Cyber security incentives & regulation review: summary of responses to the call for evidence

gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence/cyber-security-incentives-regulation-review-summary-of-responses-to-the-call-for-evidence

Ministerial foreword

Matt Warman MP, Minister for Digital Infrastructure

Protecting the British public will always be the first priority of this government. We believe in the transformative potential of digital technologies to promote growth and positive social change. We are also not naive about the risks those technologies might bring. That is why we are investing £1.9 billion in cyber security and utilising our world-leading capabilities to make the UK the safest place to live and work online. We want to ensure that the procurement and use of technology is underpinned by robust cyber security measures so that organisations can protect their business, their data and their customers.

The central importance of digital transformation to the UK economy and society has been brought into stark relief through the coronavirus pandemic, with citizens and organisations from across the country relying on technology and new digital services more than ever before. The UK's digital infrastructure has supported us all throughout this difficult period.

We’ve also seen cyber criminals continue to target individuals and organisations with a range of ransomware and malware attacks. With new and innovative technologies entering our lives, the challenge of using them securely is of great importance. To bounce back and start our economic recovery, we must unlock the benefits of digital in an effective, responsible and secure way.

In 2019, we sought industry feedback on the core barriers organisations face in managing their digital security risks in the Cyber Security Incentives and Regulation Call for Evidence. The responses have given us a nuanced and industry-focused understanding of the challenges organisations face, and where we should be focusing government’s efforts.

In the months since we launched the Call for Evidence, we have also launched the Cyber Aware campaign to help keep the public secure online. The National Cyber Security Centre has published new guidance to help organisations operate securely in the new digital environment and in April, the NCSC launched the Suspicious Email Reporting Service to help us take down malicious websites. The new service has received a fantastic response from the public, with over 1.7 million reports received, leading to the removal of over 15,000 malicious sites. The Government will shortly be announcing additional support to help organisations improve their cyber risk management during the current pandemic.

Our work in this area will be most effective when done in partnership. I am grateful to all those who took the time to respond to the Call for Evidence. As organisations adapt to the markedly different environment they are operating in, we will continue to engage with them to ensure they are supported and equipped to manage their cyber risk effectively. Now more than ever, the digital resilience of all citizens and organisations is essential to the prosperity of the UK economy.

Matt Warman MP

Minister for Digital Infrastructure

Executive summary

The Cyber Security Incentives and Regulation Call for Evidence ran from 4 November 2019 until 20 December 2019. It sought industry input on the barriers faced by organisations and the economy as a whole in taking effective action to manage cyber risks. In particular, it called on industry to identify the information and assurances that would result in organisations better prioritising and investing in the mitigation of cyber risks as part of their broader organisational resilience and business continuity.

This public response sets out a summary of the main findings from the Call for Evidence, including analysis of the 21 questions that respondents answered. This document brings together the collective insights that have been gathered as part of the process of this consultation.

To progress this work, the Government has been reassessing the current risk landscape in light of the Covid-19 crisis and the increasingly rapid digitisation of the economy. Coronavirus has fundamentally altered our lives and the role that tech plays within it. Tech plays a central role in enabling the UK's economic, social and health recovery - from analysing data to creating new jobs to ensuring education can continue and people remain connected. In this context, of particular interest is ensuring small and medium-sized businesses (SMEs) are well supported to embark on this transition in a way that both stimulates their economy recovery and growth whilst ensuring their security risks are mitigated. Likewise, supporting procurement professionals and those managing supplier risks to undertake their roles effectively is of utmost priority to ensuring any organisation is resilient in the current context.

The Department for Digital, Culture, Media and Sport (DCMS) will be working with industry over the coming months to develop policy proposals which seek to address some of these barriers, as highlighted through our evidence gathering efforts. Further details are outlined in the Next Steps section.

Summary of the call for evidence findings

The Call for Evidence was a key first step in testing our understanding of the barriers that many organisations face in managing their risks. These barriers were outlined as:

- a range of **inabilities** that organisations may have, from not knowing what to do, to not having the right skills and resources;
- a **lack of commercial rationale** or business drivers that stimulate the prioritisation of and investment in cyber risk management; and
- a **complex and insecure digital environment** within which organisations base many business operations in this digital era.

The majority of respondents agreed with the three barriers that were presented in the Call for Evidence. Over 70% of respondents agreed that each presented a moderate or severe barrier to organisations managing their risk effectively, providing validation for DCMS' understanding of the main barriers to organisations undertaking effective cyber risk management. Respondents also highlighted two further barriers of:

1. a lack of incentives to support organisations to protect their organisation online; and
2. insufficient regulation to compel organisations to better manage cyber risks.

While we believe that Government initiatives to date have had a positive impact on cyber security, these efforts have tended to focus on improving organisational capability, and more recently on addressing insecurities in the design and provision of products or services. Less explicit focus has been placed on exploring and addressing commercial rationales for investment in cyber security. The Call for Evidence focused more extensively on the underlying reasons for the apparent lack of commercial drivers (barrier

2). The findings highlight that a lack of commercial rationale is a significant barrier for organisations, and was identified to be an even more severe barrier for micro and small organisations.

Respondents highlighted that a lack of commercial rationale was particularly due to organisations being unable to justify the cost of investment in cyber risk mitigations without clear articulation and proof of the benefits. The evidence confirms that cyber security investment decisions are not currently underpinned by clear, easily accessible or assured information. For example, the Call for Evidence findings indicate that organisations are attempting to use information on impact to inform cyber security investment decisions. However, 86% of respondents stated that an inability to fully understand and anticipate the direct and indirect impact of cyber attacks is a moderate or severe barrier to effective risk management. These types of information failure are currently preventing many organisations from being able to accurately make an assessment of their cyber risk. Accordingly, in the short to medium term, it is likely that organisations will continue to face barriers in developing a strong commercial rationale for investment in their cyber security risk mitigation activities.

The Call for Evidence also sought input on where Government should focus the development of a new programme of activity. The majority of respondents (75%) agreed that additional Government solutions are required for assuring and standardising information used in cyber risk management, whether this is information on the cyber threat, impact of a cyber breach, or mitigation activity. A large number of respondents provided suggestions for this information being provided through the introduction of new, or improvement of existing, frameworks and standards. The Call for Evidence responses also highlighted key issues around SMEs, who are less likely to have specialised cyber security teams. They often therefore lack technical expertise and cyber security is likely an additional responsibility of staff focused on other areas.

