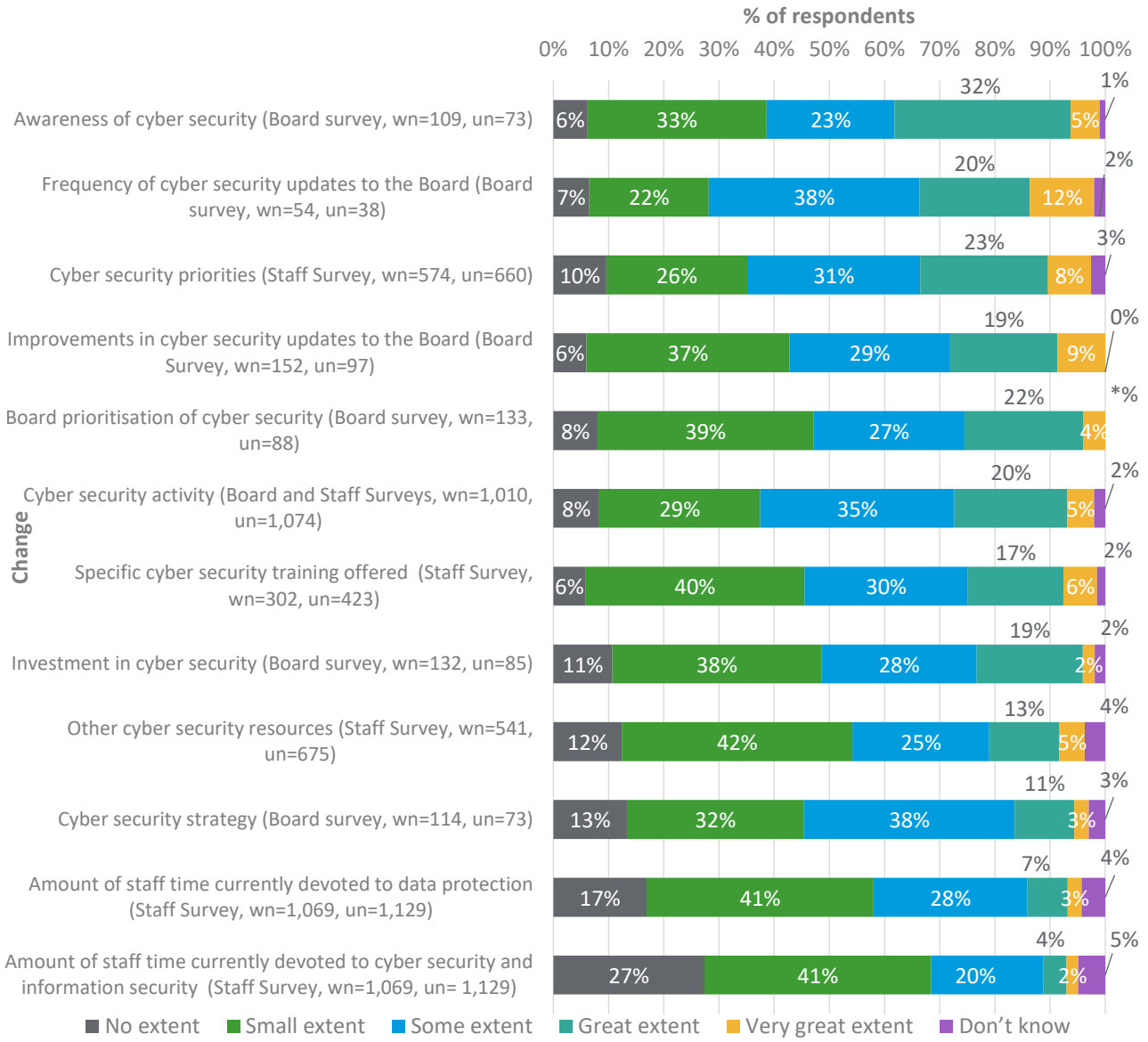
The changes most likely to have been influenced by the introduction of the GDPR to a great or very great extent were:

- Board's awareness of cyber security (37% of all respondents to the Board survey)
- frequency of cyber security updates to the Board (32% of respondents to the Board survey)
- cyber security policies (31% of respondents to the staff survey)

The amount of staff time currently devoted to data protection and cyber security and information security were the least likely to have been influenced to by the introduction of the GDPR, i.e. respondents were more likely to have responded 'no extent' (17% and 27% of respondents to the staff survey answered 'no extent' respectively). There was some variation in response by industry and type of respondent. Where these variations were statistically significant, they are summarised overleaf.

[98] *When rounded to the nearest whole number*

Figure 4.3: Extent to which the following changes have been influenced by the GDPR



Source: This chart is based on staff and Board surveys questions about the extent to which the changes made had been influenced by the introduction of the GDPR as opposed to other factors (Q21, BQ22, BQ14, BQ20, BQ24, Q27/BQ26, Q25, BQ9, Q23, BQ12, Q12 and Q15)

Note: wn= Weighted Base, un= Unweighted Base.
Only respondents who reported a change in the above aspects of cyber security were asked to what extent the introduction of the GDPR had influenced that change, hence lower bases

Cyber security priorities

Respondents that had completed a DPIA were more likely than the average respondent to have said that the GDPR influenced their cyber security priorities (91% answered at least to a 'small extent,' compared to 88%). Respondents who were IT or cyber security professionals were more likely to have attributed these changes to the GDPR than non-IT or cyber security professionals (92% answered at least to a 'small extent', compared to 86%).

Organisations in the finance and insurance industry (100%) and information and communication industry (96%) were more likely than the average respondent (88%) to have said that the GDPR influenced this change at least to a small extent.

Cyber security activity

Respondents that experienced a cyber security incident or processed personal data were more likely to attribute changes in their cyber security activity to the GDPR (93% and 92% respectively answered at least to a 'small extent,') than those that had not experienced an incident (89%), did not process personal data (81%) or had not completed a DPIA (86%). There was no statistically significant variation in the response to this question by industry.

Other cyber security resources

Respondents that experienced a cyber security incident or processed personal data were also more likely to attribute changes in other cyber security resources, such as software, hardware, outsourcing/consultancy or recruitment, to the GDPR at least to a small extent (97% and 87% respectively) than those that had not experienced an incident (81%) or did not process personal data (62%). Respondents who were IT or cyber security professionals were more likely to have attributed these changes to the GDPR than non-IT or cyber security professionals (93% answered at least to a 'small extent', compared to 79%).

Respondents in the finance and insurance industry and information and communication industry were more likely to attribute changes in other cyber security resources to the GDPR than the average respondent (100% and 96% answered at least to a 'small extent' respectively, compared to 84% of all respondents to the staff survey).

Staff time devoted to data protection

Respondents from organisations that had experienced a cyber security incident, completed a DPIA or processed personal data were more likely to attribute changes in staff time devoted to data protection to the introduction of the GDPR than those that had not experienced an incident, completed a DPIA or processed personal data.

Box 24: Proportion of respondents that attributed changes in staff time devoted to data protection to the introduction of the GDPR by organisational characteristic

- 90% of respondents that had experienced a cyber security incident answered, at least to a small extent, compared to 77% of those that had not experienced an incident
- 88% of those that had completed a DPIA, compared to 69% of those that had not done a DPIA
- 84% of those that processed personal data, compared to 58% of those that did not process personal data

Respondents who were IT or cyber security professionals were also more likely to have attributed these changes to the GDPR than non-IT or cyber security professionals (86% answered at least to a 'small extent', compared to 76%).

Compared to the average respondent (79%), the introduction of the GDPR had more of an influence on the amount of staff time devoted to data protection for those in the: property; arts, entertainment, recreation and other services; education; and information and communication industries than to the average respondent (93%, 90%, 88% and 86% responded at least to a 'small extent').

Staff time devoted to cyber and information security

Respondents that had experienced a cyber security incident, completed a DPIA or processed personal data were also more likely to attribute changes in staff time devoted to cyber and information security to the GDPR than those that had not experienced an incident, done a DPIA or processed personal data.

Box 25: Proportion of respondents that attributed changes in staff time devoted to cyber and information security to the introduction of the GDPR by organisational characteristic

- 84% of respondents that had experienced a cyber security incident answered, at least to a 'small extent,' compared to 65% of those that had not experienced an incident
- 76% of those that had completed a DPIA, compared to 61% of those that had not done a DPIA
- 72% of those that processed personal data, compared to 48% of those that did not process personal data

Respondents who were IT or cyber security professionals were also more likely to have attributed these changes to the GDPR than non-IT or cyber security professionals (84% answered at least to a 'small extent', compared to 62%).

Respondents in the finance and insurance, information and communication, production and education industries were more likely than average to attribute changes in staff time devoted to cyber and information security to the GDPR (88%, 87%, 81% and 81% answered, at least to a 'small extent,' compared to 68% of all respondents to the staff survey).

4.4 Organisational attitude to the GDPR

Most interviewees described their organisation's attitude to the GDPR as positive. Board members were more likely to express positive attitudes towards the GDPR than staff members. A positive attitude was most common in organisations in the health industry and the information and communication industry. The main reasons for describing their attitude to the GDPR as positive were that it provided an incentive to look into their cyber security management, and they were aware of the importance of protecting the personal information of their customers/clients. Examples of responses given by interviewees with a positive attitude to the GDPR include:

> *"Our attitude was positive. The overwhelming viewpoint of our organisation is that in the end they should be taking greater care of people's private information." (Interviewee from a non-profit in the construction industry)*

> *"Our attitude to the GDPR was definitely positive. The GDPR essentially forced us to look over our security which was a good thing for our organisation. Our policies changed accordingly and we know that these improvements wouldn't have happened if it hadn't been for the GDPR being enforced." (Interviewee from an MSP in the professional, scientific and technical industry)*

A minority of interviewees described their attitude to the GDPR as neutral. These were mainly SMEs. Some of the reasons for a neutral attitude towards the GDPR were:

> *"Our attitude towards the GDPR is neutral. We can see some benefits to the GDPR, but ultimately, I think the GDPR is an unnecessary burden and has caused us additional work. Overall, we can't see any positives but can't see any negatives of the GDPR either." (Interviewee from an SME in the construction industry)*

> *"There is definitely a neutral attitude to the GDPR, you can't choose whether you will or won't comply, you have just got to accept it. The GDPR is part of health and safety and something we need to consider in this day and age when we are dealing with someone's personal data." (Interviewee from a LA/non-profit providing important public services in the education industry)*

Organisations with no experience of a cyber incident were more likely to report a neutral attitude towards the GDPR. The main reason reported by these organisations was that they felt they already

sufficiently protected personal data and the GDPR was not likely to have a significant impact on their organisation.

A minority of interviewees described their attitude to the GDPR as negative. Interestingly, all of these interviewees were from smaller organisations. Reasons provided by these interviewees included the view that the GDPR was not appropriate for their organisation and created an additional administrative burden, which highlighted the benefits of providing more tailored guidance:

> *"Generally, the GDPR was perceived as bureaucratic and a 'one size fits all' kind of legislation that isn't appropriate for our kind of organisation. It was incredibly difficult for us to see how we were supposed to be compliant with this legislation." (Interviewee from a non-profit in the professional, scientific and technical industry)*

> *"Attitude can be described as negative. The GDPR involved a lot of administrative work and some of the requirements were not clear in terms of what the purpose of it was. The GDPR has had quite an onerous impact for small organisations like ours." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

The majority of interviewees commented on the overall attitude of their organisation, however, one interviewee provided insight on how attitudes towards the GDPR can vary within an organisation. Specifically, it was suggested that senior members of staff were more likely to report a positive attitude towards the GDPR, while frontline workers were more likely to have a neutral to negative attitude towards the GDPR. They commented that:

> *"The attitude towards the GDPR has varied between different people in the organisation. For people who are 'frontline workers' the attitude has been neutral to negative because it's extra bits for them to deal with when they have already got quite a challenging job to do. For the managers, they have certainly embraced it and seen the GDPR as necessary. Since GDPR was introduced they have treated cyber security as being a higher priority. Overall the attitude from managers has been positive." (Interviewee from an SME in the finance and insurance industry)*

4.5 Organisational approach to the GDPR

Responses in relation to their organisation's approach to the GDPR were mixed. Some interviewees said that their organisation took a proactive approach to the GDPR preparations, while others said that their approach to the GDPR was more reactive. A proactive approach was more common among larger organisations and those in the information and communication industry. Interviewees felt this was because they had a better understanding of what the GDPR meant for them and had sufficient resources to become compliant with the GDPR quickly. Examples of proactive approaches towards the GDPR provided include:

> *"We have been the equivalent of GDPR compliant since late 2016, therefore way ahead of when the GDPR was enforced." (Interviewee from an MSP in the information and communication industry)*

> *"Our approach was proactive. We already had several GDPR compliant practices in place and would have continued to make improvements even if the GDPR was not enforced." (Interviewee from an LA/non-profit providing important public services in the education industry)*

> *"We responded to the information released by the ICO, and we also follow the European Protection Board and the information that is released by them. Therefore, a lot of our changes to cyber security were implemented ahead of the GDPR being enforced in UK which is definitely*

considered to be a proactive approach." (Interviewee from an MSP in the information and communication industry)

Reactive approaches towards the GDPR were driven by organisational capacity and capability. Where interviewees described their approach as reactive, they said that this was due to having fewer resources available to make changes to their processes and policies. They also reported not having the capability to adopt robust cyber security policies. As a result, changes were only made to their cyber security when it became a legal requirement to do so. One interviewee noted:

"Our approach was reactive as the changes weren't implemented in the organisation until the GDPR was enforced. However, we feel that this wasn't our fault. Before the GDPR it was not clear how much data protection and security measures would affect our business. We were left to react to the GDPR when it came out as opposed to proactively doing anything about it and trying to get ahead. If we'd had more information beforehand then we would have had a far more proactive approach". (Interviewee from a non-profit in the information and communication industry)

The majority of interviewees got information on the GDPR from multiple sources:

"We looked at information on government websites and outsourced an external company to help with the contract law, HR policy. They gave us advice on things that we needed to do so that they would be compliant." (Interviewee from an SME in the transport and storage industry)

Some of the interviewees reported that they got information about the GDPR from the ICO website. Interviewees' opinions on this were mixed. Some interviewees felt that the information provided was helpful, but some others felt that the guidance was vague and they were unsure how their organisation should respond as a result. Thus, reiterating the benefits of providing more tailored guidance.

Some interviewees stated that they had attended training courses. Most of the training courses mentioned were free, and a minority of interviewees reported that they had sent their Data Protection Officer, or equivalent, on a high-level training course.

A minority of interviewees, mostly from SMEs, reported that they got information about the GDPR from outsourced IT/cyber security consultants who were able to give practical advice on what they needed to do to become compliant with the GDPR:

"We had a privately sourced professional come in to input and assist us in putting plans for improving our cyber security in place." (Interviewee from an SME in the health industry)

A minority of interviewees got information from professional groups and umbrella organisations. One interviewee from a local parish council said:

"As a parish council we are members of various local government associations. There was a lot of guidance and information available from organisations such as the National Association of Local Councils. Some of these organisations did try to explain the legislation in terms of 'this is what you need to be doing', 'and this is what you should not be doing'. This helped to make the information more digestible and easy to understand." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)

Thus, highlighting the value of tailoring advice and guidance to the audience to maximise impact of any future incentives and regulations.

4.6 Enablers for change

The main enablers for change reported by the interviewees were:

- support from senior management or the Board to be compliant with the GDPR and improve cyber security:

  "A big enabler for us was the fact that the Board were on board with this and shared our desire to become compliant with the GDPR. They ensured that we had the resources that we needed for this to happen." (Interviewee from an LA/non-profit providing important public services in the education industry)

- improvement in awareness of cyber security:

  "We're more aware of the risks, and that's helped us to decide which cyber security policies and processes need tightened." (Interviewee from a non-profit in the accommodation and food services industry)

- information about the GDPR found on government websites and ICO website which helped organisations understand how the GDPR would affect them and what they needed to do to be compliant:

  "The information on the government websites was really clear, and we knew what we needed to do and how the GDPR was going to affect us." (Interviewee from an LA/non-profit providing important public services in the education industry)

- principles and ethos of the organisation that meant they were aware of the importance of protecting personal data:

  "What helped us is that our ethos as an organisation is good, and we have always been aware of the importance of protecting the personal data of our clients. This meant that our staff were open to making changes to the way they work so that we could be compliant with the GDPR." (Interviewee from an SME in the finance and insurance industry)

However, some organisations felt the need to bring in outsourced cyber security consultants for information on what data protection policies and processes were required to be compliant with the GDPR:

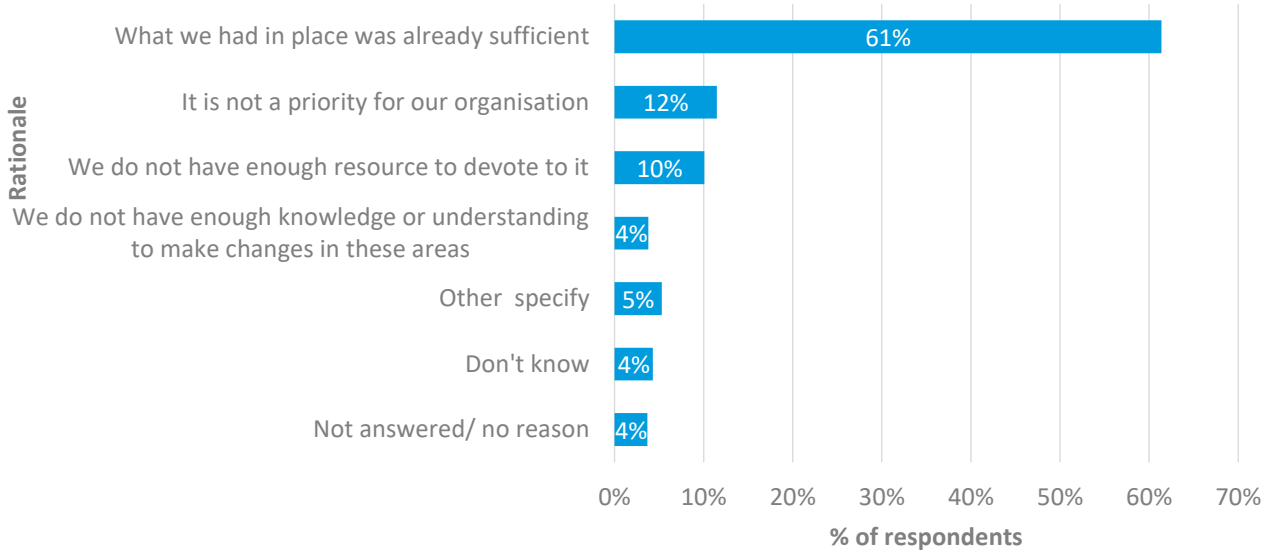
> *"We're a small organisation and didn't have the expertise to know what we needed to do to be GDPR compliant. So we had to bring in external cyber security consultants to help us. They were great and looked at everything we did and made recommendations. If it hadn't been for them then I doubt we would be GDPR compliant." (Interviewee from an SME in the property industry)*

As noted in Section 3, some interviewees had found it challenging to sustain the changes due to the costs associated with maintaining compliance and staff awareness that the GDPR is an ongoing issue.

4.7 Rationale for not making changes

Where respondents had not made changes to a particular aspect of their cyber security practices in the last 3 years they were asked why not (79% of all respondents to both surveys). The main reason given for not changing a particular aspect was that they felt existing measures were sufficient (61%) (see Figure 4.4). However, a minority of respondents said it was not a priority for their organisation (12%) or they did not have enough resources to devote to it (10%).

Figure 4.4: Rationale for not changing cyber security in the last 3 years



Source: Staff/Board survey Q28/BQ27. Considering those elements of cyber security that have not been introduced or improved in the last 3 years, what is the main reason you have not taken action in these areas? - by elements introduced/improved
Weighted Base: 1,015
Unweighted Base: 976
Note: Only respondents that said one or more aspect of cyber security 'stayed the same' were asked this question
Respondents who answered, 'Other' were asked to specify. Examples of their responses included costs, time, lack of resources, low risk/no real threat, cyber security is outsourced, tightened security, more training for staff.

What was in place was already sufficient

- organisations that did not process personal data (69%), had not experienced a cyber security incident (66%) or had not completed a DPIA (55%) were more likely to give this reason than those that had experienced an incident (37%)
- IT or cyber security specialists were less likely give this response (50%) than non-specialists (65%)
- those in production and the finance and insurance industry were less likely than average to have given this response (47% and 40% respectively, compared to 61% of all respondents)

A minority of those who took part in the qualitative interviews had not made changes to their cyber security. In all 4 cases, the interviewees stated that changes were not required because they believed what they already had in place was sufficient.

> *"When we heard that the GDPR was going to be enforced, we hired a temporary advisor to look into what we needed to do to be compliant. The advisor found that what was in place was already sufficient and there were no changes required." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)*

"We didn't need to make changes because we were already compliant with the GDPR. Also, we have never had issues with cyber attacks because we have robust policies and processes in place. As an organisation we have the view of 'if something isn't broken, then it doesn't need fixed'. If changes were required to be compliant then we absolutely would have made those." (Interviewee from an SME in the finance and insurance industry)

These interviewees all reported that they were confident in their organisation's ability to manage cyber security risks and detect security threats because they had robust policies and procedures in place, and they also had staff with good expertise in cyber security:

"We employ professionals and outsource companies who look at our cyber risk management for us. We also have robust process and policies in place so we're very confident that we can manage all cyber security risks." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)

These interviewees also reported that they were confident in their organisation's ability to protect themselves against a cyber attack:

"We are very confident that we can protect ourselves from cyber attacks. We know that we perform well in this area compared to other companies in our sector because we have never had a cyber breach, and this is because we have good procedures and policies in place." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)

Half of these interviewees stated that they were confident in their organisation's ability to respond to and recover from a cyber attack:

"We have robust recovery plans in place just in case we are the victim of a cyber attack. With these in place, we are confident that we can quickly recover from any such incident." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)

It is possible, however, that some of this confidence may be misplaced. Some organisations may benefit from assistance in assessing their risk posture and the appropriateness of the measures they have taken.

Those that said they were not confident, explained it was because they had never experienced a cyber attack and so could not definitively say that they could respond to one quickly:

"It's hard to say as we have never been the victims of a cyber attack, but we employ professionals who have the skillset to respond to a cyber attack should one happen. We are reasonably confident, but we can't say for certain." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)

It is not a priority for our organisation

- Board members were more likely than staff to have given this response (22%, compared to 10%)
- those that had not completed a DPIA were more likely to have given this response than those that had done a DPIA (16%, compared to 5%) – indicating that the DPIA is a useful tool for encouraging change
- respondents who were IT or cyber security professionals were less likely to have given this answer (4%, compared to 12% of all respondents)
- there was no statistically significant variation in this response by industry

We did not have enough resources to devote to it

- organisations that had completed a DPIA were also more likely to have given this response (13%)
- organisations that had not experienced a cyber security incident were less likely to have given this answer (9%)
- IT or cyber security specialists were more likely to give this answer (16%)
- organisations in the education industry and arts, entertainment recreation and other services industry were more likely than average to have given this response (17% and 10% respectively)

5 SPECIAL INTEREST GROUPS

5.1 Context

Data was also broken down into groups of specific interest for DCMS, chosen to understand in greater detail how the impact of the GDPR has varied across different context. DCMS had a particular policy interest in the following groups:

- large businesses – any private sector organisation with 250 employees or more
- large businesses with complex and interconnected supply chains - private sector organisations in any industry with: 250 employees or more; a supply chain with more than 3 tiers of suppliers; and for whom the incapacitation of a main supplier by a cyber-attack for 48 hours would have a moderate or severe impact on their day to day business operations or service provision
- MSPs – an outsourced third-party company that manages and assumes the responsibility of a defined set of day-to-day management services to its customers
- LAs/non-profits providing important public services – Local authorities and non-profit organisations providing important public services that are not within the scope of the NIS Regulations
- SMEs – any private sector organisation with fewer than 250 employees
- Board members

The survey methodology was designed to boost the sample from these groups to enable analysis of their responses. This section presents any statistically significant differences in the survey responses of these groups when compared to total respondents. It also summarises the findings on improvements in Board level prioritisation of cyber security discussed in Sections 3 and 4.

Note: While total responses and responses for SMEs can be generalised, survey findings for large businesses, large businesses with complex and interconnected supply chains, MSPs and LAs/non-profits providing important public services are indicative and should not be generalised to represent the wider population.

5.2 Large businesses

Large businesses summary

Large businesses were more likely than the average respondent to have made changes to their cyber security in the last 3 years across a number of indicators. In particular, they were more likely than the average respondent to have increased spending on all aspects of cyber security. They were also more likely to attribute this to the GDPR. Interviewees suggested that this was because large businesses have more resources and greater capabilities than smaller organisations.

Large businesses were also more likely to have changed:

- procurement or supply chain risk management (58% reported changes, compared to 33% of all respondents to both the staff and Board surveys)
- technical controls (65% reported changes, compared to 45% of all respondents to both surveys)

They were also more likely to have:

- provided GDPR training (83%, compared to 67% of respondents to the staff survey)
- included elements of cyber security within that GDPR training (95%, compared to 86%)
- provided standalone cyber security training (69%, compared to 34%)
- introduced or improved this cyber security training in the last 3 years (91%, compared to 83%)

This indicates that the GDPR has had an impact on large businesses, particularly in relation to changes in staff awareness and training.