The onset of Covid-19 has increased the overall risk surface through a rapid increase in the use of and reliance on digital technologies - from individuals, to small businesses, to the FTSE 100. This rapid adoption has only exacerbated the real need for easily understood and standardised ways of communicating what minimum expectations and best practice in managing digital risks. This is a necessity if we are to embed cyber security as part and parcel of every business' business continuity and risk management.

Additional suggestions were provided for embedding this information in existing corporate governance and business assurance mechanisms, including supplier management, or by Government using additional regulation, incentives, and advice and guidance. In the context where businesses are becoming 'digital' overnight or are seeking to provide new online services or business models, procurement and management of digital suppliers becomes a critical part of business continuity. However, we know the great majority of organisations struggle with managing supplier risks, with the Cyber Security Breaches Survey 2020 showing just 15% of businesses currently review their supplier risks.

The Call for Evidence submissions highlight a range of difficulties organisations face - including not knowing what security measures to look for in a supplier; difficulties in finding sufficient companies to tender; the prioritisation of low costs; and SMEs not having enough leverage with large suppliers. This shows there is still further work to be done to embed standards through utilising procurement and supplier management as an effective market lever in holding organisations to account.

Overall, the Call for Evidence responses provide detailed evidence as to the barriers organisations continue to face in managing their digital risks, which are evermore heightened in today's environment. But perhaps more importantly, the responses provide a better understanding of what organisations need and how to develop and improve existing initiatives - whether market-based or provided by Government. Further next steps for engaging with DCMS in the development of joint Government and industry initiatives are included at the end of this public response. Industry should be encouraged to take part in this process to ensure that future interventions meet their needs and are effective in overcoming some of the core barriers as we step into an ever more digitised business environment.

Introduction

The Department of Digital, Culture, Media and Sport (DCMS) launched a Call for Evidence in November 2019 to seek industry evidence and insights on the barriers organisations and the economy still face in taking effective action to manage digital risks, three years after the establishment of the National Cyber Security Centre (NCSC).

In the Call for Evidence an understanding of three core barriers was outlined as:

- **Lack of ability**, comprising a lack of capacity and knowledge in organisations to manage cyber risk and protect themselves online.
- **Complexity and insecurity of the digital environment**, on the basis of insecure digital products or services in use across organisations and interconnectivity between organisations within and across sectoral and geographic barriers.
- **Lack of commercial rationale**, including that organisations find it difficult to demonstrate compelling cases for return on investment on cyber security due to the lack of quantifiable information, including the financial impact, related to cyber attacks.

Through the Call for Evidence, DCMS tested an understanding of these three categories, and sought input on industry's views on the mitigating action that is still required to improve cyber risk management across the UK economy. It has been encouraging to find that respondents have generally agreed with the outline of barriers and understanding of reasons behind the lack of commercial drivers, which DCMS set out in the Call for Evidence. It is critical that the Government's understanding of such barriers reflects the realities faced by businesses. This assists in measuring the effectiveness of Government efforts to date against these barriers, as well as enabling the identification of where and what shape future policy action is required.

Summary of responses

In total, 138 responses were received to the Call for Evidence between 4 November and 20 December 2019. This included 29 responses from individuals, 64 from organisations, and 45 unspecified responses.

Respondents were able to respond via an online survey, or via email. The Call for Evidence included a mix of open and closed questions. Respondents were not required to answer all questions. All questions and the accompanying percentages are reported based on the number of respondents that answered that individual question. This is detailed in the description of each question through each section of this public response.

For open response questions, every response has been reviewed and, while not every point that was made by each respondent can be reflected, responses were coded to identify common themes. The following sections provide an overview of the key or notable themes identified, whilst providing a balanced overview to reflect the range of views expressed.

This public response provides an overview of the findings we have collated through the analysis of the Call for Evidence responses. It does not set a policy direction but instead outlines a set of findings that broaden the evidence base for cyber security risk management practices and barriers across the economy.

As set out in the {Next Steps}(https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence/cyber-security-incentives-regulation-review-call-for-evidence-summary-of-responses?preview=4362701#next-steps) section at the end of this public response, DCMS will draw on these findings while continuing to work closely with industry, NCSC, other key Government departments to develop proposed interventions that better enable and encourage organisations to prioritise and invest in effective cyber risk management.

1. Barriers to effective cyber risk management

The first part of the Call for Evidence set out DCMS's understanding of the main barriers to organisations undertaking effective cyber risk management, based on research and engagement undertaken to date. DCMS defined these three barriers as:

- **Lack of ability**, comprising a lack of capacity and knowledge in organisations to manage cyber risk and protect themselves online.
- **Complexity and insecurity of the digital environment**, on the basis of insecure digital products or services in use across organisations and interconnectivity between organisations within and across sectoral and geographic barriers.

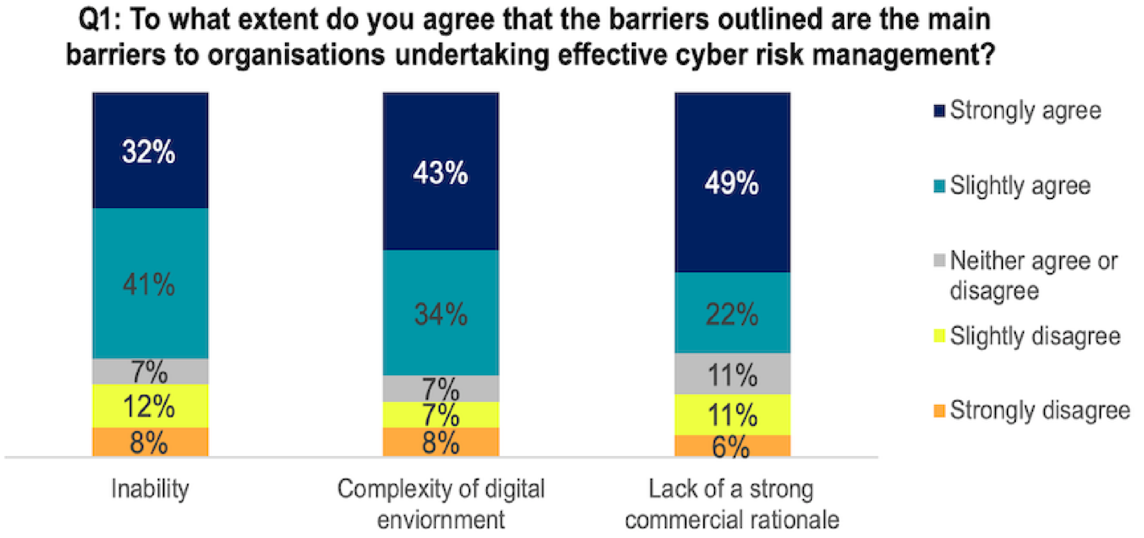
- **Lack of commercial rationale**, including that organisations find it difficult to demonstrate compelling cases for return on investment on cyber security due to the lack of quantifiable information, including the financial impact, related to cyber attacks[footnote 1].

This section of the Call for Evidence tested agreement with the three main barriers outlined; requested insights and evidence on other key barriers to effective cyber risk management; and asked respondents to identify methods that Government or industry could use to address the barriers of inability and complexity and insecurity of the digital environment.

The majority of respondents agreed with the three core barriers that were presented in the Call for Evidence. Over 70% of respondents agreed that each of the three barriers presented a moderate or severe barrier to organisations managing their risk effectively:

- 72% agreed for inability
- 77% agreed for complexity of the digital environment
- 71% agreed for a lack of strong commercial rationale.

The majority of respondents agreed with each of the 3 barriers outlined



Base: All who responded; Barrier 1 – Inability (123), Barrier 2 - Complexity of digital environment (121), Barrier 3 – Lack of a strong commercial rationale (122)

Other barriers to effective cyber risk management identified by respondents

The majority of respondents (79% of 126 who responded) stated that there were other key barriers not captured within the three main barriers outlined, and 87 respondents provided evidence or examples of these additional barriers. DCMS believes that a large proportion of these additional barriers fit within our definition of a lack of ability, complexity and insecurity of the digital environment, and a lack of commercial rationale. However, respondents did highlight two other barriers. These were:

- a lack of incentives to support organisations with protecting their organisation online, and
- insufficient regulation to compel organisations to more effectively manage their cyber risk.

Barrier 1 - A lack of ability

Many of the additional barriers identified by respondents related to a lack of capability and skills within organisations, particularly among board members. Respondents highlighted that organisations lack:

- board and senior level capability and responsibility for cyber risk.
- a skilled and experienced cyber security workforce with the resources required to manage cyber risk, including a lack of dedicated and/ or experienced staff, time constraints, and limited financial resources.
- understanding and clarity regarding the appropriate cyber security practice and requirements. Respondents also highlighted that organisations do not understand what action should be taken given the confusion caused by numerous tools and frameworks across industry.

Evidence for how Government and/or industry could address the barrier of inability was provided by 81 respondents. This was asked as an open question, with responses coded into themes, including:

- **Advice, guidance and support (58%)**: A large proportion of respondents suggested that inability could be addressed through improved advice, guidance and support, including improving training, awareness and understanding at all levels of organisations, as well as specifically at the board level. Some respondents suggested the need to further develop the cyber security industry and encourage the upskilling of cyber security professionals. There was a key theme of increased cyber security awareness and training outside of the workplace, with some submissions highlighting the need to provide cyber security education from a young age and industry taking more responsibility for providing additional training and support to employees.
- **Incentives (21%)**: Respondents indicated that there is a need to further incentivise organisations. Suggestions include:
- providing free certified resources and services,
- financial incentives to encourage organisations to invest in training.
- **Standards and frameworks (11%)**: A small proportion of respondents called for the development of appropriate security standards and certifications to ensure organisations understand what is required to mitigate cyber risk effectively.

- **Regulation (14%)**: Some respondents mentioned the need for additional regulation, including mandated standards, cyber security training at the board level or cyber risk management responsibility at the board level, and compelling organisations to have dedicated cyber security capability.
- **Security by design (5%)**: A small proportion mentioned that the lack of ability would be less of a barrier if products are secure by design. This input recognises the interrelated nature of the initial 3 barriers that were presented in the Call for Evidence, namely, that the insecurity of digital products, processes and technology presents a difficult barrier in being able to mitigate their associated risks.

Barrier 2 - Complexity and insecurity of the digital environment

Respondents indicated that the constantly evolving digital landscape was preventing organisations from being able to be secure online. In addition, the fact that organisations' digital products, services and operations are becoming increasingly integrated with other organisations, was identified by respondents as making it more difficult for organisations to manage cyber risk. A number of respondents mentioned further potential barriers: the openness of the internet network, and the limited requirements around digital products being secure by design.

Evidence for how Government and/or industry could address this barrier was provided by 76 respondents. This was asked as an open question, with responses coded into themes, including:

- **Advice, guidance and support (20%)**: Some respondents highlighted the need for additional advice, guidance and support. Specific suggestions included that a common language around cyber risk is required, including the reduction in use of technical language and promoting a common terminology that can be used by cyber security professionals, boards and all staff within organisations.
- **Frameworks/ standards (16%)**: Respondents mentioned the need for additional frameworks and standards and methods for assuring and standardising information used in cyber risk management. These are outlined in more detail in later sections.
- **Regulation (18%)**: The need to implement additional regulation, or extend existing regulation was highlighted by some respondents. Suggestions for the type of regulation that should be implemented were varied, but included: additional codes of conduct or certification requirements for software engineers; mandating Cyber Essentials or another minimum cyber security standard for all organisations; and mandating secure by design requirements for IOT devices[footnote 2].
- **Secure by design (16%)**: Some respondents also mentioned that digital products must be secure by design to reduce cyber risk before it enters the economy.
- **Supply chain management (4%)**: Respondents also highlighted the need for assistance in supply chain management.

Summary of 'barriers to effective risk management'

Findings from this section of the Call for Evidence validate DCMS' understanding of the main barriers to organisations undertaking effective cyber risk management, with over 70% of respondents agreeing that a lack of ability, complexity and insecurity of the digital environment, and a lack of commercial rationale all present a moderate or severe barrier to organisations managing their risk effectively. Findings have also highlighted that DCMS should consider how to address the lack of incentives to support organisations with protecting their organisation online, and the insufficient regulation to compel organisations to more effectively manage their cyber risk.

Government intervention to date has focused on addressing the barriers of inability and complexity and insecurity of the digital environment: * A lack of ability has started to be improved largely through advice, guidance, and investment in cyber skills and professionalisation. * In recent years, the Government has also increasingly started focusing efforts on addressing complexity and insecurity of the digital environment through a number of policy interventions which seek to reduce risk upstream, such as through the Secure by Design and Active Cyber Defence programmes.