5.2.1 Manage security risk

5.2.1.1 Governance

Large businesses, defined as any private sector organisation with 250 employees or more, were more likely to have changed their information security policies than the average respondent (73% of large businesses answered 'introduced' and/or 'improved', compared to 61% of all respondents to both surveys). These were typically improvements to existing policies (65%). Most interviewees from large businesses reported that they either made minor changes to their data protection policies or made no changes as they believed their data protection policies were already compliant with the GDPR.

Large businesses were more likely than the average respondent to the staff survey to have at least one employee who **specialised in data protection** (72% and 58% respectively). They were also more likely than the average respondent to the staff survey to have at least one employee who **specialised in cyber or information security** (66% and 36% respectively).

5.2.1.2 Risk management

Large businesses were more likely than the average respondent to have changed their risk management processes (68%, compared to 53% of all respondents to both surveys). They were also more likely than the average respondent to have done a DPIA (65%, compared to 51% of respondents to the staff survey) and to have made changes as a result of the DPIA (69%, compared to 56% of respondents to the staff survey).

5.2.1.3 Asset management

Large businesses were more likely to have changed their asset management than the average respondent (54% reported changes, compared to 34% of all respondents to both surveys).

5.2.1.4 Data processors and the supply chain

Large businesses were more likely to have changed their procurement or supply chain risk management in the last 3 years than the average respondent (58%, compared to 33% of all respondents to both surveys).

5.2.2 Protect personal data against cyber attack

5.2.2.1 Service protection policies and processes

Large businesses were more likely to have changed how they ensured that web services were protected from common security vulnerabilities than the average respondent (71% answered 'introduced' and/or 'improved', compared to 59% of all respondents to both surveys). They were also more likely than the average respondent to have changed their Cyber Essentials/Cyber Essentials Plus (56%) or ISO certification (44%) in the last 3 years (compared to 38% and 26% of all respondents to both surveys respectively). This included becoming certified for the first time, getting recertified and upgrading their certification.

5.2.2.2 Data security

Large businesses were more likely to have changed their **technical controls** than the average respondent (65% answered 'introduced' and/or 'improved', compared to 45% of all respondents to both surveys).

5.2.2.3 Identity and access control

Large businesses were more likely than the average respondent to have changed their identity and access controls (60% reported changes, compared to 46% of all respondents to both surveys).

5.2.2.4 System security

Respondents to the staff survey that were IT or cyber security professionals were asked additional questions about more technical changes to their cyber security. Large businesses were more likely than the average respondent to have changed how they ensured the processing environment remains secure, actively managed software vulnerabilities, including patching and managed end user devices in the last 3 years (66%, 73% and 65% of technical respondents from large businesses reported changes respectively, compared to 55%, 55% and 52% of all technical respondents respectively).

5.2.2.5 Staff awareness and training

Provision of the GDPR training was more common among large businesses (83%) than for the average respondent to the staff survey (67%). Large businesses were more likely to include elements of cyber security in their GDPR training (95%) than the average respondent to the staff survey (86%). The provision of specific cyber security training also was much more common among large businesses (69%, compared to 34% of respondents to the staff survey). Large businesses were also more likely to have introduced or improved this cyber security training in the last 3 years (91%, compared to 83% of all respondents to the staff survey).

5.2.3 Detect security threats

5.2.3.1 Security monitoring

Large businesses were more likely to have changed their monitoring and review processes than the average respondent (60% answered 'introduced' and/or 'improved', compared to 50% of all respondents to both surveys).

5.2.4 Minimise the impact

5.2.4.1 Response and recovery

Large businesses were more likely to have changed their incident management or recovery processes than the average respondent (62% answered 'introduced' and/or 'improved', compared to 45% of all respondents to both surveys).

5.2.5 Cyber security expenditure

Large businesses were more likely to have **increased their spending** on all aspects of cyber security:

- 66% of large businesses increased spend on security software, compared to 39% of respondents to the staff survey
- 52% increased spend on hardware, compared to 29%
- 35% increased spend on outsourcing and/or consultancy, compared to 22%
- 41% increased spend on recruitment, compared to 15%

5.2.6 Breadth and duration of impact

Large businesses were more likely than the average respondent to have agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas in their organisation (84%, compared to 74% of all respondents to both surveys).

5.2.7 Unintended consequences

Large businesses were more likely than the average respondent to have disagreed or strongly disagreed that the GDPR had led to excessive focus on data protection to the detriment of other aspects of cyber security (42%, compared to 54% of all respondents to both surveys).

Large businesses (35%) were more likely to have agreed or strongly agreed that the GDPR had led to excessive investment in cyber security, significantly beyond what is necessary than the average respondent to both surveys (27%).

5.2.8 Factors driving change

Large businesses were more likely to attribute all of the changes in their cyber security to the GDPR than the average respondent (89% answered at least to a 'small extent,' compared to 82% of all respondents to both surveys). They were also more likely to attribute the following specific changes to the introduction of the GDPR than the average respondent:

- cyber security resources (97% answered at least to a 'small extent,' compared to 84% of all respondents to the staff survey)
- amount of staff time devoted to data protection (93%, compared to 79% of respondents to the staff survey)
- amount of staff time devoted to cyber and information security (90%, compared to 68% of respondents to the staff survey)

Where no changes had been made, large businesses were less likely to have said that changing their cyber security was 'not a priority for our organisation' than the average respondent (6%, compared to 12% of all respondents to both surveys), but were more likely to have said that they 'did not have enough resource to devote to it' (19%, compared to 10% of all respondents to both surveys).

5.3 Large businesses with complex and interconnected supply chains

Large businesses with complex and interconnected supply chains summary

Large businesses with complex and interconnected supply chains were more likely than the average respondent to have made changes against a number of the NCSC cyber security outcomes in the last 3 years and to have attributed all of the changes in their cyber security in the last 3 years to the GDPR, at least to a small extent (97%, compared to 82% of all respondents to both surveys). Interviewees also reported changes in how their organisation conducted supplier risk management.

Large businesses with complex and interconnected supply chains were also more likely than the average respondent to have:

- at least one data protection role (74%, compared to 58% of respondents to the staff survey)
- at least one cyber security role (78%, compared to 36% of respondents to the staff survey)
- created one or more of these roles in the last 3 years (93% had created at least one data protection role and 91% had created at least one cyber security role, compared to 77% and 81% of respondents to the staff survey respectively)

This indicates that the GDPR has encouraged large businesses with complex and interconnected supply chains to improve their cyber security, particularly their internal capacity and capability. This could be because they are likely to be more dependent on third parties than the average respondent and, therefore, need to take greater action to mitigate these risks.

However, while this group was more likely than the average respondent to have made changes in the above areas, there was still a substantial percentage of large businesses with complex and interconnected supply chains that had not made changes. This was often because they felt that 'what was in place was already sufficient', however, lack of sufficient resource was also a factor.

Care should be taken when interpreting these findings as the base for this group was less than 100 respondents.

For the purposes of this research, large businesses with complex and interconnected supply chains were defined as:

- private sector organisations
- operating in any industry
- employing 250 employees or more
- having a supply chain with more than 3 tiers of suppliers
- an organisation for whom the incapacitation of a main supplier by a cyber-attack for 48 hours would have a moderate or severe impact on their day to day business operations or service provision

5.3.1 Manage security risk

5.3.1.1 Governance

Large businesses with complex and interconnected supply chains were more likely to have introduced new and/or improved information security policies in the last 3 years than the average respondent (72%, compared to 61% of all respondents to both surveys).

Large businesses with complex and interconnected supply chains were more likely than the average respondent to have at least one employee who specialised in data protection or cyber/information security (74% of large businesses with complex and interconnected supply chains had at least one data protection role and 78% had at least one cyber or information security role, compared to 58% and 36% of respondents to the staff survey respectively). They were also more likely to have created one or more of these roles in the last 3 years than the average respondent (93% had created at least one data protection role and 91% had created at least one cyber security role, compared to 77% and 81% of respondents to the staff survey respectively).

5.3.1.2 Risk management

Large businesses with complex and interconnected supply chains were more likely, than the average respondent, to have changed their risk management processes (69%, compared to 53% of all respondents to both surveys).

Large businesses with complex and interconnected supply chains were more likely to have done a DPIA (70%) than the average respondent to the staff survey (51%) and to have made changes as a result (78%, compared to 56% of respondents to the staff survey).

5.3.1.3 Asset management

Large businesses with complex and interconnected supply chains were more likely to have changed their asset management than the average respondent (66%, compared to 34% of all respondents to both surveys).

5.3.1.4 Data processors and the supply chain

Large businesses with complex and interconnected supply chains were more likely than the average respondent to have changed their procurement or supply chain risk management (72%, compared to 33% of all respondents to both surveys).

Some of the interviewees from large businesses with complex and interconnected supply chains reported that the GPDR had impacted how their organisation conducted supplier risk management:

> *"There has been a big change in contract management and processes around it and changing clauses in the contract. We also now have annual GDPR audits too now and will do a yearly supply visit to check to see if our suppliers are GDPR compliant." (Interviewee from a large business with a complex and interconnected supply chain in the finance and insurance industry)*

> *"We keep up to date on our suppliers' compliance with the GDPR – every year they have to fill out a questionnaire to confirm compliance." (Interviewee from a large business with a complex and interconnected supply chain in the construction industry)*

One interviewee reported that although they had made changes to their supplier risk management, these were minimal:

> *"We have started to ask new and existing contractors for evidence of GDPR compliance, but we don't actively test/check this. This has been more of a tick-box exercise just to ensure that they are being compliant." (Interviewee from a large business with a complex and interconnected supply chain in the accommodation and food services industry)*

Most of the interviewees who had made changes said that these changes had a positive impact on their organisation:

"It made sure that we have all the right information from supplier and customers that we need. We ask more questions now so we have more information about them which helps us on an ongoing basis." (Interviewee from a non-profit in the construction industry)

"These changes give us greater oversight and allows us to show clients we are careful around the whole supply chain." (Interviewee from a large business with a complex and interconnected supply chain in the finance and insurance industry)

Some of these interviewees reported that these changes had little impact or a negative impact on their organisation:

"I don't feel that this has made any difference. It could be the case that the smaller organisations in their supply chain aren't actually compliant and are just providing information to satisfy them as an employer. They are keeping up appearances with respect to this, but there could easily be an incident that would expose the fragility of this." (Interviewee from a large business with a complex and interconnected supply chain in the accommodation and food services industry)

"These changes have had a negative impact on our organisation. I honestly don't think they were necessary." (Interviewee from an SME in the construction industry)

Interviewees from large businesses with complex and interconnected supply chains who reported that the GDPR did not have any impact on how the organisation conducted supplier risk management reported that this was because:

"We have a new supplier chain risk management team, but I don't think the effectiveness of dealing with this risk has changed in any way since GDPR was enforced." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)

"Supplier risk management hasn't changed for us because personal and sensitive data is not shared outside company." (Interviewee from a large business with a complex and interconnected supply chain in the transport and storage industry)

"We already had a legal framework in place because of the nature of the supplier we use. Just a small extra layer really and all the organisations we work with are global organisations and have similar experiences and so we work a lot with e.g. amazon web services etc. All doing the same work, so we didn't have to inform we expected them to do it. They were already in the work themselves." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)

Most interviewees from large businesses with complex and interconnected supply chains stated that they were confident that they could effectively manage all risks from their supply chains:

"We have a fairly small supply chain compared to other organisations of our size so it's not too difficult to effectively manage the risks from our supply chain." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)

"We have always been able to manage risks from our supply chain because we have robust processes in place." (Interviewee from a large business with a complex and interconnected supply chain in the transport and storage industry)

A minority of interviewees from large businesses with complex and interconnected supply chains stated that they were not confident in their ability to manage all supply chains risks:

> *"The biggest obstacle is resistance from our suppliers to provide information that we ask for. They are also resistant to providing proof that they are doing things in the right way, specifically in a way that is compliant with the GDPR." (Interviewee from a non-profit in the construction industry)*

5.3.2 Protect personal data against cyber attack

5.3.2.1 Staff awareness and training

Provision of the GDPR training was more common than average among large businesses with a complex and interconnected supply chain (90%, compared to 67% of respondents to the staff survey).

5.3.2.2 Service protection policies and processes

Large businesses with complex and interconnected supply chains were more likely than the average respondent to have changed their Cyber Essentials or Cyber Essentials Plus certification (68% reported changes, compared to 38% of all respondents to both surveys) and ISO certification in the last 3 years (58% reported changes, compared to 26% of all respondents to both surveys). This included becoming certified for the first time, getting recertified and upgrading their certification.

5.3.2.3 Identity and access controls

Large businesses with complex and interconnected supply chains were more likely to have changed their identify and access controls than the average respondent (64%, compared to 46% of all respondents to both surveys).

5.3.2.4 Data security

Compared to the average respondent, large businesses with complex and interconnected supply chains were more likely to have changed their technical controls (45%, compared to 65% of all respondents to both surveys).

5.3.2.5 System security

Respondents to the staff survey that were IT or cyber security professionals were asked additional questions about more technical changes to their cyber security. Technical respondents from large businesses with complex and interconnected supply chains were more likely than the average technical respondent to have changed how they:

- undertake regular testing to evaluate the effectiveness of your security measures, such as penetration testing, virus and malware scanning (72%, compared to 60%)
- actively managed software vulnerabilities, including patching (75%, compared to 55%)
- managed end user devices (69%, compared to 52%)

5.3.3 Detect security threat

5.3.3.1 Security monitoring

Large businesses with complex and interconnected supply chains were more likely than the average respondent to have changed their monitoring and review, including audit processes (70%, compared to 50% of all respondents to both surveys).

5.3.4 Minimise the impact

5.3.4.1 Response and recovery

Large businesses with complex and interconnected supply chains were more likely to have changed their incident management or recovery processes than the average respondent (69% answered 'introduced' or 'improved', compared to 45% of all respondents to both surveys).

5.3.5 Cyber security expenditure

Large businesses, especially those with complex and interconnected supply chains were more likely to have increased their spending on all aspects of cyber security:

- 70% of large businesses with complex and interconnected supply chains increased their spend on security software, compared to 39% of respondents to the staff survey
- 60% increased their spend on hardware, compared to 29%
- 41% increased their spend on outsourcing and/or consultancy, compared to 22%
- 50% increased their spend on recruitment, compared to 15%

5.3.6 Breadth and duration of impact

Large businesses with complex and interconnected supply chains were more likely to have agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas in their organisations (86%) than the average respondent to the staff survey (74%).

5.3.7 Unintended consequences

Large businesses with complex and interconnected supply chains (46%) were more likely to have agreed or strongly agreed that the GDPR had led to excessive investment in cyber security, significantly beyond what is necessary than the average respondent (27% of all respondents to both surveys). However, they were more likely than the average respondent to have disagreed or strongly disagreed that the GDPR had led to excessive:

- focus on data protection to the detriment of other aspects of cyber security (34%, compared to 54% of all respondents to both surveys)
- caution amongst staff in the handling of data (33%, compared to 43%)

5.3.8 Factors driving change

Large businesses with complex and interconnected supply chains were more likely to attribute all of the changes in their cyber security in the last 3 years to the introduction of the GDPR, at least to a small extent, than the average respondent (97%, compared to 82% of all respondents to both surveys). They were also more likely than the average respondent to report that the introduction of the GDPR had influenced the following specific changes:

- the amount of staff time devoted to data protection (98% answered at least to a small extent, compared to 79% of respondents to the staff survey)
- the amount of staff time devoted to information security (96%, compared to 68%)
- changes in the specific cyber security training offered (100%, compared to 93%)
- changes in other cyber security resources, such as hardware, software, outsourcing/consultancy and recruitment (100%, compared to 84%)

Where no changes were made, large businesses with complex and interconnected supply chains were less likely to have said 'what was in place was already sufficient' than the average respondent (44%, compared to 61% of all respondents to both surveys). However, they were more likely to have said that they 'did not have enough resource to devote to it' than the average respondent to both surveys (27%, compared to 10% of all respondents to both surveys).

5.4 MSPs

MSP summary

MSPs were less likely than other respondents to have made changes against a number of the NCSC cyber security outcomes in the last 3 years. They were also less likely to rank 'desire to comply with the GDPR' as the most important factor than the average respondent (4%, compared to 19% of all respondents to both surveys). Other external factors were more important drivers for MSPs such as:

- 'response to business pressure' (41% of MSPs, compared to 21% of all respondents to both surveys)
- 'response to customer pressure' (37%, compared to19%)
- 'perceived, heightened external threat of cyber attacks in their sector' (36%, compared to 27%)

This indicates that the introduction of the GDPR had less of a direct impact on MSPs. It is possible, however, that these business and customer pressures were partly driven by the introduction of the GDPR. Most interviewees from MSPs also reported that the GDPR had positively impacted their relationships with the organisations they provided services to.

For the purposes of this research MSPs were defined as an outsourced third-party company that manages and assumes the responsibility of a defined set of day-to-day management services to its customers.

5.4.1 Manage security risk[99]

5.4.1.1 Governance

Where interviewees said that the priority of cyber security in their organisation had not changed over the last 3 years, this was because the priority of cyber security was already high and, therefore, the introduction of the GDPR had not changed this. This response was more common for MSPs than the average respondent.

MSPs were more likely than the average respondent to have at least one employee who specialised in data protection or cyber/information security (75% of MSPs had at least one data protection role and 67% had at least one cyber/information security role, compared to 58% and 36% of respondents to the staff survey respectively).

[99] *There were no statistically significant differences in how MSPs answered questions relating to NCSC outcomes A3: Asset management compared to the average respondent*

5.4.1.2 Risk management

MSPs that had done a DPIA were more likely than average to have made changes to their cyber security as a result of it (72%, compared to 56% of respondents to the staff survey).

5.4.1.3 Data processors and the supply chain

MSPs were more likely than the average respondent to have introduced and/or improved their procurement or supply chain risk management in the last 3 years (45%, compared to 33% of all respondents to both surveys).

Most interviewees from MSPs reported that the GDPR had an impact on their relationship or processes with the organisations they provided services to:

> *"It's had a positive impact. As part of the processes in place, we now ensure that the organisations that we provide services to have a GDPR statement and are compliant with the regulations or working towards compliance. The GDPR is going to change over time. In summary we now have to ensure that the organisations that we provide services to have processes in place to look after data and look after his organisation's data, and to ensure that they have processes in place that enable them to look after data in the same way that we do." (Interviewee from an MSP in the professional, scientific and technical industry)*

> *"We are required to provide more documentation and policy wording, terms and conditions to new clients before we can engage with them. It's good for transparency and our clients know what is expected of them, but it is extra work for us." (Interviewee from a non-profit in the information and communication industry)*

5.4.2 Protect personal data against cyber attack[100]

5.4.2.1 Service protection policies and processes

Compared to the average respondent, MSPs were more likely to have changed their ISO certification in the last 3 years (38%, answered, 'introduced' and/or 'improved', compared to 26% of all respondents to both surveys). This included becoming certified for the first time, getting recertified and upgrading their certification.

5.4.2.2 Data security

MSPs were also more likely to have changed their technical controls than the average respondent (59%, compared to 45% of all respondents to both surveys).

5.4.2.3 System security

Respondents to the staff survey that were IT or cyber security professionals were asked additional questions about more technical changes to their cyber security. Technical respondents from MSPs were less likely than the average technical respondent to have changed how they actively managed software vulnerabilities, including patching (45% answered 'introduced' or 'improved', compared to 55% of all technical respondents).

[100] *There were no statistically significant differences in how MSPs answered questions relating to NCSC outcomes B2: Identity and access control, C: Detect security threats or D: Minimise impact compared to the average respondent*

5.4.2.4 Staff awareness and training

Provision of GDPR training was more common among MSPs (79%) than average (67% of respondent to the staff survey). Among organisations that provided GDPR training, MSPs were:

- less likely to have provided mandatory GDPR training only (69%, compared to 80% of respondents to the staff survey), but more likely to have provided a combination of mandatory and optional GDPR training (24%, compared to 10%)
- more likely to include elements of cyber security in their GDPR training (94%, compared to 86%)
- more likely to provide specific cyber security training (58%, compared to 34%)
- less likely to have introduced or improved this cyber security training in the last 3 years (83%, compared to 72%)

5.4.3 Minimise the impact

5.4.3.1 Response and recovery

MSPs were more likely to have changed their incident management or recovery processes than the average respondent (55% answered 'introduced' or 'improved', compared to 45% of all respondents to both surveys).

5.4.4 Cyber security expenditure

MSPs were also more likely to have increased their spend on recruitment in the last 3 years than the average respondent (31%, compared to 15% of respondents to the staff survey).

5.4.5 Breadth and duration of impact

MSPs were more likely to have agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas in their organisation than the average respondent to both surveys (88%, compared to 74%).

5.4.6 Unintended consequences

They were also more likely to have agreed or strongly agreed that the GDPR had led to excessive focus on data protection to the detriment of other aspects of cyber security (50%, compared to 36% of all respondents to both surveys). MSPs (39%) were more likely to have agreed or strongly agreed that the GDPR had led to excessive investment in cyber security, significantly beyond what is necessary than other respondents (27% of all respondents to both surveys).

5.4.7 Factors driving change

MSPs were more likely to have cited 'perceived, heightened external threat of cyber attacks in their sector', 'response to business pressure' and 'response to customer pressure' as influencing factors than other respondents (36%, 41% and 37% of MSPs respectively, compared 27%, 21% and 19% of all respondents to both surveys respectively).

MSPs were less likely to rank 'desire to comply with the GDPR' as the most important factor (4%, compared to 19% of all respondents to both surveys). It is possible, however, that the business and customer pressures that influenced the changes made were partly driven by the introduction of the GDPR.

MSPs were more likely than the average respondent to report that the introduction of the GDPR had influenced:

- changes in their cyber security priorities (97% answered at least to a 'small extent,' compared to 88% of respondents to the staff survey)
- the amount of staff time devoted to data protection (90%, compared to 79%)
- the amount of staff time devoted to cyber and information security (92%, compared to 68%)
- changes in their cyber security resources (100%, compared to 84%)

5.5 LAs/Non-profits providing important public services

LAs/non-profits providing important services summary

Local Authorities (LAs) and non-profits providing important services were more likely than the average respondent to:

- have made changes to most aspects of their cyber security activity
- rank 'introduction of the GDPR' as the most important factor for making changes to their cyber security (30%, compared to 23% of all respondents to both surveys)
- agreed or strongly agreed that the changes had been sustained (90%, compared to 84% of all respondents to both surveys)
- attribute all of these changes to the GDPR at least to a small extent (90%, compared to 82% of all respondents to both surveys)

Where changes were not made, LAs/non-profits providing important public services were less likely to have said it was not a priority for their organisations (7%) than the average respondent to both surveys (12%).

This indicates that the GDPR had a greater impact on LAs/non-profits providing important services when compared to the average respondent.

For the purposes of this research LAs/non-profits providing important public services were defined as LAs and non-profit organisations providing important public services, that are not within the scope of the NIS Regulations.

5.5.1 Manage security risk[101]

5.5.1.1 Governance

LAs/non-profits providing important public services (69%) were more likely than the average respondent to the staff survey (55%) to rate data protection policies, processes, procedures as a high priority now. LAs/non-profits providing important services were also more likely to have changed their data protection policies and information security policies in the last 3 years than the average respondent to both surveys (85% of LAs/non-profits providing important public services said that they had 'introduced' and/or 'improved' their data protection policies and 80% 'introduced' and/or

[101] *There were no statistically significant differences in how LAs/non-profits providing important public services answered questions relating to NCSC outcome A4: Data processors and the supply chain compared to the average respondent*

'improved' their information security policies, compared to 71% and 61% of all respondents to both surveys respectively).

According to the qualitative interviewees, these changes were typically improvements to existing policies. Interviewees from LAs/non-profits providing important services were more likely than interviewees from private sector organisations to have cited the principles and ethos of their organisation as an enabler for change. They said it meant they were more aware of the importance of protecting personal data.

LAs/non-profits providing important public services were more likely to have at least one employee who specialised in data protection than the average respondent (58%, compared to 58% of respondents to the staff survey). LAs/non-profits providing important public services were also less likely to have created one or more of these roles in the last 3 years (61%, compared to 77% of respondents to the staff survey).

5.5.1.2 Risk management

LAs/non-profits providing important public services were more likely than the average respondent to have changed their risk management (65%, compared to 53% of all respondents to both surveys). They were also more likely to have done a DPIA (62%, compared to 51% of respondents to the staff survey) and to have made changes as a result of the DPIA than the average respondent to the staff survey (67% and 56% respectively). Where no changes were made as a result of a DPIA, LAs/non-profits providing important public services were less likely to have said the measures in place were already sufficient (81%) than the average respondent to the staff survey (91%).