However, despite this Government action, these barriers still remain, indicating that there is still more to be done by Government in these areas. In particular, the Call for Evidence responses suggest that additional advice, guidance and support, and standards and frameworks that set out good practice could help to further reduce these barriers.

2. Commercial barriers and incentives for investing in effective cyber risk management

In recent years, the Government has increasingly focused efforts on improving organisational capability and more recently, on securing the digital environment, with less focus on what is required to enable organisations to create a commercial rationale for investment in cyber security. Through the Call for Evidence, DCMS therefore sought industry input and evidence to better understand what drives and inhibits a strong commercial case for investment in cyber security, particularly where information is limited in its availability and there is inadequate assurance about its credibility.

It should be noted that many of the additional barriers that respondents outlined in response the Call for Evidence were encompassed in the definition of a lack of strong commercial rationale:

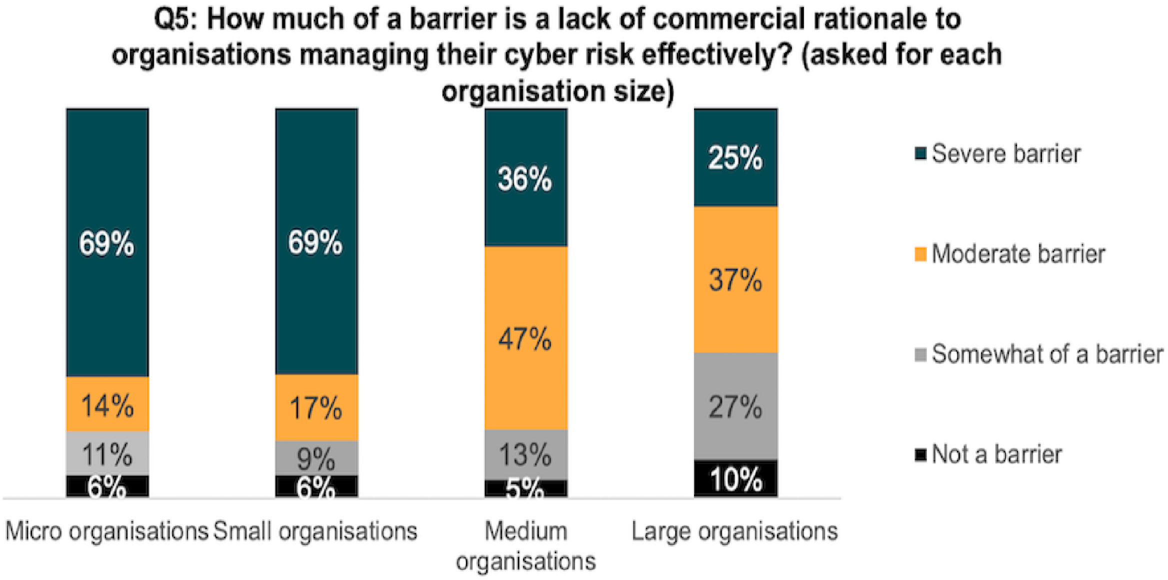
- A key theme in submissions to the Call for Evidence was that organisations find it difficult to demonstrate a return on investment as they are **unable to quantify the level of cyber risk** and therefore cannot develop a business case that justifies investment in cyber risk mitigations.
- Respondents also highlighted that organisations find it difficult to demonstrate compelling cases for return on investment on cyber security due to a **lack of information about the threat and potential impact**. Organisations do not believe they will be targeted and do not fully recognise the potential impacts if they are targeted.

- Some respondents therefore noted that, due to these **information failures**, organisations see cyber security solely as a cost to business without a strong corresponding understanding of the benefits of investment in cyber risk mitigation.

Extent to which a lack of commercial rationale presents a barrier

Respondents were asked how much of a barrier a lack of commercial rationale is to organisations of various sizes. A majority of respondents saw it as a moderate to severe barrier for organisations of all sizes. However, a lack of commercial rationale was more likely to be thought of as a severe barrier for micro and small organisations (69%), while a quarter of respondents saw this as a severe barrier for large organisations.

A lack of commercial rationale is seen to be a severe barrier particularly for micro and small organisations



Base: All who responded about Micro organisations (90), Small organisations (89), Medium organisations (88), Large organisations (91)

Reasons for a lack of strong commercial rationale to invest in cyber security

The Call for Evidence asked for input on why there is a lack of commercial rationale for organisations of all sizes to invest in cyber security, and 81 respondents provided a broad number of reasons. This was asked as an open question, with responses coded into themes, including:

- **The cost of investing in cyber risk mitigations without evidence of the benefits of that investment (63%)**: Many respondents mentioned a lack of dedicated cyber security budgets as cyber risk mitigation is seen as expensive. Organisations find it difficult to justify these budgets as they cannot prove there is a return on investment, particularly as they lack data or evidence that would enable them to better justify investment. A smaller proportion of respondents also highlighted that some organisations, particularly those in a supply chain, are expected to invest more in cyber security than is commercially viable in order to protect other organisations.
- **Lack of prioritisation (48%)**: Respondents highlighted that organisations do not prioritise cyber risk as they do not understand or recognise the cyber threat they face. Organisations also have to focus on more pressing priorities and business operations and do not have capacity to also focus on and mitigate cyber risk.
- **Limited understanding of the impact of a cyber breach (25%)**: A factor contributing to organisations finding it difficult to developing a compelling case for investment in cyber risk management is that organisations lack an understanding of the impact of a cyber breach, including not believing they will be targeted and therefore impacted, and only anticipating part of the impact that they will experience.
- **Lack of capability (31%)**: The submissions also indicated that organisations do not have enough experienced staff to properly assess and mitigate cyber risk. This included the lack of a skilled workforce, but also highlighted barriers in the lack of dedicated staff that organisations have to adequately assess the risk they face and particularly, the lack of understanding of an organisation’s assets.
- **Lack of responsibility (12%)**: Respondents highlighted that a lack of responsibility, including at Board level, was also making it more difficult for organisations to justify investment in cyber security. Organisations outsourcing their cyber risk management was also identified as a contributing factor.

Identified reasons why there is already a strong commercial rationale for organisations to invest in cyber security

The Call for Evidence asked respondents that were aware of strong commercial drivers for organisations investing in their cyber risk management to provide the reasons and evidence that underpinned this driver. This was asked as an open question, with responses from 42 responses coded into themes, including that:

- **There is a rationale for larger organisations to invest in cyber security**: Respondents highlighted that large organisations do understand the cyber risk, recognise the impact of cyber incidents and have more resources to manage their cyber security effectively. A small number of respondents also mentioned that larger organisations have more assets to protect and therefore find it less challenging to demonstrate compelling cases for return on investment on cyber security.

- **Investment in cyber security is commercially viable for smaller organisations**: A small number of respondents highlighted that smaller organisations have a strong commercial rationale to invest in cyber security as smaller organisations have a lower cyber risk posture, and therefore need basic and more affordable cyber security with these products and services being relatively secure by default/ design.
- **Organisations recognise impacts of lack of investment**: Regardless of the size of organisation, respondents highlighted that for organisations with strong commercial drivers for investment, this is based on a recognition of the impacts of cyber breaches and attacks. Organisations can therefore develop a case for the return on investment, particularly by identifying the potential financial impacts, such as the company suffering reputational damage if it experiences a significant cyber attack.
- **Organisations recognise the commercial advantages of investing in cyber security**: Only a small number of respondents highlighted that some organisations realise the advantages of investing in cyber security, such as how it can provide competitive advantage and protect the organisation's intellectual property.

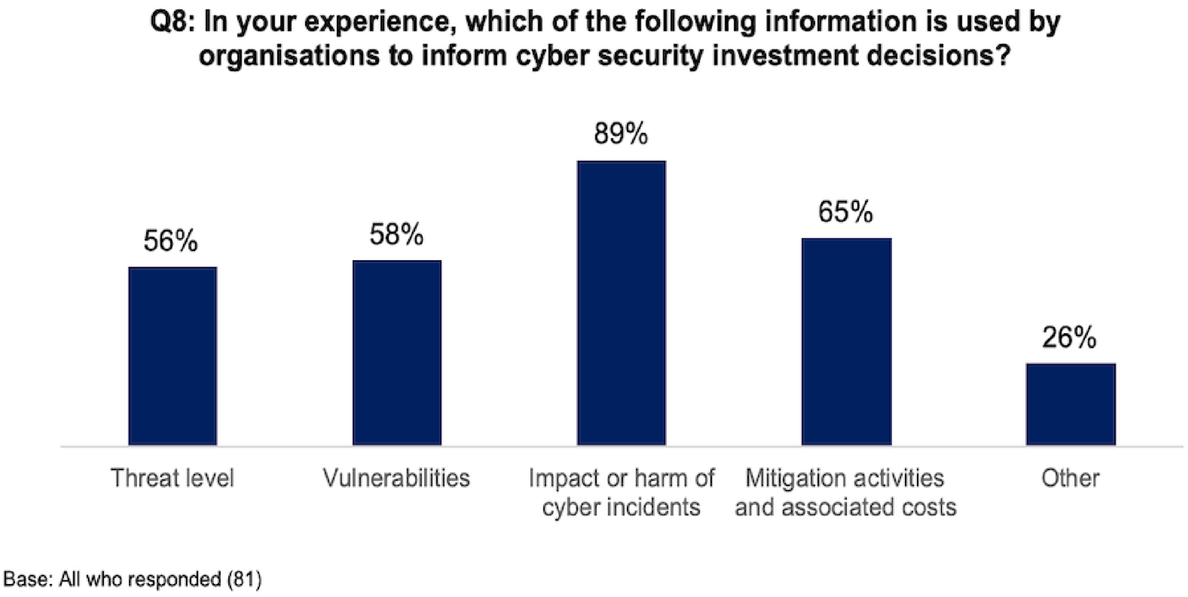
Information used by organisations to inform cyber security investment decisions

The Call for Evidence highlighted that, although cyber risk management decisions are often underpinned by a risk management assessment using complex methods and models, in simple terms, the main information that informs these decisions includes some combination of:

a. Vulnerabilities (e.g. what assets and how the company might be attacked) b. Threat (e.g. frequency and severity) c. Impact or harm of cyber incidents (e.g. direct and indirect costs) d. Mitigation activities and associated costs (e.g. activities such as the implementation of cyber security controls or training which constitute effective mitigation).

The Call for Evidence asked respondents for insights on the types of information used most by organisations to inform cyber security investment decisions. This question was answered by 81 respondents, with 89% stating that information on the impact or harm of cyber incidents is used to inform cyber risk management decisions. Between 56% and 65% of respondents stated that information on the threat level, vulnerabilities and mitigation activities is also used.

The information most required in cyber security investment decisions is information covering the impact or harm caused by cyber incidents



Use of this information was detailed by respondents as follows:

1. **Threat Level (45 respondents provided detail of how threat information is used)**: Some mentioned that threat level information is predominantly used to estimate likelihood of a cyber incident which informs a risk assessment. This information is used to determine cyber risk management decisions such as the level of investment and in which business areas to focus investment.
2. **Vulnerabilities (28 respondents)**: Respondents mentioned that known vulnerabilities are used to drive prioritisation of cyber security investment, to quantify the level of risk exposure that an organisation faces, for example, through penetration testing. Some respondents identified limitations, including that smaller companies are less able to identify vulnerabilities and that this information is not well understood by non-technical audiences.
3. **Impact or harm of cyber incidents (51 respondents)**: Respondents highlighted that information on the impact of a cyber incident was used by organisations. Information used included: * External cyber incidents such as publicised reports of attacks on similar types of organisations, reviewing breach notifications from the news, reports from the Information Commissioner's Office (ICO) or relevant authorities. Information on external incidents was noted to increase awareness amongst the board of organisations.
   * An assessment of the potential financial impacts and reputational damage that an organisation could experience. In particular, it was noted that this information was used to Inform contingency planning.

4. **Mitigation activities and associated costs (35 respondents)**: Respondents mentioned that this information is used for financial decision making, predominantly to determine the budget for cyber risk management. Some respondents mentioned that the cost of investing in mitigations is assessed against the likelihood of the organisation experiencing a cyber incident and the potential impact of a cyber incident. These costs are often assessed against other budget priorities. Limitations listed included that cyber risk assessment models are not robust, reputational harm is hard to quantify and that cyber investment is seen as optional rather than essential.

Other types of information is also used to inform cyber risk management decisions

A quarter of respondents stated that other types of information is also used by organisations to inform cyber security investment decisions (26%). This included information on:

- organisational risk appetite and tolerance thresholds
- the organisation's budget priorities
- regulatory requirements and the risk of penalties
- comparisons against peer or competitor organisations
- supply chain requirements set out by organisations that procure services or products
- an organisation's cyber risk management from audit findings.