5.5.1.3 Asset management

Respondents to the staff survey that were IT or cyber security professionals were asked additional questions about more technical changes to their cyber security. LAs/non-profits providing important public services were also more likely than the average respondent to have changed their:

- asset management (46%, compared to 34% of all respondents to both surveys)
- tracking and recording of all assets that process personal data (70% of technical respondents from LAs/non-profits providing important public services, compared to 56% of technical respondents to the staff survey)

5.5.2 Protect personal data against cyber attack[102]

The majority of interviewees were confident that the changes they had made as a result of the GDPR had improved their ability to protect themselves from a cyber attack. This response was more common amongst interviewees from LAs/non-profits providing important public services than other organisations because it has led to increased monitoring of their systems and establishing procedures for identification of current threats and weaknesses and put protective measures in place.

5.5.2.1 Service protection policies and processes

LAs/non-profits providing important public services also were more likely to have changed their, Cyber Essentials or Cyber Essentials Plus certification in the last 3 years than the average

[102] *There were no statistically significant differences in how LAs/non-profits providing important public services answered questions relating to NCSC outcome B2 Identity and access control compared to the average respondent*

respondent to both surveys (49%, compared to 38%). This included becoming certified for the first time, getting recertified and upgrading their certification.

5.5.2.2 Data security

Compared to 3 years ago, LAs/non-profits providing important public services were also more likely than the average respondent to rate technical controls for data protection as a high priority now (55%, compared to 43% of respondents to the staff survey). They were also more likely than average to have changed how they encrypt personal data (78% answered 'introduced' and/or 'improved', compared to 65% of technical respondents to the staff survey).

5.5.2.3 System security

LAs/non-profits providing important public services were more likely to have changed how they undertake regular testing to evaluate the effectiveness of their security measures than the average respondent (75% of technical respondents from LAs/non-profits providing important public services, compared to 60% of technical respondents to the staff survey).

5.5.2.4 Staff awareness and training

Provision of GDPR training was more common among LAs/non-profits providing important public services than average (81%, compared to 67% of respondents to the staff survey). Among organisations that provided GDPR training, LAs/non-profits providing important public services (91%) were also more likely to have provided mandatory GDPR training than the average respondent to the staff survey (80%). Provision of specific cyber security training was also more common than average among LAs/non-profits providing important public services (40%, compared to 34% of respondents to the staff survey). LAs/non-profits providing important public services were more likely to have introduced or improved this cyber security training in the last 3 years than the average respondent to the staff survey (92%, compared to 83%).

5.5.3 Detect security threats

5.5.3.1 Security monitoring

LAs/non-profits providing important public services were more likely to have changed their monitoring and review, including audit processes than the average respondent to both surveys (68%, compared to 50%).

5.5.4 Minimise the impact

5.5.4.1 Response and recovery

LAs/non-profits providing important services were more likely to have changed their incident management or recovery processes than the average respondent to both surveys (55%, compared to 45%).

5.5.5 Cyber security expenditure

LAs/non-profits providing important services were more likely to have increased expenditure on both cyber security software (47%) and outsourcing and/or consultancy (33%) than the average respondent to the staff survey (39% and 22% respectively).

5.5.6 Breadth and duration of impact

They were also more likely than the average respondent to both surveys to have agreed or strongly agreed that the impact of the GDPR had been felt across all cyber security related areas in their

organisation (86%, compared to 74%) and that the changes had been sustained (90%, compared to 84%).

Interviewees from LAs/non-profits providing important public services were more likely than interviewees from other organisations to report that they found it challenging to sustain the changes they had made as a result of the GDPR. This was because they had fewer resources and had more changes to make in order to become compliant with the GDPR. They were, therefore, incurring substantial additional ongoing expenses as a result of the GDPR.

5.5.7 Unintended consequences

LAs/non-profits providing important public services (69%) were more likely to have disagreed or strongly disagreed that the GDPR had led to excessive investment in cyber security, significantly beyond what is necessary, than other respondents (60% of all respondents to both surveys).

5.5.8 Factors driving change

Interviewees from LAs/non-profits providing important services were more likely than average to have said that their attitude towards the GDPR was positive. However, they were also more likely than other interviewees to have taken a reactive approach when preparing for the introduction of the GDPR. Interviewees said that this was because they had insufficient internal capacity and capability to develop robust cyber security policies processes.

Where changes had been made, LAs/non-profits providing important public services were more likely than the average respondent to have attributed these changes to:

- introduction of the GDPR (72% of LAs/non-profits providing important public services, compared to 63% of all respondents to both surveys)
- desire to comply with the GDPR and avoid penalties (72%, compared to 66%)
- advice/guidance issued by another government body (40%, compared to 26%)
- advice/guidance given by an external cyber security consultancy/service (32%, compared to 27%)
- response to pressure from the Board (29%, compared to 16%)

Interviewees from LAs/non-profits providing important services said that they would have severe financial issues and may be unable to continue operating if they had to pay a fine for non-compliance. They were, however, less likely to state ‘response to business pressure’ than the average respondent (13%, compared to 21% of all respondents to both surveys).

LAs/non-profits providing important services were more likely to rank ‘introduction of the GDPR’ as the most important factor on cyber security (30%) than the average respondent (23% of all respondents to both surveys).

LAs/non-profits providing important services were more likely to attribute all of the changes in their cyber security in the last 3 years to the introduction of the GDPR than the average respondent (only 90% answered at least to a ‘small extent,’ compared to 82% of all respondents to both surveys).

They were also more likely than average to have said the introduction of the GDPR had influenced:

- changes in their cyber security priorities (93% said the GDPR had influenced this, at least to a ‘small extent,’ compared to 88% of respondents to the staff survey)
- the amount of staff time devoted to data protection (86%, compared to 79%)
- the amount of staff time devoted to cyber and information security (78%, compared to 68%)

LAs/non-profits providing important public services were less likely to attribute changes in their cyber security training to the introduction of the GDPR than the average respondent (83% said the GDPR had influenced this training at least to a 'small extent,' compared to 93% of respondents to the staff survey).

Where no changes were made, LAs/non-profits providing important public services were less likely to have said this was because it was not a priority for their organisation (7%) than the average respondent to both surveys (12%).

5.6 SMEs

SME summary

SMEs were less likely than the average respondent to have:

- made changes to most aspects of their cyber security activity
- done a DPIA (49%, compared to 51% of respondents to the staff survey) - as noted in Section 0, DPIAs were a useful tool for encouraging change
- ranked the 'introduction of the GDPR' as the most important factor for making changes to their cyber security (22%, compared to 23% of all respondents to both surveys)
- attributed all changes in their cyber security to the GDPR (80%, compared to 82% of all respondents to both surveys)

Where changes were not made, SMEs were more likely than the average respondent to have said it was not a priority for their organisation (13%, compared to 12% of all respondents to both surveys).

Therefore, the GDPR appears to have had less of an impact on SMEs than other organisations.

It is important to note that while some of the differences between SMEs and the average respondent presented in this section appear small, they are statistically significant.[103] This is because survey findings have been weighted in line with the total population of the UK economy, which is largely made up of SMEs.

5.6.1 Manage security risk[104]

5.6.1.1 Governance

SMEs (defined as any private sector organisation with fewer than 250 employees) were less likely to rate policies, processes and procedures as a higher priority now than 3 years ago:

- 29% of SMEs rated **data protection policies, processes and procedures** a higher priority now than 3 years ago, compared to 32% of respondents to the staff survey
- 21% of SMEs rated **other information/cyber security policies, processes and procedures** a higher priority, compared to 24% of respondents to the staff survey

[103] *Z-tests were performed on all questions and t-tests were performed on numerical data to 95% confidence level*
[104] *There were no statistically significant differences in how SMEs answered questions relating to NCSC outcomes A3: Asset management or A4: Data processors and the supply chain compared to the average respondent*

They were also less likely than the average respondent to have changed cyber security policies in the last 3 years:

- 67% of SMEs said they introduced new and/or improved data protection policies, compared to 71% of all respondents to both surveys
- 59% of SMEs said they introduced new and/or improved information security policies, compared to 61% of all respondents to both surveys

Interviewees from SMEs were more likely than interviewees from other organisations to have cited outsourced cyber security expertise an enabler for change. This included information on what data protection policies and processes were required to be compliant with the GDPR.

SMEs were also more likely than the average respondent to have at least one employee devoted to cyber security or information security (37%, compared to 36% of respondents to the staff survey) and to have created one or more of these roles in the last 3 years (84% had created at least one cyber/information security role in the last 3 years and 79% had created at least one data protection role, compared to 81% and 77% of all respondents to the staff survey respectively). Where interviewees reported staff changes since the GDPR was introduced, the rationale was typically a lack of in-house expertise to enable them to understand and meet the requirements of the GDPR:

> *"We are a small organisation, and we just didn't have the expertise amongst our staff to understand how best to change our processes so that we would be compliant. It was necessary for us to hire someone with the right knowledge and skills to make us compliant and keep us protected." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

5.6.1.2 Risk management

SMEs were less likely to have changed their risk management in the last 3 years than the average respondent (only 51% of SMEs had made changes, compared to 53% of all respondents to both surveys).

SMEs were less likely to have done a DPIA (49%) than the average respondent to the staff survey (51%).

5.6.2 Protect personal data against cyber attack

The majority of interviewees were confident that the changes they have made as a result of the GDPR have improved their ability to protect themselves from a cyber attack. This response was more common amongst interviewees from SMEs than those from other organisations, because it had caused them to introduce new measures to manage their cyber security.

5.6.2.1 Service protection policies and processes

SMEs were more likely than the average respondent to have introduced and/or improved their ISO certification in the last 3 years (27%, compared to 26% of respondents to the staff survey). This included becoming certified for the first time, getting recertified and upgrading their certification.

5.6.2.2 Identity and access control

SMEs were less likely to have changed their identity and access control than the average respondent (44%, compared to 46% of all respondents to both surveys).

5.6.2.3 Data security

SMEs were less likely than the average respondent to rate technical controls as a higher priority now than 3 years ago:

- 22% of SMEs rated **technical controls for data protection** a higher priority compared to 26% of respondents to the staff survey
- 22% SMEs rated **technical controls for other aspects of information/ cyber security** a higher priority, compared to 24% of respondents to the staff survey

They were also less likely than the average respondent to have changed:

- their technical controls in the last 3 years (43% said these had been 'introduced' and/or 'improved', compared to 45% of all respondents to both surveys)
- how they encrypted personal data (63% of technical respondents from SMEs answered 'introduced' and/or 'improved', compared to 65% of technical respondents to the staff survey)

Respondents to the staff survey that were IT or cyber security professionals were asked additional questions about more technical changes to their cyber security.

5.6.2.4 System security

SMEs were less likely than the average respondent to have changed how they undertake regular testing to evaluate the effectiveness of security measures (only 58% of technical respondents from SMEs said this had changed, compared to 60% of technical respondents to the staff survey):

> *"The GDPR has led to data security being prioritised over other areas of cyber security in our organisation. The changes that we made were more to do with managing data as opposed to improving our cyber security measures. For this reason, I don't think the GDPR has made us safer from a cyber attack, but our data is better protected than before." (Interviewee from an SME in the construction industry)*

5.6.2.5 Staff awareness and training

GDPR training was less common among SMEs (64%) than average (67% of respondents to the staff survey). Among those that provided GDPR training, SMEs were less likely than the average respondent to have provided mandatory GDPR training (78%, compared 80% of respondents to the staff survey). A minority of interviewees, all from SMEs, said that they only provided GDPR training for staff members who processed personal data. They felt that this approach was necessary because they lacked the resources to offer mandatory GDPR training to all staff members. SMEs were also less likely than average to have introduced or improved this cyber security training in the last 3 years (80%, compared to 83% of respondents to the staff survey).

5.6.3 Detect security threats

The majority of interviewees reported that the changes they have made as a result of the GDPR have improved their ability to detect security threats. This response was more common among interviewees from SMEs than other organisations, because before GDPR was introduced they did not know what the risks were.

5.6.3.1 Security monitoring

In addition to tracking and recording of assets, SMEs were less likely than the average respondent to have changed their monitoring and review processes, including audit processes in the last 3 years (46% said it had been 'introduced' and/or 'improved', compared to 50% of all respondents to both surveys).

5.6.4 Minimise the impact

5.6.4.1 Response and recovery

SMEs were less likely than the average respondent to have changed their incident management or recovery processes in the last 3 years (43% said it had been 'introduced' and/or 'improved', compared to 45% of all respondents to both surveys).

5.6.4.2 Improvements

Where changes had been made, most interviewees were confident that they had improved their cyber security. Interviewees from SMEs were more likely than interviewees from other organisations to report this, as due to a lack of resources and expertise they were less likely than large organisations to have had robust cyber security measures in place before the GDPR was introduced. The enforcement of the GDPR was, therefore, a major motivator for them to improve their cyber security.

5.6.5 Cyber security expenditure

SMEs were less likely to have increased expenditure on hardware (28%) and outsourcing/consultancy (20%) than the average respondent (29% and 22% of respondents to the staff survey respectively).

5.6.6 Breadth and duration of impact

SMEs were less likely than average to have agreed or strongly agreed that the:

- impact of the GDPR had been felt across all cyber security related areas in their organisation (73% compared to 74% of all respondents to both surveys)
- changes had been sustained (82%, compared to 84% of all respondents to both surveys)

Interviewees from SMEs were more likely to report that they found it challenging to sustain the changes they had made as a result of the GDPR than those from large organisations. This was because they had relatively fewer resources and had made relatively more changes in order to become compliant with the GDPR. They were, therefore, incurring substantial additional ongoing expenses as a result of the GDPR.

5.6.7 Unintended consequences

SMEs were less likely than the average respondent to have disagreed that the GDPR had detrimental impacts:

- only 42% of SMEs disagreed or strongly disagreed that the GDPR had led to excessive caution amongst staff in the handling of data, compared to 43% of all respondents to both surveys
- only 52% of SMEs disagreed or strongly disagreed that it had led to excessive focus on data protection to the detriment of other aspects of cyber security, compared to 54% of all respondents to both surveys
- only 58% of SMEs disagreed or strongly disagreed that it had led to excessive investment in cyber security, significantly beyond what is necessary, compared to 60% of all respondents to both surveys

Some interviewees felt that the GDPR created an excessive amount of additional work:

> *"It has created a lot of extra work for us." (Interviewee from an SME in the construction industry)*

5.6.8 Factors driving change

SMEs were more likely than the average respondent to have cited 'response to business pressure, i.e. up or down the supply chain' as an influencing factor (22%, compared to 21% of all respondents to both surveys) and 'lobbying or pressure from staff responsible for cyber security/data protection' (7%, compared to 6% of all respondents to both surveys).

SMEs were less likely to rank 'introduction of the GDPR' as the most important factor (22%) than the average respondent (23% of all respondents to both surveys). However, interviewees from SMEs were also less likely to provide details of additional drivers and factors that had influenced changes to their cyber security than large organisations. When asked about this, interviewees from large organisations thought it was because the more people in an organisation, the bigger the range of factors that were likely to affect that organisation's cyber security capability.

SMEs were more likely to have taken a reactive approach to the GDPR than other organisations. Interviewees said that this was due to having fewer resources available to make changes to their processes and policies. They also reported not having the capability to adopt robust cyber security policies. As a result, changes were only made to their cyber security when it became a legal requirement to do so:

> *"Our approach was definitely reactive; in all honesty we probably wouldn't have done what we did if the GDPR was not enforced. When the legislation was announced, we did a lot of research into what it would mean for us and what we would have to do." (Interviewee from an SME in the accommodation and food services industry)*

SMEs were less likely than the average respondent to attribute all of the changes in their cyber security to the GDPR (80% answered, at least to a 'small extent,' compared to 82% of all respondents to both surveys).

SMEs were more likely than the average respondent to attribute changes in their cyber security training to the introduction of the GDPR (95% of SMEs said that the GDPR influenced changes in this training at least to a 'small extent,' compared to 93% of respondents to the staff survey).

However, SMEs were less likely than the average respondent to have said that the following changes were influenced by the introduction of the GDPR, at least to a small extent:

- cyber security activities (89%, compared to 90% of all respondents to both surveys)
- cyber security priorities (86%, compared to 88% of respondents to the staff survey)
- amount of staff time devoted to data protection (77%, compared to 79% of respondents to the staff survey)
- amount of staff time devoted to cyber and information security (66%, compared to 68% of respondents to the staff survey)

Where changes were not made to an organisations cyber security, the main reason given - by SMEs and other respondents alike - was that existing provision was sufficient. However, SMEs were more likely than the average respondent to both surveys to have said it was not a priority for their organisation (13%, compared to 12% respectively), but less likely to have said they 'did not have enough resources to devote to it' (9%, compared to 10%).

5.7 Board level prioritisation of cyber security

Board level prioritisation summary

Board level prioritisation of cyber security had increased in the last 3 years. The vast majority of Board members (92% of respondents to the Board survey) attributed this to the GDPR, at least to a small extent. They also said that the GDPR had a 'great' or 'very great' influence on the Board's awareness of cyber security (37% of respondents to the Board survey) and the frequency of cyber security updates to the Board (32% of respondents to the Board survey).

This indicates that the GDPR has increased Board level prioritisation of cyber security.

The survey found that over the last 3 years, Boards were most likely to have increased their prioritisation of:

- understanding their cyber security threat (63% of respondents to the Board survey said this had increased)
- implementing effective technical cyber security measures (57%)
- developing a positive cyber security culture (54%)
- planning their response to cyber incidents (54%)
- risk management (53%)
- establishing their risk profile baseline and identifying what they care about most (50%)

Some of the Board members interviewed provided more detail on the changes that had been made as a result of this increased prioritisation:

> *"We now ensure that software updates are maintained, and that software is secure, and we regularly monitor any threats. Staff training is now provided to ensure that staff are aware of risks and know not to click on suspicious links in emails. We also now have procedures in place which ensure that only people who should have access to sensitive information are able to access it. This has been done using password protection. We also recovery processes in place to avoid downtime as a result of any cyber attack." (Interviewee from a large business with a complex and interconnected supply chain in the property industry)*

> *"We have updated all our databases and made them more secure. We have also begun asking all clients to opt into receiving information so that we are only contacting people who have given consent to do so." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

> *"We now clear data on a regular basis and ensure that they are not keeping things that they shouldn't." (Interviewee from an SME in the wholesale and retail industry)*

The vast majority of Board members (92% of respondents to the Board survey) attributed this increased prioritisation to the GDPR, at least to a small extent. However, one interviewee reported:

> *"These changes were always in the pipeline because of the need to keep data safe and the GDPR provided additional motivation to make these changes. The GDPR effectively increased the urgency of making these changes, but the changes would likely have happened even if the GDPR was not enforced." (Interviewee from a large business with a complex and interconnected supply chain in the property industry)*

Some of the Board members interviewed said that they did not make changes to their cyber security and that Board prioritisation of cyber security had not increased because it was already high:

> *"Our cyber security measures are reviewed regularly, but Board prioritisation of cyber security has always been high, and this has not changed. We also did not need to make changes to our cyber security management because we were already compliant with the GDPR." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)*

The introduction of the GDPR also had a 'great' or 'very great' influence on the:

- Board's awareness of cyber security (37% of respondents to the Board survey)
- frequency of cyber security updates to the Board (32% of respondents to the Board survey)

Most of the Board members interviewed had a positive attitude towards the GDPR:

> *"Our attitude can be described as positive because everyone has taken the GDPR very seriously. In most recent years it has become more of a key issue." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

> *"Our attitude towards the GDPR is positive because we see it as an opportunity to make sure that we are doing all we can to protect our customer's data." (Interviewee from an SME in the wholesale and retail industry)*

Some Board members had a neutral attitude towards the GDPR. One interviewee explained that:

> *"It was a neutral attitude, because it was mixed. Although some Board members were very receptive to it, the majority felt that the GDPR was a welcome change and was needed, and they knew that more regulation was required. Several Board members pointed out that the GDPR requirements were things that the organisation was doing already and that this was going to add unnecessary work and additional costs, and they wouldn't be adding value to the work that the organisation does. Some Board members also expressed concerns that implementing changes would take time that could be used in other areas of the organisation." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)*

Most of the Board members interviewed had taken a proactive approach towards the GDPR:

> *"We knew that the GDPR was coming long before the announcement in 2016 and were already compliant." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)*

> *"Our approach was proactive because the Board have thought about cyber security well in advance of the GDPR being enforced. As a result, we were organised, and the changes were not left until the last minute." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

Some of the Board members interviewed reported taking a reactive approach to the GDPR. They felt that they would not have made changes to their cyber risk management if the GDPR had not been enforced.

A minority of the Board members interviewed reported that there had been barriers to changing their cyber risk management, mainly relating to knowledge and resources. One interviewee explained how they had overcome these barriers through staff training:

> *"Staff training was a barrier as some staff were not up to speed with IT and the need to keep data safe. This was overcome by internal training and PowerPoint presentations with mini tests at the end to ensure that staff understood what they were being taught." (Interviewee from a large business with a complex and interconnected supply chain in the property industry)*

Some of the Board members interviewed reported that there were factors that enabled some of the changes they made, including ICO guidance:

> *"The ICO provided information which was very helpful, and it was clear from reading that what we needed to do to be compliant." (Interviewee from a large business with a complex and interconnected supply chain in the property industry)*

> *"We are part of a franchise which made making the changes much easier. This was because we could talk with a wide variety of people and get advice on what to do from other Board members and stakeholders." (Interviewee from a large business with a complex and interconnected supply chain in the information and communication industry)*

All Board interviewees reported that cyber security was still on the Board's agenda:

> *"Cyber security and the GDPR are not things that will go away so it is right that they are on the Board's agenda." (Interviewee from an LA/non-profit providing important public services in the public administration and defence industry)*

> *"Cyber security in our organisation is reviewed regularly and we provide info to ICO. This is in line with regulations." (Interviewee from a large business with a complex and interconnected supply chain in property industry)*

6 CONCLUSIONS

This section presents the conclusions of the primary and secondary research against each of the key research questions. It also summarises the possible implications of these conclusions for the forthcoming review of cyber security incentives and regulations.

Based on existing research in this subject area, what has been the impact of the GDPR and NIS Regulations on organisations' cyber security outcomes?

The infancy of the GDPR[105] and NIS[106] regulations meant there was limited academic, peer-reviewed literature on how the GDPR has impacted cyber security behaviours and the actions of organisations, specifically in the UK. The NIS Review, published on 28 May 2020, could not be included in this report due to timings. Thus, firm conclusions on the impact of these regulations on the UK specifically cannot be drawn from existing research - which further supported the need to address this gap through our primary research. The Cyber Security Breaches Survey 2020[107] found that the GDPR has motivated organisations to make improvements to their cyber risk management. While it was clear that many of these improvements were being maintained, there was less evidence that they were being enhanced or improved upon.

Have organisations across the economy improved their cyber risk management as a result of the GDPR (using the NCSC cyber security outcomes as criteria for assessing whether organisations have taken the necessary cyber security measures following the introduction of the GDPR)?

The survey evidence showed that most organisations have improved their cyber risk management in line with NCSC guidance,[108] particularly in relation to governance, risk management, data security and system security. In the last 3 years, most organisations have increased their prioritisation of cyber security, as well as increasing spend in this area. Most organisations have also introduced new or improved data protection and other cyber security policies, processes, procedures and technical controls, including measures to protect personal data and the systems that processed it against cyber attack (see Figure 6.1). Less change was evident in relation to procurement and supply chain risk management.

[105] *The GDPR came into force in May 2018*
[106] *The NIS Directive came into force in May 2018*
[107] *DCMS, Ipsos MORIi and University of Portsmouth (2020) Cyber Security Breaches Survey 2020*
[108] *NCSC guidance on GDPR security outcomes: HTTPS://WWW.NCSC.GOV.UK/GUIDANCE/GDPR-SECURITY-OUTCOMES (accessed May 2020)*

Figure 6.1: Summary of improvements against the NCSC GDPR security outcomes

Manage security risk

Most organisations had improved their **governance** of cyber security:
- around half of the Board members surveyed (46%-54%) said prioritisation of cyber security governance had increased
- most organisations improved their data protection and information security policies (71% and 62% of all respondents to both surveys respectively)
- most organisations had some form of cyber security strategy (69% of respondents to the Board survey)
- most Board of Directors' awareness of cyber security increased (65% of respondents to the Board survey)
- Board cyber security updates were more comprehensive, robust and responsive to external changes (83% of respondents to the Board survey)

However, it is concerning that:
- a minority of organisations had no formal cyber security strategy (31% of respondents to the Board survey)
- only 33% of Board members were aware of the NCSC Board Toolkit and only 34% of them had used it
- over a third of Board members received cyber security updates on an ad hoc basis (14%) or not at all (22%)

Most organisations had improved their **risk management**:
- most Boards had increased their prioritisation of understanding the threat (63% of respondents to the Board survey), risk management (53%) and establishing their risk profile baseline (50%)
- most organisations had introduced new or improved risk management processes (53% of all respondents to both surveys)
- around half of organisations had completed a DPIA (51% of respondents to the staff survey), with half of these organisations having made changes as a result (56%)

Findings in relation to **asset management** were mixed**:**
- 34% of all respondents to both surveys had their organisation had introduced or improved its asset management
- 56% of technical respondents reported improved tracking and recording of all assets that process personal data

Less change was evident in relation to **data processors and the supply chain**:
- most Board members had not changed how they worked with suppliers and partners to manage supply chain risks (54%)
- a minority of organisations had improved procurement or supply chain risk management (33%)

Protect personal data against cyber attack

Findings on **service protection policies and processes** were mixed:
- most organisations improved processes for ensuring that web services were protected (59% of technical respondents)
- a minority had improved ISO (26%) and Cyber Essentials/Cyber Essentials Plus certification (38% of all respondents) including becoming certified for the first time, getting recertified and upgrading their certification

Findings were mixed in relation to **identity and access control**:
- improved cyber security technology/security of emails, including improved access control was the most common change made in response to doing a DPIA (41%)
- less than half of the organisations surveyed (46%) had introduced and/or improved their identity and access controls

Most organisations had improved their **data security**:
- most Board members increased their prioritisation of implementing effective technical cyber security measures (57%)
- most organisations had improved encryption of personal data (65% of technical respondents to the staff survey)
- around half of organisations had improved technical controls (45% of all respondents to both surveys)

The majority of organisations had improved their **system security**:
- 60% of technical respondents to the staff survey changed how they minimise the opportunity for attack
- 60% changed how they undertake regular testing to evaluate security measures
- 55% changed how they ensure the processing environment remains secure
- 55% changed how they actively manage software vulnerabilities
- 52% changed how they manage end user devices

Findings in relation to **staff awareness and training** were mixed:
- while 67% of respondents to the staff survey said their organisation provided training on the GDPR, 32% did not
- only a third of respondents (34%) provided specific cyber security training
- where specific cyber security training was provided, it had typically been introduced in the last 3 years (83%)

Detect security threats

Findings in relation to **security monitoring** were mixed:
- Half of organisations had improved monitoring and review processes (50% of all respondents to both surveys)

Minimising the impact

Findings in relation to **response and recovery** were mixed:
- 54% of Board members said their prioritisation of planning their response to cyber incidents had increased
- 45% of all respondents to both surveys said their organisation had improved incident management or recovery processes

Findings in relation to **improvements** indicate that organisations that had experienced a cyber security incident were more likely to have made changes in line with the NCSC cyber security outcomes in the last 3 years than those that had not experienced an incident.

It is encouraging to note that:

- most organisations had some form of cyber security strategy in place (69% of respondents to the Board survey)[109]
- most Board members received regular cyber security updates (52% of respondents to the Board survey received cyber security updates at least once a quarter)
- where organisations had employees who specialised in data protection or cyber security, the majority had created one or more of these roles in the last 3 years (77% of respondents to the staff survey had created at least one data protection role and 81% had created at least one cyber security role)

However, it is concerning that cyber security is still not getting the strategic focus required in a minority of organisations. The survey found that:

- 31% of Board members said they had no formal cyber security strategy
- a substantial proportion of respondents had no data protection staff (35%), and most had no additional specialist cyber security staff (54%)
- only 33% of Board members were aware of the NCSC Board Toolkit and, of those who were aware of it, only 34% had actually used it
- over a third of Board members said they only received cyber security updates on an ad hoc basis (14%) or not at all (22% of respondents to the Board survey)

This raises the question of how to change this mindset in a minority of organisations. Potential interventions could include raising awareness of the business benefits of improving cyber security. It also raises a broader issue about how to get advice and guidance to the intended audience and get them to act upon it.

Organisations identified a range of factors that had influenced changes in their cyber security in the last 3 years, however, those linked to the GDPR were considered the most important (23% said the introduction of the GDPR was the most important factor). The vast majority of respondents also said that all of the changes in their organisation's cyber security were a result of the introduction of the GDPR, at least to a small extent (82%).

There was also evidence that the impact of the GDPR varied based on certain organisational characteristics. Organisations that had experienced a cyber security incident were more likely to have improved their cyber security measures in the last 3 years than those that had not experienced an incident. As were organisations that had conducted a DPIA or those that processed personal data. It is important to note, however, that these 3 groups were not mutually exclusive and there was some overlap between them.

This suggests that the GDPR has successfully encouraged improvement in cyber risk management for organisations that are within the scope of the regulation. It also indicates that organisations that are not in scope, or those that think they are not in scope could benefit from further support and guidance in this area. This could be done by providing organisations with greater insight into the changing nature of cyber risks and the damage they can do to an organisation, without them having to undergo the trauma of an incident - as experience of an incident also appeared to encourage organisations to take action. Alternatively, encouraging greater use of Business Impact Assessments

[109] *Totals do not sum due to rounding: 18% of Board members surveyed said that their organisation had a dedicated cyber security strategy, 52% had a cyber security strategy as part of their IT strategy and 31% had no formal cyber security strategy in place*

would help organisations to understand the specific impact of a potential breach and accept that it could happen to them.

Have improvements been realised equally or partially across all aspects of cyber security (such as preventing disruption of services, protecting valuable non-personal data and protecting personal data)?

Both the primary and secondary research indicated that improvements have not been realised equally across all aspects of cyber security. Most organisations surveyed in the primary research agreed that the impact of the GDPR had been felt across all cyber security related areas within their organisation (74% of all respondents to both surveys). However, although there was evidence that most organisations had introduced or improved their cyber risk management in the last 3 years, more improvements were reported in relation to governance, risk management, data security and system security. We also found that organisations were more likely to have made changes to data protection than other aspects of cyber security. This is covered in more detail later in this section in relation to unintended consequences.

The secondary research showed that companies with technical cyber security controls in place were less likely to have formal cyber security policies, indicating a more technical response from these organisations. The literature also suggested that while the GDPR had impacted on information security in relation to data protection, there was no robust evidence to show it had impacted on other areas of cyber security to the same extent (such as application security, network security and disaster recovery and continuity planning). In addition, the 2020 Cyber Security Breaches Survey[110] suggested that there was still more that organisations could do to improve their cyber security such as audits, cyber insurance, supplier risks and breach reporting.

The greater focus on certain, mainly preventative, aspects of cyber security suggests that organisations could benefit from improving the 'non-preventative' aspects of cyber security (such as detection, response and recovery), as well as their supply chain management. The fact that organisations often took a mainly technical response to cyber security, and that it was not a strategic focus for a minority of respondents, suggests that they could benefit from interventions that encourage greater cyber resilience through incident response planning and testing and updating processes on a regular basis.

For those organisations that have taken appropriate action, has the impact been sustained over one year on from implementation?

There was limited existing research on whether the reported impact of the GDPR on cyber security practices had been sustained. However, the vast majority of organisations surveyed as part of our primary research agreed that the changes implemented due to the GDPR had been sustained (84% of all respondents to both surveys). Challenges to sustainability mainly related to the ongoing costs associated with maintaining compliance and staff awareness that the GDPR was an ongoing issue, not a 'one-off'.

It may be too soon to determine whether these changes have resulted in a longer-term behaviour change or a cultural shift towards more robust practices. This is a potential area for further research in the future.

[110] *DCMS, Ipsos MORI and University of Portsmouth (2020) Cyber Security Breaches Survey 2020*

Where organisations have not taken the actions advised by the NCSC, what are the reasons behind this?

Where organisations had not changed their cyber security practices in the last 3 years, in the majority of cases it was because they felt existing measures were sufficient (61% of all respondents to both surveys). Interviewees were confident in their organisation's ability to manage cyber security risks, protect themselves against a cyber attack, detect security threats and minimise the impact of an incident because they had robust policies and procedures in place, and their staff had appropriate cyber security expertise. It is possible, however, that in some cases this confidence may be misplaced. Some organisations may benefit from assistance in assessing their risk posture and the appropriateness of the measures they have taken. This suggests that organisations would benefit from advice and guidance on the:

- changing nature of cyber security threats
- full extent of the cyber security implications of the GDPR
- benefits to their business of improving their cyber security

Have there been any other/unintended consequences as a result of the introduction of the GDPR (such as prioritisation of data security leading to neglect of other important areas of cyber security)?

Some organisations felt that the GDPR had resulted in detrimental impacts:

- 50% of all respondents to both surveys said that the GDPR had led to excessive caution amongst staff in the handling of data
- 36% reported excessive focus on data protection to the detriment of other aspects of cyber security
- 27% noted excessive investment in cyber security, significantly beyond what was necessary
- 78% of Board members surveyed agreed or strongly agreed that, compared to 3 years ago, the cyber security updates they received were more focused on data protection than general cyber security

As noted above, organisations were also more likely to have made changes to data protection than other aspects of cyber security:

- 58% of respondents to the staff survey had at least 1 FTE devoted to data protection, while only 36% had at least 1 additional cyber security FTE
- 54% of respondents to the Board member survey said that the staff time devoted to data protection had increased in the last 3 years, while only 49% said that the staff time devoted to other aspects of cyber security had increased in during that time
- 67% of respondents to the staff survey provided GDPR training, in most cases this GDPR training included aspects of cyber security (86%), however, only 34% provided specific cyber security training
- respondents to the staff survey were also more likely to report an increase in the priority of policies, processes, procedures and technical controls for data protection than for other aspects of cyber security

This suggests that organisations would benefit from further consideration and guidance on the appropriate balance between data protection and other aspects of cyber security when developing any future cyber security regulations and incentives.

Has the GDPR improved Board level prioritisation of cyber security?

There were mixed views in the existing research about Board level prioritisation of cyber security. Some existing research suggested that there had been improvements in the management of cyber security and that Board level discussion had increased since the GDPR was introduced. However, other reports suggested that Boards were continuing to neglect cyber security as a business risk, with many stating they did not have a Board member with specific responsibility for cyber security and did not undertake a regular formal review of cyber security risks and management.

However, our primary research indicated that in the majority of organisations, the GDPR had improved Board level prioritisation of cyber security and that this improvement had been sustained. The Board survey found that, in the last 3 years, most Boards increased their prioritisation of:

- understanding their cyber security threat (63% of respondents to the Board survey)
- implementing effective technical cyber security measures (57%)
- developing a positive cyber security culture (54%)
- planning their response to cyber incidents (54%)
- risk management (53%)
- establishing their risk profile baseline and identifying what they care about most (50%)

The vast majority of Board members (92% of respondents to the Board survey) attributed this increased prioritisation to the GDPR, at least to a small extent. The introduction of the GDPR also had a 'great' or 'very great' influence on the:

- Board's awareness of cyber security (37% of respondents to the Board survey)
- frequency of cyber security updates to the Board (32%)

Most of the Board members interviewed had a positive attitude towards the GDPR and had taken a proactive approach to preparing for its introduction. However, some of the Board members interviewed reported taking a reactive approach to the GDPR. They felt that they would not have made changes to their cyber risk management if the GDPR had not been enforced.

A minority of the Board members interviewed reported that there had been barriers to changing their cyber risk management, mainly relating to knowledge and resources. Factors that enabled changes included guidance from ICO and other sources.

All Board members interviewed said that cyber security was still on the Board's agenda. However, as noted previously, a minority of organisations were still not giving cyber security the strategic focus required.

Has the impact of the GDPR varied by industry?

Note: While total responses can be generalised, survey findings by industry are indicative and should not be generalised to represent the wider population.

The survey evidence indicated that the GDPR had not impacted all organisations equally. At an industry level, organisations in the finance and insurance industry were more likely than other respondents to have made positive changes to their cyber security in the last 3 years. Interviewees attributed this to the volume and nature of personal data that they hold, which could be more valuable to a potential attacker. The finance and insurance industry is a heavily regulated industry, which may also have influenced the changes made.

It is interesting to note that the GDPR appeared to have been a greater influence on organisations providing public services. Those in public administration and defence (36%) and health (32%) were more likely than the average respondent to have cited 'introduction of the GDPR' as the most important factor in influencing changes to their cyber security (23% of all respondents to both surveys). Organisations in finance and insurance; arts, entertainment, recreation and other services; wholesale and retail; education; health; and public administration and defence were more likely than the average respondent to have attributed all of the changes in their cyber security over the last 3 years to the introduction of the GDPR (100%,[111] 94%, 90%, 89%, 89% and 89% of respondents respectively said that all of the changes in their organisation's cyber security in the last 3 years were a result of the GDPR at least to a small extent, compared to 82% of all respondents to both surveys).

This highlights the benefits of tailoring guidance and interventions by industry, taking account of differences in motivation and influences and linking security outcomes more clearly to the business goals that they care most about. The qualitative interviews showed that, where organisations had struggled to understand what they needed to do to comply with the GDPR, tailored guidance had helped them.

Has the impact of the GDPR varied by special interest group?

This was not a specific research question, however, DCMS has a particular policy interest in:

- large businesses
- large businesses with complex and interconnected supply chains
- MSPs
- LAs/non-profits providing important public services
- SMEs

We, therefore, explored any statistically significant differences in the survey responses of these groups. This indicated differences in the impact of the GDPR on the special interest groups.

Note: While total responses and responses for SMEs can be generalised, survey findings for large businesses, large businesses with complex and interconnected supply chains, MSPs and LAs/non-profits providing important public services are indicative and should not be generalised to represent the wider population.

Large businesses with complex and interconnected supply chains were more likely than other respondents to have made changes and increased their spending on all aspects of cyber security.

[111] *When rounded to the nearest whole number*

They were also more likely than the average respondent to have at least one employee who specialised in data protection and cyber security (74% had at least one data protection role and 78% had at least one cyber or information security role, compared to 58% and 36% of respondents to the staff survey respectively) and to have created one or more of these roles in the last 3 years. This indicates that the GDPR had encouraged large businesses with complex and interconnected supply chains to increase their capacity and capability in relation to data protection and cyber security. Care should be taken when interpreting these findings as the base for this group was less than 100 respondents.

LAs/non-profits providing important services were more likely to have made changes to a range of aspects of cyber security as a result of the GDPR than the average respondent. They were more likely to rank the introduction of the GDPR as the most important factor in driving changes to their cyber security (30%, compared to 23% of all respondents to both surveys). This indicates that the GDPR had more of an impact on LAs/non-profits providing important public services than on the average respondent.

Large businesses were more likely than other respondents to have made changes across a number of cyber security aspects. They were also more likely to have provided GDPR training (83%, compared to 67%) and to have included elements of cyber security within their GDPR training than the average respondent (95%, compared to 86%). They were also more likely than the average respondent to have provided specific cyber security training (69%, compared to 34%) and to have introduced or improved this cyber security training in the last 3 years (91%, compared to 83%). This indicates that the GDPR has led to improvements in staff awareness and training within large businesses.

SMEs were less likely to have made changes to their cyber security as a result of the GDPR than the average respondent. Where changes were not made, the main reason given was that existing provision was sufficient, however, SMEs were more likely than the average respondent to have said it was not a priority for their organisation (13%, compared to 12% of all respondents to both surveys). SMEs were also less likely than the average respondent to have done a DPIA (49%, compared to 51% of respondents to the staff survey).

SMEs were less likely to rank the introduction of the GDPR as the most important factor in driving changes to their cyber security (22%, compared to 23% of all respondents to both surveys). They were also less likely than the average respondent to attribute all of these changes to the GDPR (80% of SMEs said that the GDPR had influenced all changes at least to a small extent, compared to 82% of all respondents to both surveys). This indicates that the GDPR had less of an impact on SMEs than on the average respondent.

MSPs were less likely than other respondents to have changed their cyber security behaviour in the last 3 years. This indicates that the introduction of the GDPR had less of an impact on MSPs directly than on the average respondent. However, most interviewees from MSPs reported that the GDPR had positively impacted their relationships with the organisations they provide services to.

This reiterates the value of tailoring guidance and intervention, taking account of differences in motivation and influences across different organisations and more clearly linking security outcomes to their business goals.

What are the possible implications for the forthcoming review of cyber and regulatory landscape?

Our findings in relation to the above research questions suggest further consideration could be given to:

- raising awareness of the NCSC Board Toolkit and the benefits of using it
- providing organisations outside the scope of the GDPR, or those that think they are out of scope, with greater insight into the changing nature of cyber risks and the damage they can do to an organisation, so that they may learn from others without the need to actually experience an incident themselves
- encouraging organisations to undertake Business Impact Assessments to understand the specific impact of a potential breach and accept that it could happen to them
- promoting greater cyber resilience by encouraging organisations to take a more holistic approach to cyber security, expanding their current focus on manage and protect to include aspects such as detect, respond, recover and improve
- making all organisations more aware of the:
  - changing nature of cyber security threats
  - full extent of the cyber security implications of the GDPR
  - benefits to their business of improving their cyber security
- the appropriate balance between data protection and other aspects of cyber security
- tailoring any future guidance and incentives to their audience, for example, by industry and type of organisation, taking account of differences in motivation and influences and linking security outcomes more clearly to the business goals that they care most about – there is also a broader issue around ensuring the message is reaching its intended audience and that they are motivated to act upon it
- the feasibility and timing of further research to determine whether the changes in cyber security risk management or cyber security measures have resulted in a longer-term behaviour change or a cultural shift towards more robust practices

7 APPENDIX A: METHODOLOGY

7.1 Stage 1: Project Inception

The assignment commenced with a formal inception meeting with DCMS and representatives from the National Cyber Security Centre (NCSC) in line with Prince 2 project management principles on 14th August 2019. At this meeting the online methodology was discussed and agreed as documented in the Project Inception Document.

7.2 Stage 2: Stakeholder engagement

RSM engaged with 21 representative bodies and associations to promote the benefits of the research and to ask for their support in promoting the involvement of their members. Stakeholder consultations were conducted via structured telephone interview (see Appendix C for interview topic guide). A short, written response template was also developed and shared with stakeholders who wanted to take part in the research but who were unable to do so by phone. No respondents submitted a written response.

Only one stakeholder declined to take part in our research. A total of 7 stakeholders took part in a telephone interview between 2nd September 2019 and 11th October 2019. Of these, all 7 agreed to promote the survey to their members. These included a cross section of organisation types. We also emailed details of the survey to those stakeholders who did not respond, inviting them to share this information with their members (see textbox below).

Stakeholder email

Following our discussion in September, I am writing to provide you with more information about our survey to assess the impact that the GDPR has had on cyber security. We appreciate any support you can offer to help promote this survey to your members (e.g. through regular comms channels, local meetings/ chapters and events).

The Department for Digital, Culture, Media and Sport (DCMS) has commissioned research to assess the impact that the introduction of General Data Protection Regulation (GDPR) has had on incentivising organisations across the UK to improve their cyber security outcomes. The research findings will be used to inform the Department's comprehensive review of the UK's cyber security incentives and regularity landscape, in order to consider whether further intervention is needed.

This important research will be informed by a telephone survey, conducted by BMG Research Ltd (BMG) in collaboration with RSM UK Consulting LLP (RSM). The survey will take place between October and December 2019. It aims to capture the views and experiences of over 1,000 staff and Board members across the UK. Its success depends on the participation of staff responsible for cyber security and relevant Board members (e.g. the Chair of the Audit Committee or Risk Committee). Your participation in this research would be appreciated by DCMS and the research team. For more information about the survey please contact [contact name and email] at BMG, or visit the survey microsite https://www.bmgresearch.co.uk/gdprsurvey/

7.3 Stage 3: Rapid literature review

A rapid literature review was completed using a range of online databases including Google; Google Scholar; Cochrane Library; Wiley Online Library; IngentaConnect; Journal of Cybersecurity; and International Journal of Law and Information Technology.

The following search terms were used: 'impact of NIS Regulations', 'impact of GDPR', 'changes to practices and behaviours', 'investment in cyber security', and 'prioritisation of approaches'. Each were cross-referenced with 'cyber security', 'NIS', and 'GDPR'.

Due to the relatively recent implementation of the GDPR[112] and NIS[113] regulations, there was limited academic, peer-reviewed literature available. Therefore, additional information was sourced from grey literature, including online articles relating to the impact of the GDPR and the NIS Regulations on cyber security. In total 24 articles were selected that met the research objectives (see Section 2.3).

7.4 Stage 4: Design and piloting of the quantitative surveys (Staff and Board members)

The design of the quantitative survey questionnaires was based on the NCSC cyber security outcomes (see Table 7.1) and built on data already available from the DCMS Cyber Security Breaches Survey as well as the NCSC/DCMS UK Cyber Security Survey. The questionnaires for the staff and Board member surveys are contained in Appendix D-G.

We performed cognitive testing of the survey instruments with the first 19 respondents between 28th October and 1st November 2019 and refined the questions as needed.

Note: All fieldwork activity, including the survey pilot, was paused from w/c 4th November 2019 following general election guidance issued by the Cabinet Office on 4th November 2019. Fieldwork resumed on 6th January 2020 and was completed on 28th February 2020.

[112] *The GDPR came into force in May 2018*
[113] *The NIS Directive came into force in May 2018*

Table 7.1: Mapping survey questions to NCSC Outcomes

NCSC Broad Outcome	NCSC Specific Outcome	Staff Survey Questions	Board Survey Questions
A: Manage Security Risks	1: Governance	10,11,13,14, 24a,b,26a,b	10, 11, 13, 15, 16, 17, 18, 19, 21, 23a-c,25a,b
	2: Risk Management	26c,29,30,31,32	23d,e,f, 25c
	3: Asset Management	26d, (+ 26l technical)	25d
	4: Data Processors and the Supply Chain	26e	23h,25e
B: Protect your Personal Data Against Attack	1: Service Protection Policies and Processes	26f,g (+ 26q technical)	25f,g
	2: Identity Access and Control	26h	25h
	3: Data Security	24c,d,26i, (+ 26p technical)	25i
	4: System Security	26m,n,o,r,s technical	N/A
	5: Staff Awareness and Training	16,17,18,19,20	8c,d
C: Detect Security Threats	1: Security Monitoring	26k	25k
D: Minimise the Impact	1: Response and Recovery Planning	26j	23i,25j
	2: Improvements	9	7

7.5 Stage 5: Refined research methodology and tools/research plan

We refined our proposed research methodology in collaboration with DCMS during Stages 1 to 4 of our research. The finalised research methodology, project plan and research tools where submitted to DCMS for review on 16th October and finalised on 8th November 2019 following the survey pilot.

7.6 Stage 6: Quantitative surveys of staff and Board members

The quantitative surveys of staff and Board members was undertaken primarily using Computer Assisted Telephone Interviewing (CATI) due to better typical response rates relative to online surveys and to better allow for targeting of interviews in key subgroups (particularly large businesses). However, this was used in combination with Computer Assisted Web Interviewing (CAWI), using Dynata survey panel to help boost response rates.

Inter-Departmental Business Register (IDBR) data was used to identify target organisations. IDBR covers businesses, non-profits and Local Authorities in all industry across the UK at the enterprise level, which was desirable for this research because multi-site organisations will typically have connected IT devices and centralised cyber security. The framework used for compiling the IDBR is robust and its use has been validated by multiple Government surveys.

We undertook telematching to address gaps in IDBR data and then called the numbers listed to work directly with organisational gatekeepers to identify the appropriate individual to speak with, and to share information and letters of assurance designed to maximise engagement. Interviewers were

provided with tiered lists of the types of job titles we would expect appropriate respondents to hold (e.g. Chief Executive, Head of Compliance/Data Protection, Chief Data Officer, Data Protection Officer, Information Officer, Privacy Officer, Data Protection/Compliance Manager, Information Security Architect/Engineer), to support gatekeepers to direct calls and ensure we were put through to the correct person.

Table 7.2 details the population profile and the target sample agreed with DCMS for each group of interest. The groups noted below are not mutually exclusive (e.g. large businesses with complex and interconnected supply chains are also included under 'large business') and as such, their sum will exceed the total sample size of 1,170.

Table 7.2: Sampling by special interest group

Special interest group	Total Population (2018)	Target sample size
Large businesses (private sector organisations with 250 employees or more)	7,465	342
Large businesses with complex and interconnected supply chains	2,340	203
Managed service providers (an outsourced third-party company that manages and assumes the responsibility of a defined set of day-to-day management services to its customers)	1,500 (Source Cloudtango)	50[114]
LAs/non-profits providing important public services not in scope of the NIS Regulations	28,460	315
SMEs (private sector organisations with less than 250 employees)	2,721,734	748

Source: ONS UK BUSINESS: ACTIVITY, SIZE AND LOCATION – 2018; Cloudtango https://www.cloudtango.org/MSPs/UK/map/

To facilitate a robust analysis by size and type of organisation, we disproportionately stratified the sample (see Table 7.3).

We also disproportionately stratified the sample by industry, boosting the strata for industries of salient interest to this research (to at least 100 organisations).

In order to maximize response rates, we offered a flexible approach to CATI interview times and appointment booking. The survey stressed the long-term significance of this research, emphasising to respondents that their contribution really did matter; we reassured respondents as to the confidentiality of any information they provided via a Privacy Notice; all interviewers were briefed in advance; we created a survey micro-site to provide information on the research and used Confirmit software to monitor quotas in real-time.