Summary of 'commercial barriers and incentives'

Responses to this section confirmed that a lack of commercial rationale is a significant barrier to effective cyber risk management, especially for micro and small organisations. Responses also demonstrated that the main causes of this lack of commercial rationale are the cost of investing in cyber risk mitigations without evidence to demonstrate a return on investment, and a lack of prioritisation among organisations.

The Call for Evidence findings confirm that information on threat, vulnerability, impact and risk mitigation activities is required to make effective commercial decisions and is critical to ensuring organisations are prioritising and appropriately investing in cyber risk mitigations. This evidence in this section demonstrates that many organisations are currently using impact information to inform their cyber security investment decisions. However, Section 3 outlines the limitations in the use of this information.

The evidence, however, also highlights that cyber security investment is not underpinned by clear, easily accessible or assured sources of information on the above areas and accordingly, in the short to medium term, it is likely that organisations will continue to face barriers in developing be a lack of strong commercial rationale for investment in their cyber security risk mitigation activities.

3. Access to the right information for effective cyber risk management

Whilst the second part of the Call for Evidence sought input on what information needs organisations have in informing commercial decision making processes, the third part focused on the specific barriers organisations are experiencing in accessing this information. As tested in the Call for Evidence and outlined in Section 2 of this public response, access to the appropriate information to inform risk management decisions is a prerequisite for an organisation making sound investments in cyber security. Conversely, where this information is not available, organisations face a key barrier to determining the level and type of investment appropriate to their cyber risk posture.

The Call for Evidence tested three information failures that had been identified through Government research and engagement:

- Some organisations often either do not draw on, find it difficult to engage with, or do not invest in information about **cyber threats** and their exposure to them.
- The direct and indirect **impacts of a cyber attack** are often not fully recognised. Businesses often do not understand the totality of either short or long-term, indirect and intangible costs associated with a cyber attack (e.g. fines, share price or client/ customer base loss).
- There is no agreed definition or standard of **effective risk management**, which leads to businesses not knowing how they should invest or the potential cost of mitigation activity.

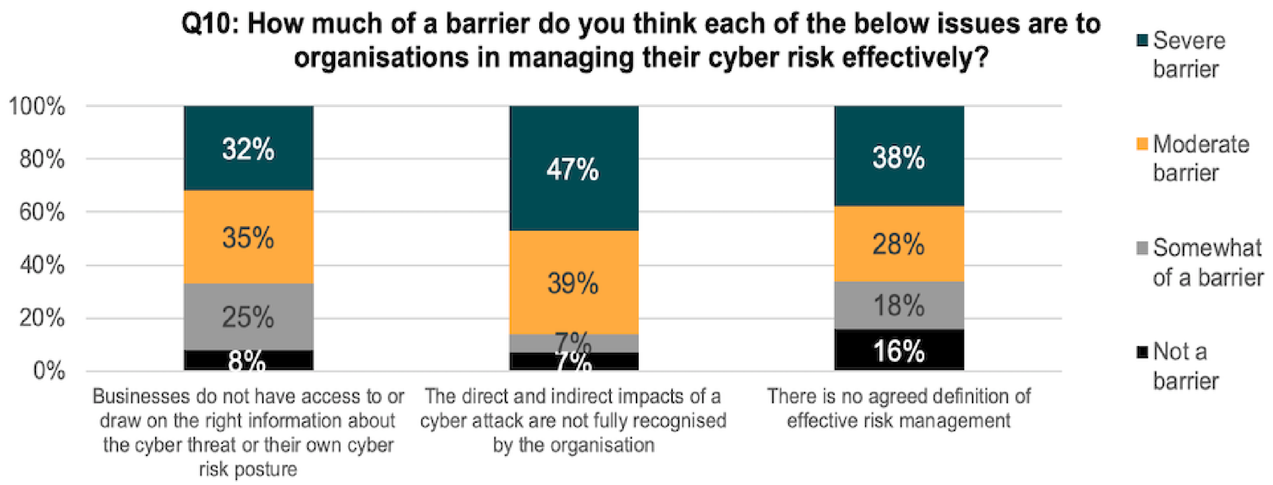
This section asked respondents how much of a barrier each of the three identified information-based issues posed to organisations. Respondents were also asked about what other information would allow organisations to make better investment decisions; the barriers to creating, collecting or accessing this information; and how the market is currently addressing these information transparency barriers.

Information barriers to organisations managing their cyber risk effectively

As highlighted below, a majority of respondents agreed that the three information failures outlined in the Call for Evidence presented severe or moderate barriers:

- Not having the right information on the potential **impacts of a cyber attack** was thought to be the most significant barrier, with just under half of respondents stating that this is a severe barrier for organisations (47%).
- No agreed definition of **effective risk management** was thought to be a severe barrier by four in ten respondents (38%).
- Businesses not having the right information on the **cyber threat** was identified as a severe barrier by a third of respondents (32%).

Despite many organisations requiring impact information to make investment decisions, the majority stated that organisations not fully recognising impacts is a moderate/ severe barrier, highlighting the need for further good quality impact information



Q10: How much of a barrier do you think each of the below issues are to organisations in managing their cyber risk effectively?

Base: All who responded (85)

Information that would allow organisations to make better investment decisions in cyber security

Respondents were asked to provide input on what information would allow organisations to make better investment decisions in cyber security, with 80 respondents answering this open response question[footnote 3]. Responses have been coded into themes. Suggested information included:

- **Cyber threat (20%)**: A fifth of respondents highlighted that additional information on the cyber threat would be beneficial to organisations.
- **Vulnerabilities (13%)**: Some respondents thought that additional information on vulnerabilities information would be useful, with a small number specifically referencing information for more effective asset management and protection.
- **Impact or harm of cyber incidents (21%)**: Where respondents were specific about the types of impact or harm information that would be useful, they mentioned the need for more case studies and stories, and tools to support organisations to carry out cyber impact assessments.
- **Mitigation activities and associated costs (27%)**: Specific suggestions from respondents included information that could inform a return on investment case, including more information on costs of mitigative activities. Respondents also highlighted that organisations would benefit from products that enabled more effective benchmarking against organisations with similar cyber risk postures, and a means to better manage supply chain risks.

- **Other information (7%)**: Some respondents mentioned the need for other kinds of information, for example, information that is tailored or relevant to specific types of organisations or sectors.