[114] *Plus any organisations interviewed that fall within the DCMS definition of a MSP but who are not listed under SIC codes 6209 or 6311 (see screening questions of survey)*

Table 7.3: Sampling by industry, size and type of organisation

Standard Industrial Classification (SIC) code	Private sector			Non-profit Body or Mutual Association			Local Authority			Sample		
	0-249	250+	Sub-total	0-249	250+	Sub-total	0-249	250+	Sub-total	0-249	250+	Total
01-03: Agriculture, forestry & fishing	15	5	20			0			0	15	5	20
05-39: Production (incl. energy and excl. manufacturing 10-32)	5	5	10			0	5		5	10	5	15
10-32: All Manufacture excl. Pharm (see below)	5	85	90			0			0	5	85	90
21: Manufacture of basic pharmaceutical products and pharmaceutical preparations	5	5	10			0			0	5	5	10
41-43: Construction	90	10	100			0			0	90	10	100
45: Motor trades	12	5	17			0			0	12	5	17
46: Wholesale	26	6	32			0			0	26	6	32
47 Retail	5	46	51			0			0	5	46	51
49-53: Transport & Storage (incl. air transport)	64	36	100			0			0	64	36	100
55-56: Accommodation & food services	34	16	50			0			0	34	16	50
58-63: Information & communication excl. MSP (see below)	45	5	50			0			0	45	5	50
6209: Other information technology and computer service activities- MSPs	9	16	25			0			0	9	16	25
6311: Data processing; hosting and related activities- MSPs	9	16	25			0			0	9	16	25
64-66: Finance & insurance	15	20	35	15		15			0	30	20	50
68: Property	25	10	35	10	5	15			0	35	15	50
69: Legal and accounting activities	5	21	26			0			0	5	21	26
70-75: Professional, scientific & technical excl. 7022 (see below)	24	5	29	15		15			0	39	5	44
7022: Business and other management consultancy activities	20	10	30			0			0	20	10	30
77-82: Business administration & support services	35	15	50			0			0	35	15	50
84: Public administration & defence			0			0	80	20	100	80	20	100
85: Education excl. 8542: Tertiary education (see below)	5		5			0	65	10	75	70	10	80
8542: Tertiary education (target 20/130 universities			0		20	20			0	0	20	20
86-88: Health excl. 87, 8810 & 8899 (see below)			0	30	5	35	10		10	40	5	45
87: Residential care activities			0	20	5	25			0	20	5	25
8810: Social work activities without accommodation for the elderly and disabled			0	10	5	15			0	10	5	15
8899: Other social work activities without accommodation n.e.c.			0	20	5	25			0	20	5	25
90-99: Arts, entertainment, recreation & other services		5	5	10	5	15	5		5	15	10	25
Total	**453**	**342**	**795**	**130**	**50**	**180**	**165**	**30**	**195**	**748**	**422**	**1,170**

	Large businesses (private sector organisations with 250 employees or more)
	Large businesses with complex and interconnected supply chains
	MSPs (an outsourced third-party company that manages and assumes the responsibility of a defined set of day-to-day management services to its customers)
	LAs/non-profits providing important public services not in scope of the NIS Regulations

7.7 Stage 7: Quantitative survey analysis and qualitative field work planning

The survey findings were weighted by size and industry to match the characteristics of the overall population profile (see Table 7.4).

Table 7.4: Weighting factors

	0-49	50-249	250+	Total
01-03: Agriculture, forestry & fishing	148,675	400	80	149,155
05-39: Production	142,500	6,505	1,400	150,405
41-43: Construction	329,185	2,070	310	331,565
45-47: Wholesale and retail; repair of motor vehicles	374,025	5,105	1,130	380,260
49-53: Transport & Storage (incl. postal)	107,010	1,575	395	108,980
55-56: Accommodation & food services	149,230	3,250	630	153,110
58-63: Information & communication	216,880	1,865	390	219,135
64-66: Finance & insurance	57,125	925	375	58,425
68: Property	95,605	585	220	96,410
69-75: Professional, scientific & technical	463,725	3,700	750	468,175
77-82: Business administration & support services	218,390	4,040	1,140	223,570
84: Public administration & defence	6,755	170	375	7,300
85: Education	38,550	4,030	1,385	43,965
86-88: Health	102,090	5,195	1,135	108,420
90-99: Arts, entertainment, recreation & other services	168,095	1,965	505	170,565
Total	**2,617,840**	**41,380**	**10,220**	**2,669,440**

Survey data was analysed using descriptive statistics to summarise findings for the total population as well as by individual variables to identify patterns (for example, by special interest group and industry). The figures used throughout this report are based on the weighted base, but the unweighted base has also been included for reference.

We shared a summary of the salient findings from the survey with DCMS on 16th March 2020 and met on 23rd March 2020 to discuss these findings.

7.8 Stage 8: In depth interviews with staff and Board members

In-depth interviews were used to probe the findings of the quantitative survey in more detail. While the quantitative survey identified what changes have been made regarding cyber security and differences between certain groups, the in-depth interviews identified the reasons behind these changes.

We completed 67 in-depth telephone interviews with a sample of staff and Board members who consented, via the quantitative survey, to do a follow up interview. An incentive of a £50 voucher or charity donation was offered to encourage participation. The topic guide for these interviews are included in Appendix H.

The total number of interviews achieved (67) between 3rd February 2020 and 20th March 2020 was below target (100). The outbreak of COVID-19 in the UK had a substantial impact on interview

scheduling. A total of 31 interviewees dropped out of interviews scheduled in March 2020 citing COVID-19 planning or preparations as the reason. As shown in the tables below, we targeted a diverse mix of interviewees.

We also sought to interview those that reported improvements via the quantitative survey (63) and those that had not (4), as well as those that had experienced a cyber security incident (15) and those that had not (52).

Table 7.5: Profile of interviewees by Board members and staff

Interviewee	Target	Achieved	%
Board member	25	5	20%
Staff	75	62	83%
Total	**100**	**67**	**67%**

Table 7.6: Profile of interviewees' organisations by size

No. of employees	Target	Achieved	%
250+	25	12	48%
0 - 249	75	55	73%
Total	**100**	**67**	**67%**

Table 7.7: Profile of interviewees' organisations by industry

SIC Code	Target	Achieved	%
05-39: Production	10	1	10%
41-43: Construction	10	2	20%
45-47: Wholesale and retail; repair of motor vehicles	10	2	20%
49-53: Transport & Storage (incl. postal)	10	3	30%
58-63: Information & communication	10	10	100%
69-75: Professional, scientific & technical	10	4	40%
84: Public administration & defence	10	3	30%
85: Education	10	5	50%
86-88: Health	10	19	190%
Other*	10	18	180%
Total	**100**	**67**	**67%**

**incl. 01-03 : Agriculture, forestry & fishing, 55-56 : Accommodation & food services, 64-66 : Finance & insurance, 68 : Property, 77-82 : Business administration & support services and 90-99 : Arts, entertainment, recreation & other services*

Table 7.8: Profile of interviewees' organisations by special interest group

Special interest group	Target	Achieved	%
Large business with complex and interconnected supply chain	20	19	95%
MSPs	5	6	120%
LAs/non-profits providing important or public services	30	35	117%

Interviewers recorded interviews to facilitate accurate recall, interview notes were written up and peer reviewed to maintain consistency across interviewers.

7.9 Stage 9: Qualitative interview analysis

Responses to the qualitative interviews were coded using NVivo software to identify themes, patterns and relationships in the responses. The frequency of the qualitative responses is described using the following scale:

- 'None' or 'no interviewees' = 0/67 interviewees (or 0%)
- 'A minority interviewees' = 1-16 interviewees (or 1-24%)
- 'Some interviewees' = 17-33 interviewees (or 25-49%)
- 'Most interviewees' = 34-49 interviewees (or 51-74%)
- 'The vast majority of interviewees' = 50-66 interviewees (or 75-99%)
- 'All interviewees' = 67 interviews (or 100%)

7.10 Stage 10: Development of case studies

Following submission of the final report and based on the findings of the literature review and primary research, we will develop 5-10 short case studies describing a range of organisations' experiences in relation to the GDPR and its impact on their cyber security outcomes.

7.11 Stage 11: Reporting

This stage triangulated the evidence from the Stages 1-9. This report presents our conclusions against the research questions.

8 APPENDIX B: PROFILE OF RESPONSES

8.1 Introduction

We received a total of 1,233 responses to the quantitative survey, which is equivalent to 105% of the target of 1,170 responses. This was achieved using a combination of CATI (1,005 responses) and CAWI approaches (1,005 responses were achieved via CATI and 228 via CAWI). It included 104 completed Board questionnaires (8% of total responses: 81 via CATI; and 23 via CAWI) and 1,129 staff questionnaires (92% of total responses: 924 via CATI; and 205 via CAWI).

The remainder of this appendix provides a profile of the key characteristic of the responses received. It is structured under the following headings:

- respondents - profile of the key characteristics of the individual respondents
- organisations - profile of the key characteristics of the respondents' organisations
- experience - profile of respondents' experience of cyber security incidents
- limitations

8.2 Respondents

A third of respondents to the staff survey were IT/cyber professionals (378 respondents).

The vast majority of respondents to both surveys (95%) had heard of the GDPR before taking part in the survey, however it is concerning that 5% of respondents had not heard of the regulation. Organisations that processed personal data, experienced a cyber security incident or completed a DPIA were more likely to have heard about the GDPR (97% of organisations that processed personal data, compared to 90% of those that did not; 98% of organisations that had experienced an incident, compared to 95% of all respondents; and 98% of organisations that had completed a DPIA), compared to the average respondent. There was no statistically significant variation in response by IT or cyber security professionals.

Respondents in the education, public administration and defence, and health industries were also more likely state they had heard of the GDPR (100% of education, 99% of public administration and defence and 99% of health industry respondents). Moreover, respondents in LAs/non-profits providing important public services and large businesses were more likely to have heard of the GDPR than SMEs (100% of LAs/non-profits providing important public services and 99% of respondents in and large businesses compared to 94% in SMEs).

8.3 Organisations

Table 8.1: Responses by special interest group – all respondents compared to total population

	Total population (2019)	Source	Target sample size	No. of responses received	% of target	Margin of error
Large businesses	7,595	ONS Table 12	342	206	60%	7%
Large businesses with complex and interconnected supply chains	2,500*	ONS Tables 3&4	203	99	49%	10%
MSP	1,500*	Cloud-tango	50	110	220%	9%
LAs/non-profits providing important public services not in scope of the NIS Regulations	28,740[116]	ONS Table 12	315	314	100%	6%
SMEs	2,405,905	ONS Table 12	748	537	72%	4%

Source: ONS, UK Business: Activity, Size and Location – 2019; BMG/RSM- Impact of the GDPR quantitative survey; Survey Monkey- Margin of Error Calculator (https://www.surveymonkey.com/mp/margin-of-error-calculator/); Cloud-tango (https://www.cloudtango.org/MSPs/UK/map)
*Note: * denotes an estimated figure in lieu of published data*

Table 8.2: Size of organisation – all respondents compared to total population

	Total population (2019)	No. of responses received	Margin of error
Large organisations (250 employees or more)	10,480	655	4%
Medium-sized organisations (50-249 employees)	42,000	292	6%
Small organisations (0-49 employees)	2,665,955	286	6%
Total	**2,718,435**	**1,233**	3%

Source: ONS, UK Business: Activity, Size and Location – 2019; BMG/RSM- Impact of the GDPR quantitative survey; Survey Monkey- Margin of Error Calculator (https://www.surveymonkey.com/mp/margin-of-error-calculator/)

[115] *to 95% confidence level*

[116] *8,660 LAs, 19,950 non-profits in the health industry (Source ONS, Table 12 - Number of VAT and/or PAYE based enterprises by legal status, broad industry group and employment sizebands) and 130 universities*
[117] *To 95% confidence level*

Table 8.3: Type of organisation– all respondents compared to total population

	Total population (2019)	No. of responses received	Margin of error
Private sector	2,617,435	747	4%
LA	8,660	155	8%
Non-profit	88,240	325	5%
Total	**2,714,335**	**1,233**[119]	**3%**

Source: ONS, UK Business: Activity, Size and Location – 2019, Table 12; BMG/RSM- Impact of the GDPR quantitative survey; Survey Monkey- Margin of Error Calculator (https://www.surveymonkey.com/mp/margin-of-error-calculator/)

Table 8.4: Organisation industry – all respondents compared to total population

	Total pop. (2019)		Response		Margin of error
	n	%	n	%	
01-03: Agriculture, forestry & fishing	149,540	6%	32	3%	17%
05-39: Production	152,015	6%	78	6%	11%
41-43: Construction	343,715	13%	81	7%	11%
45-47: Wholesale and retail; repair of motor vehicles	389,105	14%	88	7%	10%
49-53: Transport & Storage (incl. postal)	111,360	4%	61	5%	13%
55-56: Accommodation & food services	157,040	6%	28	2%	19%
58-63: Information & communication	226,215	8%	152	12%	8%
64-66: Finance & insurance	60,630	2%	55	4%	13%
68: Property	100,340	4%	39	3%	16%
69-75: Professional, scientific & technical	471,715	17%	91	7%	10%
77-82: Business administration & support services	228,745	8%	57	5%	13%
84: Public administration & defence	7,505	0%	129	10%	9%
85: Education	44,490	2%	110	9%	9%
86-88: Health	102,000	4%	172	14%	7%
90-99: Arts, entertainment, recreation & other services	174,020	6%	60	5%	13%
Total	**2,718,435**	**100%**	**1,233**	**100%**	**3%**

Source: ONS, UK Business: Activity, Size and Location – 2019; BMG/RSM- Impact of the GDPR quantitative survey

The total number of responses achieved (1,233) was above target (1,170), resulting in a margin of error of +/-3% at the 95% confidence level. This means that we can be confident that the responses received are representative of the views of the wider population of organisations in the UK. We also

[118] *To 95% confidence level*
[119] *It was not possible to code 6 responses*
[120] *To 95% confidence level*

received sufficient responses from respondents with certain characteristics to allow us to generalise these findings, including:

- **private sector organisations** - we can be confident that the responses received are representative of the views of the wider population of UK businesses (to +/-4% margin of error at the 95% confidence level)
- **SMEs** - we can be confident that the responses received are representative of the views of the wider population of SMEs in the UK (to +/-4% margin of error at the 95% confidence level)

8.4 Limitations

In some instances, however, the number of responses received from respondents with certain characteristics was below target, resulting in a higher margin of error. These included:

- large businesses (+/-7% margin of error at the 95% confidence level)
- large businesses with complex and interconnected supply chains (+/-10% margin of error at the 95% confidence level based on an estimated population of 2,500)
- MSP (+/-9% margin of error at the 95% confidence level based on an estimated population of 1,500)
- LAs/non-profits providing important public services not in scope of the NIS Regulations (+/-6% margin of error at the 95% confidence level)

Due to the size of the sample it was not possible to achieve responses by industry sector that would be representative of the views of the wider population by industry[121].

This means that survey findings for large businesses, large businesses with complex and interconnected supply chains, MSPs, LAs/non-profits providing important public services and by industry are indicative and should not be generalised to represent the wider population.

8.5 Experience of cyber incident

The vast majority of respondents, including staff and Board members (84%) had not experienced a cyber security incident which had caused disruption to day to day business operations or service provision in the last 3 years. Staff members were more likely to answer yes to this question than Board members (15% of staff compared to 8% of Board members).

Organisations that processed personal data or had completed a DPIA were more likely to have experienced a cyber security incident those that did not process personal data or complete a DPIA (16% of organisations that processed personal data, compared to 9% of organisations that had not, and 17% of organisations that had completed a DPIA, compared to 11% of organisations that had not).

Where a respondent was an IT or cyber security professional, they were much more likely to have experienced a cyber security incident (32% of IT or cyber security professionals, compared to 10% of non-IT or cyber security professionals).

[121] *The margins of error by industry ranged from +/- 7% margin of error in the health industry to +/- 19% margin of error in the accommodation and food services industry at the 95% confidence level*

Organisations in the production industry and information and communication industry were more likely to have experienced a cyber security incident compared to those in the public administration and defence industry (29% of organisations in the production industry and 23% in the information and communication industry answered yes compared to 6% of those in public administration and defence industry).

Large businesses with complex and interconnected supply chains (55%), large businesses (33%) MSPs (30%) and LAs/non-profits providing important public services (21%) were more likely to have experienced an incident than SMEs (15%).

9 APPENDIX C: STAKEHOLDER TOPIC GUIDE

1. In general, do you think that the introduction of GDPR[122] has caused your members to increase their investment in cyber security?
   Probe in relation to:

   Number of staff specialising in data protection (e.g. Head of compliance, Chief Data Officer, Data Protection Officer etc)

   Number of staff specialising in cyber security and information security (e.g. Information Officer, Security Architects, Engineers etc)

   Cyber security training for all staff (e.g. Securely managing personal data, Safe use of technology, Individual responsibility and accountability etc)

   Specialist training for staff involved in cyber security, information security or data protection (e.g. Identifying cyber breaches, Protecting information systems, Responding to cyber breaches, Recovering from cyber breaches etc)

   Cyber security resources (e.g. anti-virus software, antihacking software, encryption)

   Professional cyber security advice
2. In general, has the introduction of GDPR caused your members to prioritise cyber security?
   Probe in relation to:

   Policies, processes and procedures and technical controls generally and specifically in relation to data protection

   ISO certification

   Use of banks and/or merchant services that offer protection measures
3. As a result of the introduction of GDPR do more of your members:
   a. Have established data protection and information security policies, processes and procedures?
   b. Have a Data Protection Officer?
   c. Carry out regular assessments of personal data held by their organisation and the systems that process it to identify and understand security risks?
   d. Catalogue personal data?
   e. Have clear justification for collecting personal data?
4. Reflecting on your previous answers:
   a. Do you think that the introduction of GDPR has caused more of your members to prioritise and invest in improvements to cyber security?

[122] *Regulation introduced in April 2016 and enforceable in UK since May 2018*

b. Has the impact been felt across all aspects of cyber security (as opposed to data protection)?

c. Have the changes been sustained?

5. Has the GDPR led to any perverse behaviours (e.g. focus on one aspect of cyber security to the detriment of others)?
6. Are there any noticeable differences in the way that different types of organisations have responded to the GDPR (e.g. by size, type of ownership, sector etc)?
7. Are there any other factors that could have contributed to the above changes in cyber security (e.g. other policies, regulation, internal or external factors)?

   If so:

   - What are these factors?
   - To what extent are these changes a result of the introduction of GDPR as opposed to other factors?
     Probes:

     To little or no extent (i.e. 0-20% of changes due to introduction of GDPR)

     To a small extent (21-40% of changes due to introduction of GDPR)

     To some extent (41-60% of changes due to introduction of GDPR)

     To a great extent (61-80% of changes due to introduction of GDPR)

     To a very great extent (81-100% of changes due to introduction of GDPR)
8. Is there anything else you would like to add in relation to this research, the GDPR or the UK's cyber and regularity landscape?
9. Are you willing to promote the telephone survey to your members?

   If Yes, please provide contact details for the person within your organisation who will be responsible for distributing this information:

   Name:

   Role:

   Email:

   Tel:
10. Has your organisation undertaken any research into the impact of GDPR on cyber security or are you aware of any other research in this area, which could be included in our literature review?

    If Yes, ask for details/copies/hyperlinks
11. Are you willing to be contacted again by a member of the RSM research team in relation to this research?

    If Yes, note preferred contact details

    Name:

    Role:

    Email:

    Tel:

Thank interviewee and close

10 APPENDIX D: STAFF SURVEY CATI QUESTIONNAIRE

DCMS: Research on the impact of GDPR on cyber security outcomes

Introduction

Name of organisation [CONFIRM]:

Good morning/afternoon, My name is _____ and I'm calling on behalf of the Department for Digital, Culture, Media and Sport (DCMS) from BMG Research (BMG) to obtain feedback on the impact of the introduction of General Data Protection Regulation (GDPR) on organisations' and their day to day operations. The Department wants to understand the additional steps and processes organisations have to take to manage data (whether digital or not) as a result of the introduction of GDPR and how it may have impacted, if at all, on IT systems and practices.

Can I please speak to the person there best suited to provide some feedback on this?

IF NECESSARY: GDPR was announced by the Council of the EU and the European Parliament in April 2016 and became enforceable in May 2018. It aims to give people control of their personal data and create a standard for data protection in the European Union (EU). GDPR legislation applies to all organisations that process the personal data of an EU resident. Personal data refers to any information that relates to an individual person who can be directly or indirectly identified by reference to an identifier. This includes: name, identification number, location data, etc. GDPR also covers sensitive personal data which uniquely identifies an individual, e.g. genetic and biometric data.

IF QUESTION WHETHER IT IS RELEVANT TO THEM:

IF NECESSARY: All organisations hold data on their employers, customers or even suppliers and GDPR governs how this data is managed, whether it is held digitally or in hard copy.

IF NECESSARY: If your organisation uses a third party business or consultancy to manage your IT and data storage the Department would still like to hear about the direct impact of GDPR within your organisation.

We would greatly appreciate your participation in this assessment in order that your views can be represented alongside those of a range of organisations of various sizes and within private sectors. The interview will take approximately 20 minutes to complete.

You can find out more about this survey in our Privacy Notice. INTERVIEWER ESTABLISH IF WEBSITE ADDRESS WANTED OVER PHONE OR VIA EMAIL www.bmgresearch.co.uk/ GDPR survey

RECORD EMAIL SENT YES/NO

Please note that this call may be monitored or recorded for training purposes.

INTERVIEWER CHECK – Are you happy to continue?

IF NO REQUEST ANOTHER CONVENIENT TIME OR THANK AND CLOSE

IF YES CONTINUE

If you have any queries in relation to this research please feel free to contact the project manager at BMG [contact name and email].

Quota variables

Type of organisation: [Database]

1 Private business
2 Non-profit Body or Mutual Association
3 Local Authority (LA)

Private sector: [Database]

01-03 : Agriculture, forestry & fishing
05-39 : Production (incl. energy and excl. manufacturing 10-32)
10-32: All Manufacture excl Pharm (see below)
21 : Manufacture of basic pharmaceutical products and pharmaceutical preparations
41-43 : Construction
45 : Motor trades
46 : Wholesale
47: Retail
49-53 : Transport & Storage (incl. air transport)
55-56 : Accommodation & food services
58-63 : Information & communication excl MSP (see below)
6209 : Other information technology and computer service activities - specifically MSPs
6311 : Data processing; hosting and related activities - specifically MSPs
64-66 : Finance & insurance
68 : Property
69 : Legal and accounting activities
70-75 : Professional, scientific & technical excl. 7022 (see below)
7022 : Business and other management consultancy activities
77-82 : Business administration & support services
84 : Public administration & defence
85 : Education excl. 8542: Tertiary education (see below)
8542 : Tertiary education (target 20/130 universities
86-88 : Health excl. 87, 8810 & 8899 (see below) - specifically target 5/25 emergency service providers (e.g. air ambulances, St John's Ambulance and the British Red Cross)
87 : Residential care activities
8810 : Social work activities without accommodation for the elderly and disabled
8899 : Other social work activities without accommodation n.e.c.
90-99 : Arts, entertainment, recreation & other services

Sub group(s): [multi-code. Database and survey responses]

1 Large businesses
2 Large organisations with complex and interconnected supply chains [i.e. organisations with 250+ employees in SIC codes: 10-32: All Manufacture (incl. Pharma), 47: Retail, 49-53: Transport & Storage (incl. air transport), 69: Legal and accounting activities and 7022: Business and other management consultancy activities. These variables will be used to identify and target organisations with complex and interconnected supply chains – use Q6 - Q8 to confirm and to identify SMEs with complex and interconnected supply chains]
3 Managed service providers (MSP) [i.e. SIC codes: 6209: Other information technology and computer service activities and 6311: Data processing; hosting and related activities. These SIC codes will be used to identify and target managed service providers – use definition in footnote and Q5 to confirm they are a MSP]
4 LAs and organisations providing important/ public services, but not in scope of the NIS Regulations
5 Small and medium-sized enterprises (SMEs)

Interviewee name:

Interviewee's role:

What is your job title or job role within the organisation?

[WRITE IN AND CODE ONE ONLY – BEST FIT]

1 Chief Executive
2 Head of Compliance and Data Protection
3 Chief Data Officer
4 Data Protection Officer
5 Information Officer
6 Privacy Officer
7 Data Protection Compliance Manager
8 Information Security Architect
9 Information Security Engineer
10 **[Local Authorities only]** IT Manager
11 **[Local Authorities only]** Functional Head/ SRO (Senior Responsible Owner)/ Section 151 Officer
12 Other (please specify):_____

ASK ALL

1. Do you consider yourself an Information Technology (IT) or cyber security professional?

1 Yes
2 No

ASK ALL

2. Approximately how many Full Time Equivalent (FTE) staff are directly employed in your organisation, where 1 FTE is equal to the hours worked by 1 employee on a full-time basis?
PROMPT FOR AN APPROXIMATION

____FTEs X Don't know Y Refused

WHERE X/Y: PROMPT FOR A BANDING Would you say the number of Full Time Equivalent staff falls into one of the following size bands?

1 0-9
2 10-49
3 50-249
4 250+
5 Don't know
6 Refused

ASK ALL

3. A new data protection law called the General Data Protection Regulation, or GDPR, was announced in April 2016 and came into effect in May 2018. Had you heard of General Data Protection Regulation or GDPR before this interview?

    1 Yes
    2 No

ASK ALL

4. Which of the following types of personal data, if any, does your organisation process? **READ OUT AND CODE ALL THAT APPLY**

    1 Personal data about consumers/ service users
    2 Personal data about a business or organisation
    3 N/a – we do not process personal data of any sort
    4 Don't know

ASK ALL

5. Does your organisation **build or operate** any of the following services for **multiple** customers or clients? **READ OUT AND CODE ALL THAT APPLY**

    1 Outsourced Information and Communications Technology services **[EXAMPLES PROVIDED IF REQUIRED: datacentre or cloud service provision, infrastructure hosting, systems integration, software systems development, applications service provision, applications maintenance and support, end-user support/helpdesk, information security management services, managed cyber defence services, managed telecommunications services, disaster recovery services or overall service integration and management (SIAM).]**
    2 Business process outsourcing (underpinned by ICT) **[EXAMPLES PROVIDED IF REQUIRED: HR, payroll and procurement functions]**
    3 None of these
    4 Don't know
    5 Prefer not to say

ASK ALL

6. Would you consider your organisation to have complex and interconnected supply chains?

    1 Yes
    2 No
    3 Don't know

ASK ALL

7. Does your organisation have a supply chain with more than 3 tiers of suppliers?

    1 Yes
    2 No
    3 Don't know

ASK ALL

8. If one of your main suppliers was incapacitated by a cyber attack for 48 hours, what impact would this have on your day to day business operations or service provision? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY**

    1 No impact
    2 Small impact
    3 Moderate impact
    4 Severe impact
    5 Don't know

ASK ALL

9. Has your organisation experienced a cyber security incident which has caused disruption to your day to day business operations or service provision in the last 3 years?

    1 Yes
    2 No
    3 Don't know

Invest

ASK ALL

10. How many employees, in terms of FTEs, specialise in data protection within your organisation (e.g. Chief Data Officer, Head of Compliance and data protection, Data Protection Officer, Privacy Officer, Data Protection Compliance Manager etc) **PROMPT FOR AN APPROXIMATION** ***INTERVIEWER PLEASE NOTE FTE = FULL TIME EQUIVALENT***

    Now? ___FTE X Don't know Y Refused

WHERE Q10/1+

11. [Q10/2+: How many of these roles have been **Q10/1**: Was this role] created in the last 3 years since GDPR was announced in April 2016? **PROMPT FOR AN APPROXIMATION**

    Q10/2+: ___FTE **Q10/1:** 1 Yes 2 No

    X Don't know Y Refused

ASK ALL

12. There are many different factors that influence changes in cyber security (e.g. perceived, heightened external threat of cyber attacks, awareness of the cost of potential breaches and their impact, advice and guidance etc). To what extent has the amount of staff time currently devoted to data protection been influenced by the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

13. Excluding those who specialise in data protection, how many FTE employees specialise in cyber security or information security (e.g. Information Officer, Security Architect, Engineer, Analysts etc) **PROMPT FOR AN APPROXIMATION**

Now? ___FTE X Don't know Y Refused

WHERE Q13/1+

14. [Q13/2+: How many of these roles have been Q13/1: Was this role] created in the last 3 years?

___FTE X Don't know Y Refused

ASK ALL

15. To what extent has the amount of staff time currently devoted to cyber security and information security been influenced by the introduction of GDPR as opposed to other factors IF NECESSARY: such as those I mentioned earlier? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

ASK ALL

16. Do you provide GDPR training for <u>all staff</u> in your organisation who have access to personal data or IT systems? **NOTE: THIS INCLUDES ALL TRAINING, INCLUDING INDUCTIONS**

1 Yes
2 No
3 Don't know

Q16/1

17. Is any of this training mandatory? **–NOTE: GDPR TRAINING IN INDUCTIONS COUNTS AS MANDATORY IF THE INDUCTION IS MANDATORY AND NOT IF IT ISN'T PROBE AS NECESSARY AND CODE ONE ONLY**

1 Yes
2 Some (i.e. We provide both mandatory and optional GDPR training)
3 No
4 Don't know

Q16/1

18. Does this training include elements of cyber security (i.e. password protection, access control, patching, avoiding phishing etc.)?

1 Yes
2 No
3 Don't know

ASK ALL

19. Excluding other types of training that cover elements of cyber security only, do any staff within your organisation receive specific cyber security training (i.e. password protection, access control, patching, avoiding phishing etc.)?

1 Yes
2 No
3 Don't know

Q19/1

20. Has this training been introduced or improved in the last 3 years?

1 Yes
2 No
3 Don't know

Q20/1

21. To what extent are these changes in the specific cyber security training offered in your organisation a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

ASK ALL

22. Has your organisation's expenditure on the following cyber security resources increased, decreased or stayed the same in the last 3 years? **READ OUT AND CODE ONE FOR EACH**

Resource	Increased	Decreased	Stayed the same	Don't know
a) cyber security software	□	□	□	□
b) cyber security hardware	□	□	□	□
c) outsourcing/consultancy	□	□	□	□
d) recruitment	□	□	□	□

Q22a-e/ANY INCREASED/DECREASED

23. To what extent are these changes in other cyber security resources a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

Prioritise

ASK ALL

24. Are the following aspects of cyber security a high, medium or low priority for your organisation.

    A. now
    B. and were they a high, medium or low priority 3 years ago?

    READ OUT AND CODE ONE FOR EACH. PROMPT WITH QUESTION AND CODES AS REQUIRED

	Now				3 years ago			
Aspect	**H**	**M**	**L**	**DK**	**H**	**M**	**L**	**DK**
a) data protection policies, processes and procedures	□	□	□	□	□	□	□	□
b) other information/ cyber security policies, processes and procedures	□	□	□	□	□	□	□	□
c) technical controls for data protection	□	□	□	□	□	□	□	□
d) technical controls for other aspects of information/ cyber security	□	□	□	□	□	□	□	□

[If responses to Q24 indicate a change in priority across any row, go to 25, otherwise go to 26]

WHERE DIFFERENT RESPONSES BETWEEN Q24A/a-e AND Q24B/a-e

25. To what extent are these changes in your cyber security priorities a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

Act

ASK ALL

26. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years? **READ OUT AND CODE ONE FOR EACH MULTI-CODE ALLOWED FOR INTRODUCED/IMPROVED ONLY**

FOR ALL:

Element	Introduced	Improved	Stayed the same	Don't know
a) data protection policies	□	□	□	□
b) information security policies	□	□	□	□
c) risk management	□	□	□	□
d) asset management	□	□	□	□
e) procurement or supply chain risk management	□	□	□	□
f) Cyber Essentials/ Cyber Essentials Plus certification	□	□	□	□
g) ISO certification	□	□	□	□
h) identity and access controls	□	□	□	□
i) technical controls	□	□	□	□
j) incident management or recovery processes	□	□	□	□
k) monitoring and review, including audit processes	□	□	□	□

Q1/1 ADDITIONAL RESPONSE OPTIONS (TECHNICAL)

Element		Introduced	Improved	Stayed the same	Don't know
l)	Tracking and recording of all assets that process personal data	□	□	□	□
m)	Minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity	□	□	□	□
n)	Actively managing software vulnerabilities, including patching	□	□	□	□
o)	Managing end user devices	□	□	□	□
p)	Encrypting personal data	□	□	□	□
q)	Ensuring that web services are protected from common security vulnerabilities	□	□	□	□
r)	Ensuring your processing environment remains secure throughout its lifecycle.	□	□	□	□
s)	Undertaking regular testing to evaluate the effectiveness of your security measures (e.g. penetration testing, virus and malware scanning)	□	□	□	□

WHERE Q26/ANY INTRODUCED OR IMPROVED

27. To what extent are these changes in your cyber security a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

WHERE Q26/ANY STAYED THE SAME

28. Considering those elements of cyber security that have not been introduced or improved in the last 3 years, what is the main reason you have not taken action in these areas? **PROBE AND CODE ONE ONLY**

1 What we had in place was already sufficient
2 It is not a priority for our organisation
3 We do not have enough resource to devote to it
4 We do not have enough knowledge or understanding to make changes in these areas
95 Other specify
96 Don't know

ASK ALL

29. Has your organisation done one or more Data Protection Impact Assessments (or DPIA) (as required by GDPR where data processing is likely to result in a high risk to personal data)?

    1 Yes
    2 No
    3 Don't know

Q29/1

30. Have you made any changes to your cyber security arrangements as a result of doing a DPIA?

    1 Yes
    2 No
    3 Don't know

Q30/1

31. What type of changes have you made as a result of doing a DPIA?

    _____

    X Don't know Y Prefer not to say

Q30/2

32. What is the main reason you haven't made any changes as a result of doing a DPIA? **PROBE AND CODE ONE ONLY**

    1 What we had in place was already sufficient
    2 It is not a priority for our organisation
    3 We do not have enough resource to devote to it
    4 We do not have enough knowledge or understanding to make any changes
    95 Other specify
    96 Don't know

Summary

ASK ALL

33. Reflecting on your answers to these questions, where you have made changes to your organisation's cyber security personnel, training, resources, priorities and activities, which of the following factors, if any, have influenced these changes? **READ OUT AND CODE ALL THAT APPLY.**

    1 Introduction of GDPR
    2 Desire to comply with GDPR (and avoid penalties)
    3 Increased or greater awareness of the financial cost of potential data breaches or cyber attacks (excluding penalties)
    4 ….and/or the reputational cost of potential data breaches or cyber attacks
    5 Advice / guidance issued by ….the National Cyber Security Centre (NCSC)
    6 …. another government body
    7 …. a trade association or union
    8 … an external cyber security consultancy / service
    9 Drive for change from internal staff (e.g. from Chief Data Officer or cyber professionals)
    10 Perceived, heightened external threat of ….cyber attacks in your sector
    11 …. cyber attacks globally
    12 Response to ….business pressure, i.e. up or down the supply chain
    13 … customer pressure
    14 …pressure from your Board
    15 Other (Please specify):_____
    16 None of these/nothing/don't know

WHERE MORE THAN ONE SPECIFIED Q33/1-15

34. Which factors were most important in terms of influencing these changes? USE LIST OF RESPONSES FROM Q33 TO REMIND RESPONDENT OF CHOICES **CODE UP TO 3**

    1.
    2.
    3.
    X all as important/unable to choose

ASK ALL

35. To what extent are all of the changes in your organisation's cyber security in the last 3 years a result of the introduction of GDPR as opposed to the other factors noted? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

36. To what extent do you agree or disagree with the following statements: **READ OUT AND PROMPT WITH SCALE FOR EACH. CODE ONE ONLY FOR EACH**

a) 'The impact of GDPR has been felt across all cyber security related areas within our organisation (e.g. preventing disruption of services, protecting valuable data), not just within specific areas (e.g. data protection'

1 Strongly agree
2 Agree
3 Disagree
4 Strongly disagree
5 Don't know/unsure

b) 'The changes that our organisation has implemented due to GDPR have been sustained.'

1 Strongly agree
2 Agree
3 Disagree
4 Strongly disagree
5 Don't know/unsure

ASK ALL

37. To what extent do you agree or disagree that GDPR has led to the following consequences in your organisation? **READ OUT AND CODE ONE ONLY FOR EACH. PROMPT WITH SCALE AS NECESSARY**

Consequence	Strongly agree	Agree	Disagree	Strongly disagree	Don't know/unsure	Not applicable
a) Excessive focus on data protection to the detriment of other aspects of cyber security	□	□	□	□	□	-
b) Excessive caution amongst staff in the handling of data	□	□	□	□	□	-
c) Excessive investment in cyber security, significantly beyond what is necessary	□	□	□	□	□	-
d) Other consequences for the cyber security of your organisation*	□	□	□	□	□	□

*What were these other consequences? WRITE IN _____

ASK ALL

38. Finally, is there anything else you would like to add in relation to the impact of GDPR on cyber security? **LISTEN. PROBE AND WRITE IN VERBATIM**

X Nothing

ASK ALL

39. DCMS is undertaking follow up interviews with selected organisations*. They will take 30-50 minutes and will be carried out by RSM** between February and March (2020). As a thank you, those who take part in an additional interview, will be given a £50 voucher or charity donation. Would you be willing to take part in a follow-up interview and have your contact details passed to RSM for this purpose?

1 Yes
2 No

IF ASKED:

* The purpose of the follow up interviews will be to better understand the findings from this survey. For example, to find out why certain organisations have reacted to GDPR in a particular way and any variation in the impact of GDPR by size of organisation or sector

**RSM is an independent research company who has been commissioned by DCMS to undertake this research into the impact of GDPR, along with BMG.

WHERE YES, RECORD CONTACT DETAILS BELOW, OTHERWISE THANK AND CLOSE

Contact details for follow up interview

Email: _____

Is the telephone number I've called you on today the best number to call back on? Or would you prefer to be called on another number? IF ANOTHER NUMBER ASK:

What number is it best to call you on?

Tel: _____ X Number as called

Q39/1

40. For the purposes of the follow up interview are you happy for DCMS and their appointed research contractor to see your responses from this interview? This would only be to help guide the discussion and keep it relevant to your organisation and to avoid asking you any of the same questions again.

1 Yes
2 No

Thank and close:

Thank you for taking part in this survey to inform the Department's understanding of the impact that GDPR has had on cyber security outcomes to date. You can find more information and guidance on cyber security issues via the following websites:

- **National Cyber Security Centre (NCSC)- https://www.ncsc.gov.uk/**
- **Information Commissioner's Office (ICO) - https://ico.org.uk/**

11 APPENDIX E: BOARD SURVEY CATI QUESTIONNAIRE

DCMS: Research on the impact of GDPR on cyber security outcomes

Introduction

Name of organisation [CONFIRM]:

Good morning/afternoon, My name is _____ and I'm calling on behalf of the Department for Digital, Culture, Media and Sport (DCMS) from BMG Research (BMG) to obtain feedback on the impact of the introduction of General Data Protection Regulation (GDPR) on organisations and their day to day operations. The Department wants to understand the additional steps and processes organisations have to take to manage data (whether digital or not) as a result of the introduction of GDPR and how it may have impacted, if at all, on IT systems and practices.

Can I please speak to a member of the Board – someone who is able to provide feedback on this at a very senior level within the organisation?

IF NECESSARY: GDPR was announced by the Council of the EU and the European Parliament in April 2016 and became enforceable in May 2018. It aims to give people control of their personal data and create a standard for data protection in the European Union (EU). GDPR legislation applies to all organisations that process the personal data of an EU resident. Personal data refers to any information that relates to an individual person who can be directly or indirectly identified by reference to an identifier. This includes: name, identification number, location data, etc. GDPR also covers sensitive personal data which uniquely identifies an individual, e.g. genetic and biometric data.

IF QUESTION WHETHER IT IS RELEVANT TO THEM:

IF NECESSARY: All organisations hold data on their employers, customers or even suppliers and GDPR governs how this data is managed, whether it is held digitally or in hard copy.

IF NECESSARY: If your organisation uses a third party business or consultancy to manage your IT and data storage the Department would still like to hear about the direct impact of GDPR within your organisation.

We would greatly appreciate your participation in this assessment in order that your views can be represented alongside those of a range of organisations of various sizes and within private sectors. The interview will take approximately 20 minutes to complete.

You can find out more about this survey in our Privacy Notice. INTERVIEWER ESTABLISH IF WEBSITE ADDRESS WANTED OVER PHONE OR VIA EMAIL
www.bmgresearch.co.uk/privacy/GDPRsurvey

RECORD EMAIL SENT YES/NO

Please note that this call may be monitored or recorded for training purposes.

INTERVIEWER CHECK – Are you happy to continue?

IF NO REQUEST ANOTHER CONVENIENT TIME OR THANK AND CLOSE

IF YES CONTINUE

If you have any queries in relation to this research please feel free to contact the project manager at BMG [contact name and email].

Quota variables

Type of organisation: [Database]

1 Private business
2 Non-profit Body or Mutual Association
3 Local Authority (LA)

Private sector: [Database]

01-03 : Agriculture, forestry & fishing
05-39 : Production (incl. energy and excl.manufacturing 10-32)
10-32: All Manufacture excl Pharm (see below)
21 : Manufacture of basic pharmaceutical products and pharmaceutical preparations
41-43 : Construction
45 : Motor trades
46 : Wholesale
47: Retail
49-53 : Transport & Storage (incl. air transport)
55-56 : Accommodation & food services
58-63 : Information & communication excl MSP (see below)
6209 : Other information technology and computer service activities - specifically MSPs
6311 : Data processing; hosting and related activities - specifically MSPs
64-66 : Finance & insurance
68 : Property
69 : Legal and accounting activities
70-75 : Professional, scientific & technical excl. 7022 (see below)
7022 : Business and other management consultancy activities
77-82 : Business administration & support services
84 : Public administration & defence
85 : Education excl. 8542: Tertiary education (see below)
8542 : Tertiary education (target 20/130 universities
86-88 : Health excl. 87, 8810 & 8899 (see below) - specifically target 5/25 emergency service providers (e.g. air ambulances, St John's Ambulance and the British Red Cross)
87 : Residential care activities
8810 : Social work activities without accommodation for the elderly and disabled
8899 : Other social work activities without accommodation n.e.c.
90-99 : Arts, entertainment, recreation & other services

Sub group(s): [multi-code. Database and survey responses]

1 Large businesses
2 Large organisations with complex and interconnected supply chains [i.e. organisations with 250+ employees in SIC codes: 10-32: All Manufacture (incl. Pharma), 47: Retail, 49-53: Transport & Storage (incl. air transport), 69: Legal and accounting activities and 7022: Business and other management consultancy activities. These variables will be used to identify and target organisations with complex and interconnected supply chains – use Q4 – Q6 to confirm and to identify SMEs with complex and interconnected supply chains]
3 Managed service providers (MSP) [i.e. SIC codes: 6209: Other information technology and computer service activities and 6311: Data processing; hosting and related activities. These SIC codes will be used to identify and target managed service providers – use definition in footnote and Q3 to confirm they are a MSP]
4 LAs and organisations providing important/ public services, but not in scope of the NIS Regulations
5 Small and medium-sized enterprises (SMEs)

Interviewee name:

Interviewee's role:

What is your job title or job role within the organisation?

[WRITE IN AND CODE ONE ONLY – BEST FIT]

1 Chair of Audit Committee/ Risk Committee
2 Chair of the Board of Directors (Non-Executive/ Independent members only)
3 Deputy/ Vice Chair of the Board of Directors (Non-Executive/ Independent members only)
4 Chief Executive Officer
5 Chief Finance Officer
6 Non-Executive Director
7 **[Local Authorities only]** Councillor
8 Other (please specify):_____

ASK ALL

1. A new data protection law called the General Data Protection Regulation, or GDPR, was announced in April 2016 and came into effect in May 2018. Had you heard of General Data Protection Regulation or GDPR before this interview?

    1 Yes
    2 No

ASK ALL

2. Which of the following types of personal data, if any, does your organisation process? **READ OUT AND CODE ALL THAT APPLY**

    1 Personal data about consumers/ service users
    2 Personal data about a business or organisation
    3 N/a – we do not process personal data of any sort
    4 Don't know

ASK ALL

3. Does your organisation **build or operate** any of the following services for **multiple** customers or clients? **READ OUT AND CODE ALL THAT APPLY**

    1 Outsourced Information and Communications Technology services **[EXAMPLES PROVIDED IF REQUIRED: datacentre or cloud service provision, infrastructure hosting, systems integration, software systems development, applications service provision, applications maintenance and support, end-user support/helpdesk, information security management services, managed cyber defence services, managed telecommunications services, disaster recovery services or overall service integration and management (SIAM).]**
    2 Business process outsourcing (underpinned by ICT) **[EXAMPLES PROVIDED IF REQUIRED: HR, payroll and procurement functions]**
    3 None of these
    4 Don't know
    5 Prefer not to say

ASK ALL

4. Would you consider your organisation to have complex and interconnected supply chains?

    1 Yes
    2 No

ASK ALL

5. Does your organisation have a supply chain with more than 3 tiers of suppliers?

    1 Yes
    2 No

ASK ALL

6. If one of your main suppliers was incapacitated by a cyber attack for 48 hours, what impact would this have on your day to day business operations or service provision? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY**

    1 No impact
    2 Small impact
    3 Moderate impact
    4 Severe impact
    5 Don't know

ASK ALL

7. Has your organisation experienced a cyber security incident which has caused disruption to your day to day business operations or service provision in the last 3 years?

    1 Yes
    2 No
    3 Don't know

Invest

ASK ALL

8. Has your organisation's investment in the following areas increased, decreased or stayed the same in the last 3 years since GDPR was announced in April 2016? **READ OUT AND CODE ONE FOR EACH**

Resource	Increased	Decreased	Stayed the same	Don't know
a) Staff time devoted to data protection (e.g. including roles such as Chief Data Officer, Head of Compliance and data protection, Data Protection Officer, Privacy Officer, Data Protection Compliance Manager etc)	☐	☐	☐	☐
b) Staff time devoted to other aspects of cyber security or information security (e.g. Information Officer, Security Architect, Engineer, Analysts etc)	☐	☐	☐	☐
c) Amount of cyber security training provided	☐	☐	☐	☐
d) Range of cyber security training provided	☐	☐	☐	☐
e) Spend on other cyber security resources (e.g. cyber security software and hardware, awareness raising, outsourcing/consultancy, recruitment)	☐	☐	☐	☐

Q8a-f/ANY INCREASED/DECREASED

9. There are many different factors that influence changes in investment in cyber security (e.g. perceived, heightened external threat of cyber attacks, awareness of the cost of potential breaches and their impact, advice and guidance etc). To what extent are these changes in your investment in cyber security a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

Prioritise

ASK ALL

10. Has the Board approved a cyber security strategy for your organisation? **PROMPT FOR CODES 1 OR 2 CODE ONE ONLY**

    1 Yes, we have a dedicated cyber security strategy
    2 Yes, we have a cyber security strategy as part of our IT strategy
    3 No, we do not have a formal cyber security strategy

WHERE Q10/1, 2

11. Is it…? **READ OUT AND CODE ALL THAT APPLY**

    1 Risk based?
    2 Aligned with business objectives?
    3 Supported by a dedicated budget?
    4 Don't know

WHERE Q10/1, 2

12. To what extent has your cyber security strategy been influenced by the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

13. Has the Board of Director's awareness of cyber security increased, decreased or stayed the same in the last 3 years (since the introduction of GDPR)? **CODE ONE ONLY**

    1 Increased
    2 Stayed the same
    3 Decreased
    4 Don't know

WHERE Q13/1, 3 (INCREASED/DECREASED)

14. To what extent is this change a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

ASK ALL

15. Are you aware of the National Cyber Security Centre (NCSC) Board Toolkit?

1 Yes
2 No

WHERE Q15/1

16. Has your organisation used it?

1 Yes
2 Not yet but plan to in the future
3 No
4 Don't know

WHERE Q16/3

17. Why not? **PROBE FULLY AND WRITE IN VERBATIM**

X Don't know Y Prefer not to say

ASK ALL

18. How often does the Board receive reported updates on cyber security? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY**

1 Weekly
2 Monthly
3 Quarterly
4 Annually
5 Not at all
6 Done on an ad hoc basis
7 Other (Please specify):_____

ASK ALL

19. Has the frequency of these of cyber security updates increased, decreased or stayed the same in the last 3 years?

1 Increased
2 Stayed the same
3 Decreased
4 Don't know

WHERE Q19/1,3

20. To what extent are these changes in frequency a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

ASK ALL

21. To what extent do you agree with the following statements about updates on your organisation's cyber security (e.g. the information reported to the Board by those responsible for cyber security in your organisation about the risk relating to the confidentiality, integrity and availability of data, assets and systems)? **READ OUT AND CODE ONE ONLY FOR EACH**

Statement	Strongly agree	Agree	Disagree	Strongly disagree	Don't know
a) It is more comprehensive than it was 3 years ago (i.e. covers people, processes and technology)	□	□	□	□	□
b) It is more robust than it was 3 years ago (i.e. reliable, accurate, high quality and stands up to scrutiny)	□	□	□	□	□
c) It is more responsive to external changes than it was 3 years ago	□	□	□	□	□
d) It is more focused on data protection, rather than general cyber security, than it was 3 years ago	□	□	□	□	□

WHERE STRONGLY AGREE/AGREE (1, 2) IN ANY Q21a-d

22. To what extent are these changes a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

ASK ALL

23. In the last 3 years, has the Board increased, decreased or given the same prioritisation to the following aspects of cyber security: **READ OUT AND CODE ONE ONLY FOR EACH ROW**

Aspect	Increased	Decreased	Stayed the same	Don't know
a) Embedding cyber security into your structure and organisation's objectives	□	□	□	□
b) Growing in-house cyber security expertise	□	□	□	□
c) Developing a positive cyber security culture	□	□	□	□
d) Establishing your risk profile baseline and identifying what you care about most	□	□	□	□
e) Understanding your cyber security threat	□	□	□	□
f) Risk management	□	□	□	□
g) Implementing effective technical cyber security measures	□	□	□	□
h) Working with suppliers and partners to manage supply chain risks	□	□	□	□
i) Planning your response to cyber incidents	□	□	□	□

WHERE INCREASED/DECREASED (1, 2) IN ANY Q23a-j

24. To what extent are these changes in your cyber security priorities a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

Act

ASK ALL

25. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years? **READ OUT AND CODE FOR EACH. MULTI-CODE ALLOWED FOR INTRODUCED/IMPROVED ONLY**

Element	Introduced	Improved	Stayed the same	Don't know
a) data protection policies	□	□	□	□
b) information security policies	□	□	□	□
c) risk management	□	□	□	□
d) asset management	□	□	□	□
e) procurement or supply chain risk management	□	□	□	□
f) Cyber Essentials/ Cyber Essentials Plus certification	□	□	□	□
g) ISO certification	□	□	□	□
h) identity and access controls	□	□	□	□
i) technical controls	□	□	□	□
j) incident management or recovery processes	□	□	□	□
k) monitoring and review, including audit processes	□	□	□	□

WHERE Q25/ANY INTRODUCED OR IMPROVED

26. To what extent are these changes a result of the introduction of GDPR as opposed to other factors? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

WHERE Q25/ANY STAYED THE SAME

27. Considering those elements of cyber security that have not been introduced or improved in the last 3 years, what is the main reason you have not taken action in these areas? **PROBE AND CODE ONE ONLY**

1 What we had in place was already sufficient
2 It is not a priority for our organisation
3 We do not have enough resource to devote to it
4 We do not have enough knowledge or understanding to make changes in these areas
95 Other specify
96 Don't know

Summary

ASK ALL

28. Reflecting on your answers to these questions, where you have made changes to your organisation's cyber security personnel, training, resources, priorities and activities, which of the following factors, if any, have influenced these changes? **READ OUT AND CODE ALL THAT APPLY.**

    1 Introduction of GDPR
    2 Desire to comply with GDPR (and avoid penalties)
    3 Increased or greater awareness of the financial cost of potential data breaches or cyber attacks (excluding penalties)
    4 …and/or the reputational cost of potential data breaches or cyber attacks
    5 Advice / guidance issued ….by the National Cyber Security Centre (NCSC)
    6 …. by another government body
    7 …. by a trade association or union
    8 … by an external cyber security consultancy / service
    9 Drive for change from internal staff (e.g. from Chief Data Officer or cyber professionals)
    10 Perceived, heightened external threat of ….cyber attacks in your sector
    11 … cyber attacks globally
    12 Response to…. business pressure, i.e. up or down the supply chain
    13 … customer pressure
    14 … pressure from staff responsible for cyber security/data protection
    15 Other (Please specify):_____
    16 None/nothing/don't know

ASK ALL

29. Which factors were most important in terms of influencing these changes? USE LIST OF RESPONSES FROM Q28 TO REMIND RESPONDENT OF CHOICES **CODE UP TO 3**

    1.
    2.
    3.
    X all as important/unable to choose

ASK ALL

30. To what extent are all of the changes in your organisation's cyber security in the last 3 years a result of the introduction of GDPR as opposed to the other factors noted? **PROBE FOR OPTIONS GIVEN AND CODE ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

31. To what extent do you agree or disagree with the following statements: **READ OUT AND PROMPT WITH SCALE FOR EACH. CODE ONE ONLY FOR EACH**

a) 'e.g. preventing disruption of services, protecting valuable data), not just within specific areas (e.g. data protection).'