Respondents also provided suggestions of how this information should be provided This was asked as an open question, with responses coded into themes, including:

- **Advice, guidance and support (28%)**: Suggestions included cyber risk management training, improving cyber expertise in organisations and additional advice and guidance more generally.
- **Standards/ frameworks/ models (9%)**: Some respondents suggested standards that enabled more effective risk assessments, and that these standards should be supported by models that enable an organisation to receive a score on how effectively they are managing their cyber risk.

Barriers preventing organisations from creating, collecting or accessing this information

Details on barriers preventing organisations from currently creating, collecting or accessing the information they require was provided by 77 respondents. This was asked as an open question, with responses coded into themes. These barriers included:

- **Information failures (40%)**: Issues in this category were broad ranging - from some respondents outlining the difficulties of information overload, to others highlighting the lack of existence of other types of information needed to support cyber risk assessments. Responses further focused on organisations not having access to the right information; and a lack of information sharing.
- **Lack of knowledge and understanding (36%)**: Over a third of respondents highlighted a lack of knowledge, understanding and awareness as a barrier preventing organisations from creating, collecting or accessing information.
- **Lack of resources (32%)**: Respondents specifically mentioned a lack of funding, time, dedicated staff and trusted resources. Some also commented that the current commercial offerings are overpriced.
- **Lack of prioritisation (27%)**: A lack of motivation and prioritisation was identified as a barrier to organisations developing and using cyber risk management information, including amongst board members.
- **No standardised approach (22%)**: Respondents stated that there are too many cyber risk management frameworks and standards, with some specifically mentioning that existing frameworks are not suitable for some types of organisation.
- **Lack of regulation (10%)**: Some respondents highlighted that a lack of appropriate or enforced regulation creates a barrier for the creation and use of information as without such regulation organisations have little appetite to seek out cyber risk management information.

Evidence of how the market is currently effectively addressing information transparency barriers

A third of respondents stated that there is no evidence of anything currently in the market addressing information transparency barriers (32%), while 14% stated that they did not know. However, just over half (54% of 84 respondents) stated that there is evidence that the market is currently addressing information transparency barriers:

- These respondents cited services and products provided by industry, including risk management frameworks (e.g. ISO 27001), threat intelligence services and penetration testing. However, these respondents also highlighted the limitations of current industry products and services, such as tools being overpriced and organisations not being able to appropriately use the tools once purchased. Some respondents also mentioned the difficulty organisations have in selecting the appropriate products and services.
- Some respondents also highlighted Government products and services that are being used by organisations and the market to address information transparency barriers. This included advice and guidance from NCSC (e.g. Cyber Essentials).
- A small number of respondents mentioned the need for increased information sharing to address cyber risk information failures.

Summary of ‘access to the right information for effective cyber risk management’

When organisations make cyber risk management decisions they draw upon estimates of the cost of investing in cyber security against the potential benefits procured or impacts mitigated. However, the Call for Evidence findings strongly indicate that information failures currently prevent most organisations from being able to conduct these cyber risk assessments.

In particular, responses regarding the three information failures outlined in the Call for Evidence findings have indicated that for organisations to conduct an effective cyber risk assessment, they require additional information on:

- The direct and indirect impacts of a cyber attack with 86% of respondents stating the inability to fully understand the impact of cyber attacks is a moderate or severe barrier to effective risk management.
- An agreed definition of ‘good’ risk management with 65% of respondents stating this information is critical to investment decisions. This is compounded by 66% stating that the lack of an agreed definition of ‘good’ risk management is a moderate or severe barrier to mitigating their cyber risk.

These findings point to ongoing market failures based on information asymmetries and imperfect information regarding cyber security risk management across the economy. The Call for Evidence responses support research which suggests that this stems from businesses not knowing enough about their cyber security risk or what forms of protection are most effective. Overarchingly, many cannot accurately calculate the cost or benefits to their business of investing in increased cyber protection, and many do not consider it a priority. This information failure is supported by Government Office for Science research that indicates that not all organisations have the knowledge, understanding and confidence around cyber security in order to implement appropriate measures.

4. Future policy and regulatory interventions

The final section of the Call for Evidence sought industry engagement on future policy and regulatory interventions that could help to normalise investment in cyber security across the UK economy and improve cyber risk management in organisations.

Respondents were asked to provide evidence of the solutions organisations currently have for assuring and standardising information used in cyber risk management; whether additional solutions are required; what types of information should be assured or standardised and how Government or industry could help to generate more useful information. Respondents were also asked what is required to improve responsibility and accountability at a senior level within organisations.

Current solutions organisations have for assuring and standardising the information used in cyber risk management

Solutions that organisations currently use for assuring and standardising the information used in cyber risk management were provided by 69 respondents. This was asked as an open question, with responses coded into themes. Solutions were predominantly industry frameworks and standards; and Government regulation and standards.

- **Government regulation and standards (35%)**: Of Government regulation, standards and frameworks, most commonly mentioned were NCSC's Cyber Essentials, General Data Protection Regulation (GDPR) and the Security of Network & Information Systems Directive's (NIS) Cyber Assessment Framework (CAF). More broadly, some mentioned NCSC guidance as a solution for assuring and standardising information.
- **Industry standards and frameworks (45%)**: The most commonly referenced industry frameworks and standards were International Organization for Standardization's (ISO) certifications, such as ISO 27001, 27002, 27701 and 27005, and the National Institute of Standards and Technology's (NIST) framework.
- **Other**: A small number of respondents mentioned other commercial offerings or informal industry information networks. Other types of products mentioned included general risk management solutions, risk maturity models and cyber threat intelligence. Some respondents mentioned services that provide organisations with support for assuring and standardising information, specifically consultancies and internal audit services, and the cyber insurance industry.