1 Strongly agree
2 Agree
3 Disagree
4 Strongly disagree
5 Don't know/unsure

b) 'The changes that our organisation has implemented due to GDPR have been sustained.'

1 Strongly agree
2 Agree
3 Disagree
4 Strongly disagree
5 Don't know/unsure

ASK ALL

32. To what extent do you agree that GDPR has led to the following consequences in your organisation? **READ OUT AND CODE ONE ONLY FOR EACH. PROMPT WITH SCALE AS NECESSARY**

Consequence	Strongly agree	Agree	Disagree	Strongly disagree	Don't know	Not applicable
a) Excessive focus on data protection to the detriment of other aspects of cyber security	□	□	□	□	□	-
b) Excessive caution amongst staff in the handling of data	□	□	□	□	□	-
c) Excessive investment in cyber security, significantly beyond what is necessary	□	□	□	□	□	-
d) Other consequences for the cyber security of your organisation*	□	□	□	□	□	□

*What were these other consequences? WRITE IN _____

ASK ALL

33. Finally, is there anything else you would like to add in relation to the impact of GDPR on cyber security? **LISTEN. PROBE AND WRITE IN VERBATIM**

X Nothing

ASK ALL

34. DCMS is undertaking follow up interviews with selected organisations*. They will take 30-50 minutes and will be carried out by RSM** between February and March (2020). As a thank you, those who take part in an additional interview, will be given a £50 voucher or charity

donation. Would you be willing to take part in a follow-up interview and have your contact details passed to RSM for this purpose?

1 Yes
2 No

IF ASKED:

* The purpose of the follow up interviews will be to better understand the findings from this survey. For example, to find out why certain organisations have reacted to GDPR in a particular way and any var9iation in the impact of GDPR by size of organisation or sector

**RSM is an independent research company who has been commissioned by DCMS to undertake this research into the impact of GDPR, along with BMG.

WHERE YES, RECORD CONTACT DETAILS BELOW, OTHERWISE THANK AND CLOSE

Contact details for follow up interview

Email: _____

Is the telephone number I've called you on today the best number to call back on? Or would you prefer to be called on another number? IF ANOTHER NUMBER ASK:

What number is it best to call you on?

Tel: _____ X Number as called

Q34/1

35. For the purposes of the follow up interview are you happy for DCMS and their appointed research contractor to see your responses from this interview? This would only be to help guide the discussion and keep it relevant to your organisation and to avoid asking you any of the same questions again.

1 Yes
2 No

Thank and close:

Thank you for taking part in this survey to inform the Department's understanding of the impact that GDPR has had on cyber security outcomes to date. You can find more information and guidance on cyber security issues via the following websites:

- **National Cyber Security Centre (NCSC)- https://www.ncsc.gov.uk/**
- **Information Commissioner's Office (ICO) - https://ico.org.uk/**

12 APPENDIX F: STAFF SURVEY CAWI QUESTIONNAIRE

DCMS: Research on the impact of GDPR on cyber security outcomes

Introduction

BMG Research are conducting a survey on behalf of the Department for Digital, Culture, Media and Sport (DCMS) to obtain feedback on the impact of the introduction of General Data Protection Regulation (GDPR) on organisations' and their day to day operations. The Department wants to understand the additional steps and processes organisations have to take to manage data (whether digital or not) as a result of the introduction of GDPR and how it may have impacted, if at all, on IT systems and practices. We'd greatly appreciate your views on behalf of the organisation in which you are employed.

The survey will take around 15 minutes to complete. The deadline for completing a survey is 20th February 2020.

Before beginning the survey, please tell us which of the following best describes the level of your position at your company?

- C-Level executive (i.e. CFO, CEO)
- Board level director
- Director/Department Manager/Senior Manager
- Manager
- Non managerial *(screen out)*

Just to confirm, your responses will be treated in the strictest confidence. BMG Research abides by the Market Research Society Code of Conduct at all times.

You can find out more information about our surveys and what we do with the information we collect in our Privacy Notice which is here www.bmgresearch.co.uk/GDPRsurvey

GDPR was announced by the Council of the EU and the European Parliament in April 2016 and became enforceable in May 2018. It aims to give people control of their personal data and create a standard for data protection in the European Union (EU). GDPR legislation applies to all organisations that process the personal data of an EU resident. Personal data refers to any information that relates to an individual person who can be directly or indirectly identified by reference to an identifier. This includes: name, identification number, location data, etc. GDPR also covers sensitive personal data which uniquely identifies an individual, e.g. genetic and biometric data.

All organisations hold data on their employers, customers or even suppliers and GDPR governs how this data is managed, whether it is held digitally or in hard copy.

If your organisation uses a third party business or consultancy to manage your IT and data storage the Department would still like to hear about the direct impact of GDPR within your organisation.

Click here to begin the survey XXX

By clicking the button you agree to participate in the survey.

If you have any queries in relation to this research please feel free to contact the project manager at BMG [contact name and email].

ASK ALL

S1. How would you describe the type of organisation that you work within? Would you say it was a…. Select one only

1 Private business
2 Non-profit Body or Mutual Association
3 Local Authority (LA)
4 Something else Please tell us what type of organisation you work within:

S2. What is your job title or job role within the organisation?

Please select the most appropriate or write in if not listed

1 Chief Executive
2 Head of Compliance and Data Protection
3 Chief Data Officer
4 Data Protection Officer
5 Information Officer
6 Privacy Officer
7 Data Protection Compliance Manager
8 Information Security Architect
9 Information Security Engineer
10 **[Local Authorities only]** IT Manager
11 **[Local Authorities only]** Functional Head/ SRO (Senior Responsible Owner)/ Section 151 Officer
12 Other Please tell us what your job title is:

ASK ALL

1. Do you consider yourself an Information Technology (IT) or cyber security professional? Select one only

1 Yes
2 No

ASK ALL

2. Approximately how many Full Time Equivalent (FTE) staff are directly employed in your organisation, where 1 FTE is equal to the hours worked by 1 employee on a full-time basis? Please provide an estimate of the number of staff

____FTEs X Don't know Y Refused

WHERE X/Y: Would you say the number of Full Time Equivalent staff falls into one of the following size bands?

1 0-9
2 10-49
3 50-249
4 250+
5 Don't know
6 Refused

ASK ALL

2b. How would you describe the main activity of the organisation in which you work?

What is the main product or service of the organisation?

What exactly is made or done within the organisation?

Who does it sell its product/services or provide services to?

What would you type into a search engine to find an organisation like yours online?

Please provide detail below

ASK ALL

3. A new data protection law called the General Data Protection Regulation, or GDPR, was announced in April 2016 and came into effect in May 2018. Had you heard of General Data Protection Regulation or GDPR before now? Select one only

   1 Yes
   2 No

ASK ALL

4. A new data protection law called the General Data Protection Regulation, or GDPR, was announced in April 2016 and came into effect in May 2018. Had you heard of General Data Protection Regulation or GDPR before now? Select one only

Which of the following types of personal data, if any, does your organisation process? ***Please select all that apply***

   1 Personal data about consumers/ service users
   2 Personal data about a business or organisation
   3 N/a – we do not process personal data of any sort
   4 Don't know

ASK ALL

5. Does your organisation **build or operate** any of the following services for **multiple** customers or clients? *Please select all that apply*

   1 Outsourced Information and Communications Technology services For example: datacentre or cloud service provision, infrastructure hosting, systems integration, software systems development, applications service provision, applications maintenance and support, end-user support/helpdesk, information security management services, managed cyber defence services, managed telecommunications services, disaster recovery services or overall service integration and management (SIAM).
   2 Business process outsourcing (underpinned by ICT) For example: HR, payroll and procurement functions
   3 None of these
   4 Don't know
   5 Prefer not to say

ASK ALL

6. Would you consider your organisation to have complex and interconnected supply chains? *Select one only*

   1 Yes
   2 No
   3 Don't know

ASK ALL

7. Does your organisation have a supply chain with more than 3 tiers of suppliers? Select one only

1 Yes
2 No
3 Don't know

ASK ALL

8. If one of your organisation's main suppliers was incapacitated by a cyber attack for 48 hours, what impact would this have on your day to day business operations or service provision? Select one only
   1 No impact
   2 Small impact
   3 Moderate impact
   4 Severe impact
   5 Don't know

ASK ALL

9. Has your organisation experienced a cyber security incident which has caused disruption to your day to day business operations or service provision in the last 3 years? Select one only
   1 Yes
   2 No
   3 Don't know

Invest

ASK ALL

10. How many employees, in terms of FTEs, specialise in data protection within your organisation (e.g. Chief Data Officer, Head of Compliance and data protection, Data Protection Officer, Privacy Officer, Data Protection Compliance Manager etc) Please provide an estimate of the number of staff

    Now? ___FTE X Don't know Y Refused

WHERE Q10/1+

11. [**Q10/2+**: How many of these roles have been **Q10/1:** Was this role] created in the last 3 years since GDPR was announced in April 2016? Please provide an estimate of the number of staff

    Q10/2+: ___FTE **Q10/1:** 1 Yes 2 No

    X Don't know Y Refused

ASK ALL

12. There are many different factors that influence changes in cyber security (e.g. perceived, heightened external threat of cyber attacks, awareness of the cost of potential breaches and their impact, advice and guidance etc). To what extent has the amount of staff time currently devoted to data protection within your organisation been influenced by the introduction of GDPR as opposed to other factors? Select one only

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 : Don't know

ASK ALL

13. Excluding those who specialise in data protection, how many full time equivalent employees within your organisation specialise in cyber security or information security (e.g. Information Officer, Security Architect, Engineer, Analysts etc) Please provide an estimate of the number of staff

    Now? ___FTE X Don't know Y Refused

WHERE Q13/1+

14. [Q13/2+: How many of these roles have been Q13/1: Was this role] created in the last 3 years? Please provide an estimate of the number of staff

    ___FTE X Don't know Y Refused

ASK ALL

15. To what extent has the amount of staff time currently devoted to cyber security and information security within your organisation been influenced by the introduction of GDPR as opposed to other factors such as those mentioned earlier*? Select one only*

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

16. Does your organisation provide GDPR training (including inductions) for <u>all staff</u> who have access to personal data or IT systems? *Select one only*

    1 Yes
    2 No
    3 Don't know

Q16/1

17. Is any of this training (including inductions) mandatory? *Select one only*
    1 Yes
    2 Some (i.e. We provide both mandatory and optional GDPR training)
    3 No
    4 Don't know

Q16/1

18. Does this training include elements of cyber security (i.e. password protection, access control, patching, avoiding phishing etc.)? *Select one only*
    1 Yes
    2 No
    3 Don't know

ASK ALL

19. Excluding other types of training that cover elements of cyber security only, do any staff within your organisation receive specific cyber security training (i.e. password protection, access control, patching, avoiding phishing etc.)? *Select one only*
    1 Yes
    2 No
    3 Don't know

Q19/1

20. Has this training been introduced or improved in the last 3 years? Select one only
    1 Yes
    2 No
    3 Don't know

Q20/1

21. To what extent are these changes in the specific cyber security training offered in your organisation a result of the introduction of GDPR as opposed to other factors? Select one only
    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

22. Has your organisation's expenditure on the following cyber security resources increased, decreased or stayed the same in the last 3 years? Select one only for each

Resource	Increased	Decreased	Stayed the same	Don't know
a) cyber security software	□	□	□	□
b) cyber security hardware	□	□	□	□
c) outsourcing/consultancy	□	□	□	□
d) recruitment	□	□	□	□

Q22a-e/ANY INCREASED/DECREASED

23. To what extent are these changes in other cyber security resources a result of the introduction of GDPR as opposed to other factors? Select one only

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

Prioritise

ASK ALL

24. Are the following aspects of cyber security a high, medium or low priority for your organisation…

A. now
B. and were they a high, medium or low priority 3 years ago? Select one only for each

	Now				3 years ago			
Aspect	High	Medium	Low	Don't know	High	Medium	Low	Don't know
1 data protection policies, processes and procedures	□	□	□	□	□	□	□	□
2 other information/ cyber security policies, processes and procedures	□	□	□	□	□	□	□	□
3 technical controls for data protection	□	□	□	□	□	□	□	□
4 technical controls for other aspects of information/ cyber security	□	□	□	□	□	□	□	□

[If responses to Q24 indicate a change in priority across any row, go to 25, otherwise go to 26]

WHERE DIFFERENT RESPONSES BETWEEN Q24A/a-e AND Q24B/a-e

25. To what extent are these changes in your cyber security priorities within your organisation a result of the introduction of GDPR as opposed to other factors? Select one only

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

Act

ASK ALL

26. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years? You can select both introduced and improved for each but not if you've also selected stayed the same or don't know

FOR ALL:

Element	Introduced	Improved	Stayed the same	Don't know
a) data protection policies	□	□	□	□
b) information security policies	□	□	□	□
c) risk management	□	□	□	□
d) asset management	□	□	□	□
e) procurement or supply chain risk management	□	□	□	□
f) Cyber Essentials/ Cyber Essentials Plus certification	□	□	□	□
g) ISO certification	□	□	□	□
h) identity and access controls	□	□	□	□
i) technical controls	□	□	□	□
j) incident management or recovery processes	□	□	□	□
k) monitoring and review, including audit processes	□	□	□	□

Q1/1 ADDITIONAL RESPONSE OPTIONS (TECHNICAL)

Element	Introduced	Improved	Stayed the same	Don't know
l) Tracking and recording of all assets that process personal data	□	□	□	□
m) Minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity	□	□	□	□
n) Actively managing software vulnerabilities, including patching	□	□	□	□
o) Managing end user devices	□	□	□	□
p) Encrypting personal data	□	□	□	□
q) Ensuring that web services are protected from common security vulnerabilities	□	□	□	□
r) Ensuring your processing environment remains secure throughout its lifecycle.	□	□	□	□
s) Undertaking regular testing to evaluate the effectiveness of your security measures (e.g. penetration testing, virus and malware scanning)	□	□	□	□

WHERE Q26/ANY INTRODUCED OR IMPROVED

27. To what extent are these changes in your cyber security a result of the introduction of GDPR as opposed to other factors? Select one only

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

WHERE Q26/ANY STAYED THE SAME

28. Considering those elements of cyber security that have not been introduced or improved in the last 3 years, what is the main reason your organisation has not taken action in these areas?

Please write in providing as much detail as you can

ASK ALL

29. Has your organisation done one or more Data Protection Impact Assessments (or DPIA) (as required by GDPR where data processing is likely to result in a high risk to personal data)? Select one only

    1 Yes
    2 No
    3 Don't know

Q29/1

30. Has your organisation made any changes to your cyber security arrangements as a result of doing a DPIA? Select one only

    1 Yes
    2 No
    3 Don't know

Q30/1

31. What type of changes has your organisation made as a result of doing a DPIA? Please write in providing as much detail as you can

    _____

    X Don't know Y Prefer not to say

Q30/2

32. What is the main reason your organisation hasn't made any changes as a result of doing a DPIA?

Please write in providing as much detail as you can

Summary

ASK ALL

33. Reflecting on your answers to these questions, where your organisation has made changes to your organisation's cyber security personnel, training, resources, priorities and activities, which of the following factors, if any, have influenced these changes? ***Select all that apply***

    1 Introduction of GDPR
    2 Desire to comply with GDPR (and avoid penalties)
    3 Increased or greater awareness of the financial cost of potential data breaches or cyber attacks (excluding penalties)
    4 Increased or greater awareness of the reputational cost of potential data breaches or cyber attacks
    5 Advice / guidance issued by the National Cyber Security Centre (NCSC)
    6 Advice / guidance issued by another government body
    7 Advice / guidance issued by a trade association or union
    8 Advice / guidance issued by an external cyber security consultancy / service
    9 Drive for change from internal staff (e.g. from Chief Data Officer or cyber professionals)
    10 Perceived, heightened external threat of cyber attacks in your sector
    11 Perceived, heightened external threat of cyber attacks globally
    12 Response to business pressure, i.e. up or down the supply chain
    13 Response to customer pressure
    14 Response to pressure from your Board
    15 Other (Please specify):_____
    16 None of these/nothing/don't know

WHERE MORE THAN ONE SPECIFIED Q33/1-15

34. Which factors were most important in terms of influencing these changes? *Please select up to three options*

    1.
    2.
    3.
    X all as important/unable to choose

ASK ALL

35. To what extent are all of the changes in your organisation's cyber security in the last 3 years a result of the introduction of GDPR as opposed to the other factors noted? Select one only

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

36. To what extent do you agree or disagree with the following statements: Select one only for each statement

a) *'The impact of GDPR has been felt across all cyber security related areas within our organisation (e.g. preventing disruption of services, protecting valuable data), not just within specific areas (e.g. data protection)'*

1 Strongly agree
2 Agree
3 Disagree
4 Strongly disagree
5 Don't know/unsure

b) *'The changes that our organisation has implemented due to GDPR have been sustained.'*

1 Strongly agree
2 Agree
3 Disagree
4 Strongly disagree
5 Don't know/unsure

ASK ALL

37. To what extent do you agree or disagree that GDPR has led to the following consequences in your organisation? Select one only for each

Consequence	Strongly agree	Agree	Disagree	Strongly disagree	Don't know/unsure	Not applicable
a) Excessive focus on data protection to the detriment of other aspects of cyber security	□	□	□	□	□	-
b) Excessive caution amongst staff in the handling of data	□	□	□	□	□	-
c) Excessive investment in cyber security, significantly beyond what is necessary	□	□	□	□	□	-
d) Other consequences for the cyber security of your organisation*	□	□	□	□	□	□

*What were these other consequences? WRITE IN _____

ASK ALL

38. Finally, is there anything else you would like to add in relation to the impact of GDPR on cyber security? Please add in anything else you would like to tell us about this

X Nothing

ASK ALL

39. DCMS is undertaking follow up interviews with selected organisations*. They will take 30-50 minutes and will be carried out by RSM** between February and March (2020). As a thank you, those who take part in an additional interview, will be given a £50 voucher or charity donation. Would you be willing to take part in a follow-up interview and have your contact details passed to RSM for this purpose?

1 Yes
2 No

IF ASKED:

* The purpose of the follow up interviews will be to better understand the findings from this survey. For example, to find out why certain organisations have reacted to GDPR in a particular way and any variation in the impact of GDPR by size of organisation or sector

**RSM is an independent research company who has been commissioned by DCMS to undertake this research into the impact of GDPR, along with BMG.

WHERE YES, RECORD CONTACT DETAILS BELOW, OTHERWISE THANK AND CLOSE

Please provide an email address so that we can contact you for the purpose of these follow up interviews and for no other reason

Email: _____

What is the best number to call you on?

Tel: _____ X Number as called

Q39/1

40. For the purposes of the follow up interview are you happy for DCMS and their appointed research contractor to see your responses from this interview? This would only be to help guide the discussion and keep it relevant to your organisation and to avoid asking you any of the same questions again.

1 Yes
2 No

ASK ALL

41. We'd be grateful if you would provide the postcode for the organisation in which you work. This is purely to ensure that we can identify where there is more than one response from a representative of the organisation in which you work.

Postcode:_____ X Don't know Y Refused

Thank you for taking part in this survey to inform the Department's understanding of the impact that GDPR has had on cyber security outcomes to date. You can find more information and guidance on cyber security issues via the following websites:

- **National Cyber Security Centre (NCSC)- https://www.ncsc.gov.uk/**
- **Information Commissioner's Office (ICO) - https://ico.org.uk/**

13 APPENDIX G: BOARD SURVEY CAWI QUESTIONNAIRE

DCMS: Research on the impact of GDPR on cyber security outcomes

Introduction

BMG Research are conducting a survey on behalf of the Department for Digital, Culture, Media and Sport (DCMS) to obtain feedback on the impact of the introduction of General Data Protection Regulation (GDPR) on organisations' and their day to day operations. The Department wants to understand the additional steps and processes organisations have to take to manage data (whether digital or not) as a result of the introduction of GDPR and how it may have impacted, if at all, on IT systems and practices. We'd greatly appreciate your views as a Board member of the organisation in which you are employed.

The survey will take around 15 minutes to complete.

Just to confirm, your responses will be treated in the strictest confidence. BMG Research abides by the Market Research Society Code of Conduct at all times.

You can find out more information about our surveys and what we do with the information we collect in our Privacy Notice which is here www.bmgresearch.co.uk/GDPRsurvey

GDPR was announced by the Council of the EU and the European Parliament in April 2016 and became enforceable in May 2018. It aims to give people control of their personal data and create a standard for data protection in the European Union (EU). GDPR legislation applies to all organisations that process the personal data of an EU resident. Personal data refers to any information that relates to an individual person who can be directly or indirectly identified by reference to an identifier. This includes: name, identification number, location data, etc. GDPR also covers sensitive personal data which uniquely identifies an individual, e.g. genetic and biometric data.

All organisations hold data on their employers, customers or even suppliers and GDPR governs how this data is managed, whether it is held digitally or in hard copy.

If your organisation uses a third party business or consultancy to manage your IT and data storage the Department would still like to hear about the direct impact of GDPR within your organisation.

Click here to begin the survey XXX

By clicking the button you agree to participate in the survey.

If you have any queries in relation to this research please feel free to contact the project manager at BMG [contact name and email].

Interviewee name:

Interviewee's role:

What is your job title or job role within the organisation?

[WRITE IN AND PLEASE SELECT ONE ONLY – BEST FIT]

1 Chair of Audit Committee/ Risk Committee
2 Chair of the Board of Directors (Non-Executive/ Independent members only)
3 Deputy/ Vice Chair of the Board of Directors (Non-Executive/ Independent members only)
4 Chief Executive Officer
5 Chief Finance Officer
6 Non-Executive Director
7 **[Local Authorities only]** Councillor
8 Other (please specify):_____

ASK ALL

S1. Can you please confirm that you are a member of the Board within your organisation

1 Yes CONTINUE
2 No THANK AND CLOSE. Thank you for your time but for the purposes of this survey I can only speak to someone at your company that sits on the Board.

ASK ALL

S1b. We'd be grateful if you would provide the **full** postcode for the organisation in which you work. This is purely to ensure that we can identify where there is more than one response from a representative of the organisation in which you work.

Postcode:_____ X Don't know Y Refused

ASK ALL

S1c. For the same reasons, that is to ensure that we don't have more than one response from your organisation, we'd very much appreciate it if you would provide the name of the organisation in which you work.

This is completely confidential and will not be shared with a third party, including DCMS, unless you give permission at the end of this survey.

Postcode:_____ X Don't know Y Refused

ASK ALL

S1d. Approximately how many Full Time Equivalent (FTE) staff are directly employed in your organisation, where 1 FTE is equal to the hours worked by 1 employee on a full-time basis? Please provide an estimate of the number of staff

____FTEs X Don't know Y Refused

WHERE X/Y: Would you say the number of Full Time Equivalent staff falls into one of the following size bands?

1 0-9
2 10-49
3 50-249
4 250+
5 Don't know
6 Refused

ASK ALL

S1e. How would you describe the main activity of the organisation in which you work?

What is the main product or service of the organisation?
What exactly is made or done within the organisation?
Who does it sell its product/services or provide services to?
What would you type into a search engine to find an organisation like yours online?

Please provide detail below

ASK ALL

1. A new data protection law called the General Data Protection Regulation, or GDPR, was announced in April 2016 and came into effect in May 2018. Had you heard of General Data Protection Regulation or GDPR before this interview?

    1 Yes
    2 No

ASK ALL

2. Which of the following types of personal data, if any, does your organisation process? **PLEASE SELECT ALL THAT APPLY**

    1 Personal data about consumers/ service users
    2 Personal data about a business or organisation
    3 N/a – we do not process personal data of any sort
    4 Don't know

ASK ALL

3. Does your organisation **build or operate** any of the following services for **multiple** customers or clients? **PLEASE SELECT ALL THAT APPLY**

    1 Outsourced Information and Communications Technology services **[EXAMPLES PROVIDED IF REQUIRED: datacentre or cloud service provision, infrastructure hosting, systems integration, software systems development, applications service provision, applications maintenance and support, end-user support/helpdesk, information security management services, managed cyber defence services, managed telecommunications services, disaster recovery services or overall service integration and management (SIAM).]**
    2 Business process outsourcing (underpinned by ICT) **[EXAMPLES PROVIDED IF REQUIRED: HR, payroll and procurement functions]**
    3 None of these
    4 Don't know
    5 Prefer not to say

ASK ALL

4. Would you consider your organisation to have complex and interconnected supply chains?

    1 Yes
    2 No

ASK ALL

5. Does your organisation have a supply chain with more than 3 tiers of suppliers?

    1 Yes
    2 No

ASK ALL

6. If one of your main suppliers was incapacitated by a cyber attack for 48 hours, what impact would this have on your day to day business operations or service provision? **PLEASE SELECT ONE ONLY**

    1 No impact
    2 Small impact
    3 Moderate impact
    4 Severe impact
    5 Don't know

ASK ALL

7. Has your organisation experienced a cyber security incident which has caused disruption to your day to day business operations or service provision in the last 3 years?

    1 Yes
    2 No
    3 Don't know

Invest

ASK ALL

8. Has your organisation's investment in the following areas increased, decreased or stayed the same in the last 3 years since GDPR was announced in April 2016? **PLEASE SELECT ONE FOR EACH**

Resource	Increased	Decreased	Stayed the same	Don't know
a) Staff time devoted to data protection (e.g. including roles such as Chief Data Officer, Head of Compliance and data protection, Data Protection Officer, Privacy Officer, Data Protection Compliance Manager etc)	□	□	□	□
b) Staff time devoted to other aspects of cyber security or information security (e.g. Information Officer, Security Architect, Engineer, Analysts etc)	□	□	□	□
c) Amount of cyber security training provided	□	□	□	□
d) Range of cyber security training provided	□	□	□	□
e) Spend on other cyber security resources (e.g. cyber security software and hardware, awareness raising, outsourcing/consultancy, recruitment)	□	□	□	□

Q8a-f/ANY INCREASED/DECREASED

9. There are many different factors that influence changes in investment in cyber security (e.g. perceived, heightened external threat of cyber attacks, awareness of the cost of potential breaches and their impact, advice and guidance etc). To what extent are these changes in your investment in cyber security a result of the introduction of GDPR as opposed to other factors? **PLEASE SELECT ONE ONLY. PLEASE USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

Prioritise

ASK ALL

10. Has the Board approved a cyber security strategy for your organisation? **PLEASE SELECT ONE ONLY**

    1 Yes, we have a dedicated cyber security strategy
    2 Yes, we have a cyber security strategy as part of our IT strategy
    3 No, we do not have a formal cyber security strategy

WHERE Q10/1, 2

11. Is it…? **PLEASE SELECT ALL THAT APPLY**

    1 Risk based?
    2 Aligned with business objectives?
    3 Supported by a dedicated budget?
    4 Don't know

WHERE Q10/1, 2

12. To what extent has your cyber security strategy been influenced by the introduction of GDPR as opposed to other factors? **PLEASE SELECT ONE ONLY PLEASE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

13. Has the Board of Director's awareness of cyber security increased, decreased or stayed the same in the last 3 years (since the introduction of GDPR)? **PLEASE SELECT ONE ONLY**

1 Increased
2 Stayed the same
3 Decreased
4 Don't know

WHERE Q13/1, 3 (INCREASED/DECREASED)

14. To what extent is this change a result of the introduction of GDPR as opposed to other factors?
PLEASE SELECT ONE ONLY
USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

ASK ALL

15. Are you aware of the National Cyber Security Centre (NCSC) Board Toolkit?

1 Yes
2 No

WHERE Q15/1

16. Has your organisation used it?

1 Yes
2 Not yet but plan to in the future
3 No
4 Don't know

WHERE Q16/3

17. Why not? **PLEASE PROVIDE AS MUCH INFORMATION AS YOU CAN**

X Don't know Y Prefer not to say

ASK ALL

18. How often does the Board receive reported updates on cyber security? **PLEASE SELECT ONE ONLY**

1 Weekly
2 Monthly
3 Quarterly
4 Annually
5 Not at all
6 Done on an ad hoc basis
7 Other (Please specify):_____

ASK ALL

19. Has the frequency of these of cyber security updates increased, decreased or stayed the same in the last 3 years?

    1 Increased
    2 Stayed the same
    3 Decreased
    4 Don't know

WHERE Q19/1,3

20. To what extent are these changes in frequency a result of the introduction of GDPR as opposed to other factors? **PLEASE SELECT ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

21. To what extent do you agree with the following statements about updates on your organisation's cyber security (e.g. the information reported to the Board by those responsible for cyber security in your organisation about the risk relating to the confidentiality, integrity and availability of data, assets and systems)? **PLEASE SELECT ONE ONLY FOR EACH**

Statement	Strongly agree	Agree	Disagree	Strongly disagree	Don't know
a) It is more comprehensive than it was 3 years ago (i.e. covers people, processes and technology)	□	□	□	□	□
b) It is more robust than it was 3 years ago (i.e. reliable, accurate, high quality and stands up to scrutiny)	□	□	□	□	□
c) It is more responsive to external changes than it was 3 years ago	□	□	□	□	□
d) It is more focused on data protection, rather than general cyber security, than it was 3 years ago	□	□	□	□	□

WHERE STRONGLY AGREE/AGREE (1, 2) IN ANY Q21a-d

22. To what extent are these changes a result of the introduction of GDPR as opposed to other factors? **PLEASE SELECT ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

23. In the last 3 years, has the Board increased, decreased or given the same prioritisation to the following aspects of cyber security: **PLEASE SELECT ONE ONLY FOR EACH ROW**

Aspect	Increased	Decreased	Stayed the same	Don't know
a) Embedding cyber security into your structure and organisation's objectives	☐	☐	☐	☐
b) Growing in-house cyber security expertise	☐	☐	☐	☐
c) Developing a positive cyber security culture	☐	☐	☐	☐
d) Establishing your risk profile baseline and identifying what you care about most	☐	☐	☐	☐
e) Understanding your cyber security threat	☐	☐	☐	☐
f) Risk management	☐	☐	☐	☐
g) Implementing effective technical cyber security measures	☐	☐	☐	☐
h) Working with suppliers and partners to manage supply chain risks	☐	☐	☐	☐
i) Planning your response to cyber incidents	☐	☐	☐	☐

WHERE INCREASED/DECREASED (1, 2) IN ANY Q23a-j

24. To what extent are these changes in your cyber security priorities a result of the introduction of GDPR as opposed to other factors? **PLEASE SELECT ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

Act

ASK ALL

25. Has your organisation introduced or improved any of the following elements of cyber security in the last 3 years? **PLEASE SELECT ONE FOR EACH ALTHOUGH YOU CAN SELECT BOTH INTRODUCED AND IMPROVED IF THAT IS APPROPRIATE**

Element	Introduced	Improved	Stayed the same	Don't know
a) data protection policies	□	□	□	□
b) information security policies	□	□	□	□
c) risk management	□	□	□	□
d) asset management	□	□	□	□
e) procurement or supply chain risk management	□	□	□	□
f) Cyber Essentials/ Cyber Essentials Plus certification	□	□	□	□
g) ISO certification	□	□	□	□
h) identity and access controls	□	□	□	□
i) technical controls	□	□	□	□
j) incident management or recovery processes	□	□	□	□
k) monitoring and review, including audit processes	□	□	□	□

WHERE Q25/ANY INTRODUCED OR IMPROVED

26. To what extent are these changes a result of the introduction of GDPR as opposed to other factors? **PLEASE SELECT ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

1 To no extent (e.g. 0%)
2 To a small extent (e.g. 1-25%)
3 To some extent (e.g. 26-50%)
4 To a great extent (e.g. 51-75%)
5 To a very great extent (e.g. 76-100%)
6 Don't know

WHERE Q25/ANY STAYED THE SAME

27. Considering those elements of cyber security that have not been introduced or improved in the last 3 years, what is the main reason you have not taken action in these areas? **PLEASE SELECT ONE ONLY**

1 What we had in place was already sufficient
2 It is not a priority for our organisation
3 We do not have enough resource to devote to it
4 We do not have enough knowledge or understanding to make changes in these areas
95 Other specify
96 Don't know

Summary

ASK ALL

28. Reflecting on your answers to these questions, where you have made changes to your organisation's cyber security personnel, training, resources, priorities and activities, which of the following factors, if any, have influenced these changes? **PLEASE SELECT ALL THAT APPLY.**

    1 Introduction of GDPR
    2 Desire to comply with GDPR (and avoid penalties)
    3 Increased or greater awareness of the financial cost of potential data breaches or cyber attacks (excluding penalties)
    4 Increased or greater awareness of the reputational cost of potential data breaches or cyber attacks
    5 Advice / guidance issued by the National Cyber Security Centre (NCSC)
    6 Advice / guidance issued by another government body
    7 Advice / guidance issued by a trade association or union
    8 Advice / guidance issued by an external cyber security consultancy / service
    9 Drive for change from internal staff (e.g. from Chief Data Officer or cyber professionals)
    10 Perceived, heightened external threat of.cyber attacks in your sector
    11 Perceived, heightened external threat of cyber attacks globally
    12 Response to business pressure, i.e. up or down the supply chain
    13 Response to customer pressure
    14 Response to pressure from staff responsible for cyber security/data protection
    15 Other (Please specify):_____
    16 None/nothing/don't know

ASK ALL

29. Which factors were most important in terms of influencing these changes? PLEASE SELECT **UP TO 3**

    1.
    2.
    3.
    X all as important/unable to choose

ASK ALL

30. To what extent are all of the changes in your organisation's cyber security in the last 3 years a result of the introduction of GDPR as opposed to the other factors noted? **PLEASE SELECT ONE ONLY USE PERCENTAGES AS AN ADDITIONAL GUIDE TO RESPONSE WHERE NECESSARY**

    1 To no extent (e.g. 0%)
    2 To a small extent (e.g. 1-25%)
    3 To some extent (e.g. 26-50%)
    4 To a great extent (e.g. 51-75%)
    5 To a very great extent (e.g. 76-100%)
    6 Don't know

ASK ALL

31. To what extent do you agree or disagree with the following statements: **PLEASE SELECT ONE ONLY FOR EACH**

    a) *'e.g. preventing disruption of services, protecting valuable data), not just within specific areas (e.g. data protection).'*

    1 Strongly agree
    2 Agree
    3 Disagree
    4 Strongly disagree
    5 Don't know/unsure

    b) *'The changes that our organisation has implemented due to GDPR have been sustained.'*

    1 Strongly agree
    2 Agree
    3 Disagree
    4 Strongly disagree
    5 Don't know/unsure

ASK ALL

32. To what extent do you agree that GDPR has led to the following consequences in your organisation? **PLEASE SELECT ONE ONLY FOR EACH**

Consequence	Strongly agree	Agree	Disagree	Strongly disagree	Don't know	Not applicable
a) Excessive focus on data protection to the detriment of other aspects of cyber security	□	□	□	□	□	-
b) Excessive caution amongst staff in the handling of data	□	□	□	□	□	-
c) Excessive investment in cyber security, significantly beyond what is necessary	□	□	□	□	□	-
d) Other consequences for the cyber security of your organisation*	□	□	□	□	□	□

*What were these other consequences? WRITE IN _____

ASK ALL

33. Finally, is there anything else you would like to add in relation to the impact of GDPR on cyber security? **PLEASE TYPE IN BELOW**

X Nothing

ASK ALL

34. DCMS is undertaking follow up interviews with selected organisations*. They will take 30-50 minutes and will be carried out by RSM** between February and March (2020). As a thank you, those who take part in an additional interview, will be given a £50 voucher or charity donation. Would you be willing to take part in a follow-up interview and have your contact details passed to RSM for this purpose?

    1 Yes
    2 No

IF ASKED:

* The purpose of the follow up interviews will be to better understand the findings from this survey. For example, to find out why certain organisations have reacted to GDPR in a particular way and any var9iation in the impact of GDPR by size of organisation or sector

**RSM is an independent research company who has been commissioned by DCMS to undertake this research into the impact of GDPR, along with BMG.

WHERE YES, RECORD CONTACT DETAILS BELOW, OTHERWISE THANK AND CLOSE

Contact details for follow up interview

Email: _____

Is the telephone number I've called you on today the best number to call back on? Or would you prefer to be called on another number? IF ANOTHER NUMBER ASK:

What number is it best to call you on?

Tel: _____ X Number as called

Q34/1

35. For the purposes of the follow up interview are you happy for DCMS and their appointed research contractor to see your responses from this interview? This would only be to help guide the discussion and keep it relevant to your organisation and to avoid asking you any of the same questions again.

    1 Yes
    2 No

Thank and close:

Thank you for taking part in this survey to inform the Department's understanding of the impact that GDPR has had on cyber security outcomes to date. You can find more information and guidance on cyber security issues via the following websites:

- **National Cyber Security Centre (NCSC)- https://www.ncsc.gov.uk/**
- **Information Commissioner's Office (ICO) - https://ico.org.uk/**

14 APPENDIX H: QUALITATIVE INTERVIEW TOPIC GUIDE

Instructions for interviewer

All interviewees have already taken part in the quantitative survey (either online or over the phone) and were asked for their consent to share their responses to the quantitative survey with the research team.

Where **consent has been given**, the interviewer should familiarise themselves with the interviewees survey response in advance of the interview and make notes of any additional areas of interest to be discussed during the interview, such as:

- where an organisation has experienced a cyber incident - ask them to describe the incident and the impact it has had on the organisation, customers/clients, suppliers, their cyber security etc (link to Q4 if not covered in response to Qs4&5)
- where an organisation has identified cyber security improvements, but does not attribute this to the GDPR - what are the other drivers in play? (link to Q6)
- where an organisation has not identified cyber security improvements - why not? (especially if they identify a 'reduction' in cyber security in response to the GDPR) (link to Qs5&8)
- where an organisation has identified unintended consequences of the GDPR - what are they and what impact have they had on the organisation? (link to Q9/11)
- See specific questions for priority groups throughout questionnaire e.g. Board Members, MSPs, orgs with a complex interconnected supply chain.

Where **consent has been given**, the questions/probes **4d can be skipped**.

Where **consent has not been given**, the questions/probes in **4d should be covered**.

Introduction

Good morning/afternoon, my name is _____ and I'm calling on behalf of the Department for Digital, Culture, Media and Sport (DCMS) from RSM UK Consulting in relation to research we are completing for them on the impact of the GDPR on cyber security behaviours of organisations.

Thank-you for recently completing a survey with our colleagues at BMG Research and consenting to take part in this follow-up interview.

The purpose of this interview is to explore your organisation's reaction to the GDPR in more detail, e.g. why your organisation has reacted in this way and any variation in its impact. It will last approximately 45 – 60 mins.

The responses you provide will be kept in the strictest confidence and will only be reported on an aggregated basis, therefore no responses will be directly attributable to you. Your participation is voluntary, and you can choose to opt out at any time.

Please note we will protect the confidentiality of your information in accordance with our normal data handling procedures and all legal requirements. We will not use it for any purposes other than this research. We will only retain your contact details for as long as necessary to support this research and no longer than 30 June 2020.

We take all reasonable technical and organisational measures to protect personal data from loss, misuse or alteration. Only authorised employees are allowed to access data held by RSM.

You are entitled at any stage to ask that your personal data, or part or all of the record of your interview responses, be destroyed or deleted and we will carry out such a request. This can be requested during the interview itself or afterwards by emailing [contact name and email].

Can you confirm you have received and read the Privacy Notice sent out with your invite to this interview? *If Yes proceed if No send Privacy Notice via email and ask them to take a couple of minutes to read it before proceeding*

- ☐ Interviewee confirmed they have received and read the Privacy Notice

Is it okay if I record this interview for accurate recall?

- ☐ Yes
- ☐ No

Questions

Board response (approx. 10 mins)

Background: DCMS would like to understand:

- *Is cyber security viewed as a priority by Board members?*

  Ways in which Boards may demonstrate the prioritisation of cyber security include: having a dedicated cyber security strategy; having regular updates on cyber security to the Board; having clear governance processes for cyber security at Board level.
- *If yes was this as a result of the GDPR or is it due to other factors?*
- *If not, why is it not a priority (i.e. what is their rationale for decision making)?*

1. How would you describe the Board's reaction to the GDPR?

   – *Probe in relation to:*

   a) Attitude (positive/negative/neutral)
   b) Approach (proactive/reactive)
   c) Barriers and enablers
2. Has Board prioritisation of cyber security changed in the last 2 – 3 years?

If <u>yes</u>: What changes have been made and what motivated them to make these changes (e.g. was it a result of the GDPR or where they already making changes due to other reasons, if yes what were they)?

If <u>no</u>: Why have you not made any changes/why is cyber security not a Board priority (e.g. is there no desire to consider cyber security or are their other areas that are viewed being a greater priority, if so, what are these?)

3. Is cyber security still on the Board agenda? *Probe as to why it is or is not*

Organisation response to the GDPR (approx. 15 mins)

Background: DCMS would like to understand:

- *Whether organisations have improved their cyber risk management/view cyber security as a priority*
- *If yes, was this as a result of the GDPR or due to other factors? What might those other factors be?*
- *If not, why is it not a priority (to understand the reasons behind this, for example do they see it as not relevant to them/their company etc.)*

Where an organisation has experienced a cyber incident - ask them to describe the incident and the impact it has had on the organisation, customers/clients, suppliers, their cyber security etc (link to Q4 if not covered in response to Qs4&5)

Where an organisation has not identified cyber security improvements - why not? (especially if they identify a 'reduction' in cyber security in response to the GDPR) (link to Qs5&8)

Where an organisation has identified cyber security improvements, but does not attribute this to the GDPR - what are the other drivers in play? (link to Q6)

4. How would you describe your organisation's reaction to the GDPR?

- *Probe in relation to:*
  a) Attitude (positive/negative/neutral)
  b) Approach (proactive/reactive)
  c) Guidance/information sought - i.e. what was it and from where (e.g. NCSC/ICO[123])?
  d) Where **consent has not been given**: Actions taken, i.e. changes in:
     i) Resources (e.g. staff, training, software, hardware, consultancy, recruitment)
     ii) Priority of cyber security (compared with other aspects of security or business management)
     iii) Policies relating to cyber security and/or data protection
     iv) Processes (e.g. risk management, asset management, procurement/supply chain risk management, incident management/recovery processes, monitoring and review)
     v) Procedures (e.g. Cyber Essentials/Cyber Essentials Plus, ISO certification, identity and access controls, technical controls)
  e) Barriers and enablers (i.e. what has prevented/slowed/limited change to cyber security risk management and prioritisation and what has supported/enabled it)
     i) *If there are/were barriers:* How could they be/were they overcome (e.g. what additional support or guidance, if any, is needed)?

[123] National Cyber Security Centre, Information Commissioner's Office

5. Why has your organisation reacted in this way? *Prompts:*
    a) To comply with the regulations
    b) To avoid penalties for non-compliance
    c) Leadership from the Board/SMT/Cyber professionals (internal or external)
    d) Driven by customers/clients, supply chain (up or down) or non-cyber staff
    e) Lack of capacity (i.e. time and resources/budget)
    f) Lack of capability (i.e. knowledge and ability)
    g) What was in place already was sufficient
    h) Not a priority
6. What other drivers/factors have influenced changes in your cyber security (i.e. in addition to/instead of the GDPR)? *Probe relative importance of these compared to the GDPR*

Changes in cyber security (approx. 20 - 25 mins)

Background: DCMS would like to understand:

- *If any improvements been realised equally or partially across all aspects of cyber security (some research suggests that the GDPR may have resulted in a disproportionate focus on data/information security to the detriment of other areas)*
- *How companies view their cyber security capability (e.g. is it possible that some companies have not made changes however still view their cyber security as being robust)*
- *Challenges faced by organisations in relation to cyber security*

Where an organisation has <u>not</u> identified cyber security improvements - why not? *(especially if they identify a 'reduction' in cyber security in response to the GDPR) (link to Qs5&8)*

Where an organisation has identified unintended consequences of the GDPR - what are they and what impact have they had on the organisation? (link to Q9/11)

7. *Where changes have <u>not</u> been made:* How confident are you in your organisation's ability to:
    a) manage cyber security risks?
    b) protect against a cyber breach/attack?
    c) detect security threats?
    d) respond to/recover from a breach/attack?

If confident in relation to a-d: What is driving that confidence?

If not confident in relation to a-d, probe in relation to:

i. the risks identified
ii. their potential impact on the organisation
iii. what the organisation intends to do to mitigate these risks (if anything)

8. *Where changes have not been made:* Has the GDPR led to any negative impacts/unintended consequences for your organisation (e.g. prioritisation of data security leading to neglect of other important areas of cyber security)? *Tailor this question based on responses to survey if available*

9. *Where changes have been made:* Do you think the changes you have made in response to the GDPR have improved your cyber security? *Probe in relation to ability to:*

    a) manage cyber security risks
    b) protect against a cyber breach/attack
    c) detect security threats
    d) respond to/recover from a breach/attack

10. *Where changes have been made:* Has the GDPR had a bigger impact on some areas of cyber security than others (e.g. data protection over IP or continuity of service)? *If so,* why? *Tailor based on responses to survey if available and probe in relation to:*

    a) Positive impacts/improvements
    b) Negative impacts/unintended consequences (e.g. prioritisation of data security leading to neglect of other important areas of cyber security)

11. *Where changes have been made:* Were/are there any challenges to sustaining these changes (over one year on)? Please explain your answer. *Probe whether some aspects are more/less sustainable than others and why?*

Additional questions for organisations with complex and interconnected supply chains or who are managed service providers (MSPs):

Supply chain (approx. 10 – 15 mins)

12. Has the GDPR had any impact on how your company conducts supplier risk management?

If yes: What did the impact relate to specifically?

13. Did your company benefit as the result of implementing those changes? How?

- *Probe in relation to:* supply chain (cyber security) risks and the factors affecting decision making in this space.

14. Do you feel your company can manage all risks that come from its supply chains effectively?

If no: What are the biggest obstacles which prevent you from effectively managing your suppliers?

MSPs (approx. 10 mins)

15. Has the GDPR had any impact on your relationship or processes with the organisations you provide services to?

If yes: What did the impact relate to specifically? Was it positive, negative or neutral?

- *Probe in relation to:* (cyber security) risks and the factors affecting decision making in this space

Thank you and close (approx. 5 mins)

ALL ORGS

16. Is there anything else you would like to add in relation to this research?
17. As part of this research we will develop a series of anonymised case studies demonstrating the various ways in which organisations have responded to the introduction of the GDPR. Are you willing to be contacted by a member of the research team to discuss this in more detail?

- ☐ Yes
- ☐ No

Thank you for taking part in this interview inform the Department's understanding of the impact that the GDPR has had on cyber security outcomes. You are now eligible to either receive a £50 amazon voucher or have a £50 donation made to the charity of your choice. Which would you prefer:

- ☐ Amazon voucher (Confirm interviewee's email address):_____
- ☐ Charitable donation
    - If charitable donation, confirm name of charity:_____
    - How would you like the donation to appear (e.g. anon, org name, interviewer name etc)?:_____

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made.

Recommendations for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Consulting LLP for any purpose or in any context. Any party other than the Board which obtains access to this report or a copy and chooses to rely on this report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Consulting LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to our Client on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report. RSM UK Consulting LLP is a limited liability partnership registered in England and Wales no.OC397475 at 6th floor, 25 Farringdon Street, London EC4A 4AB