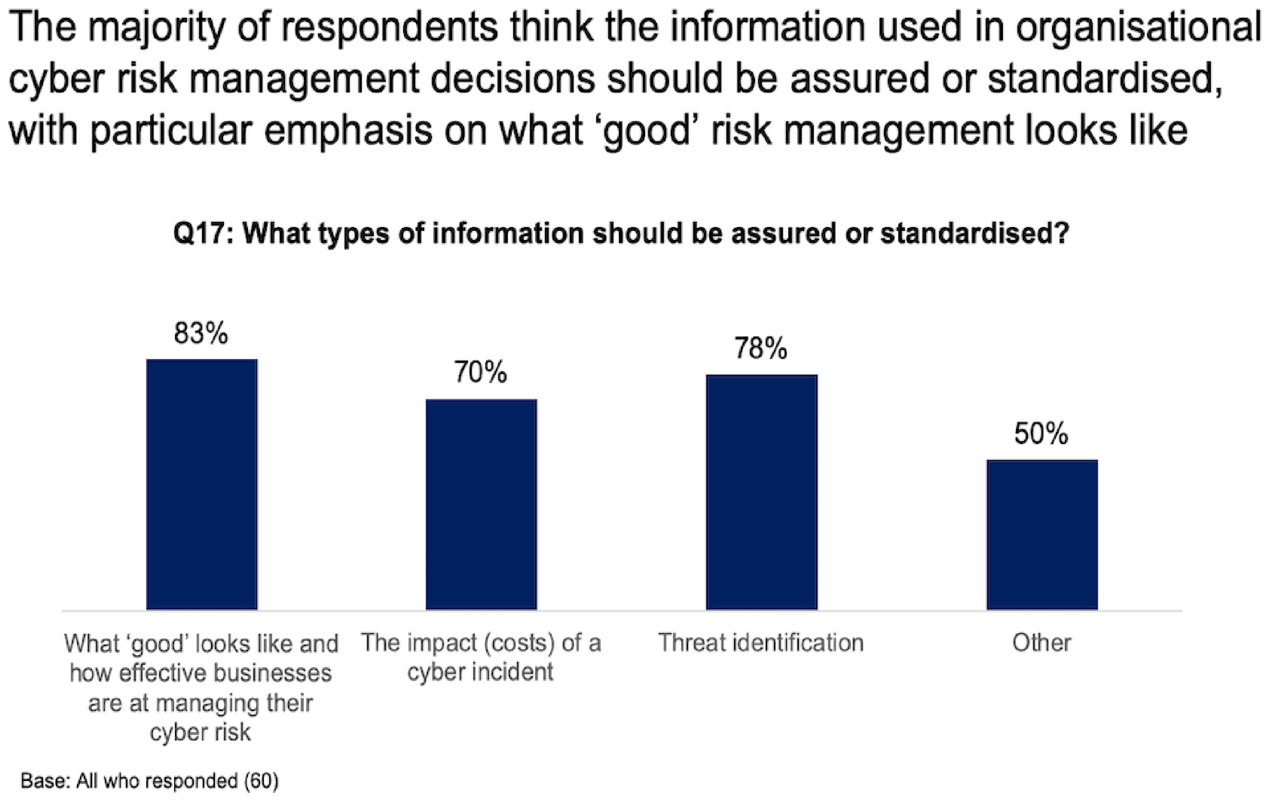
Some respondents noted the limitations of existing solutions for assuring and standardising information used in cyber risk management, including that current solutions are not fit for purpose, there are too many frameworks and standards, and issues with implementation prevent effective cyber risk management.

Additional solutions for assuring and standardising the information used in cyber risk management

Respondents were asked whether additional solutions are required for assuring and standardising information used in cyber risk management. This question was answered by 85 respondents, with three quarters stating that additional solutions are required (75%).

Respondents who highlighted that there should be additional solutions were asked to state which types of information should be assured or standardised. This question was answered by 60 respondents with:

- 83% indicating the need for additional solutions that assure and standardise 'what good looks like', that being, what constitutes effective cyber risk management.
- 78% indicating that threat identification information should be assured and standardised.
- 70% indicating the need for additional assurance and standardisation of information on the impact of cyber incidents.



The majority of respondents think the information used in organisational cyber risk management decisions should be assured or standardised, with particular emphasis on what 'good' risk management looks like

Q17: What types of information should be assured or standardised?

Base: All who responded (60)

Half of respondents (50%) also stated that other information should be assured or standardised. Examples of suggestions include: best practice examples, what cyber security controls to apply to address vulnerabilities, roles and responsibilities within organisations, cyber insurance guidance, and guidance on training for senior staff.

Solutions that assure or standardise the key information underpinning cyber risk management decisions

68 respondents provided suggestions for how Government or industry could develop solutions to provide an assured or standardised approach to defining and assessing the key information underpinning cyber risk management. This was asked as an open question, with responses coded into themes. These included:

- **Improved frameworks and standards (49%)**: Half of respondents highlighted the need to promote existing industry frameworks, improving or extending existing Government frameworks and create new standards or frameworks. A smaller proportion of respondents suggested that development of a model that enabled organisations to be scored for how effectively they were managing their cyber risk. Some respondents also highlighted that existing frameworks need to be made more accessible (e.g. in terms of cost).
- **Additional assurance mechanisms (19%)**: A fifth of respondents mentioned the need for additional assurance mechanisms, specifically that there should be a system of external verification or accreditation.
- **Additional regulation (18%)**: Some respondents suggested regulation would provide additional assurance and standardisation of cyber risk information, for example, by mandating existing Government standards such as Cyber Essentials, enforcing existing industry standards, or by embedding cyber risk management in the corporate reporting.
- **Provision of incentives (15%)**: Respondents suggested that a solution would require increased incentivisation, including financial incentives (e.g. tax breaks or tax-free dividend) or improved information sharing and collaboration.
- **Advice, guidance and support (16%)**: Some respondents also suggested that additional advice, guidance and support could improve the key information underpinning cyber risk management
- **International alignment (7%)**: A small proportion of respondents highlighted the need for solutions to be aligned with other international solutions.

Approaches Government or industry could take to make cyber risk management information more transparent, accessible and trusted

64 respondents highlighted how Government or industry could make the key information used in cyber risk management more transparent, accessible and trusted. This was asked as an open question, with responses coded into themes. Suggestions included:

- **Advice, guidance and support (41%)**: Specific solutions included delivering cyber risk management training, providing a common language to talk about cyber risk, reducing the use of technical language, and making information available for free.
- **Collaboration (30%)**: Collaboration and information sharing was highlighted by almost a third of respondents, through industry and government information sharing, collaborating across industry in peer to peer sharing networks, and the facilitation of anonymised information sharing.

- **Frameworks and standards (27%)**: Suggestions were split between those who advocated the promotion of existing industry frameworks (11%) and those who suggested the creation of new frameworks (16%). Five per cent also suggested extending or improving existing Government frameworks.
- **Regulation (13%)**: Suggestions for additional regulation included mandated reporting of cyber incidents and mandating minimum cyber security standards.
- **Accreditation (11%)**: An accreditation scheme was suggested as a means of making the key information used in cyber risk management more robust and transparent.
- **Government services (6%)**: Suggestions included Government providing additional information on official sites, and the provision of financial incentives, either through providing funds or reducing the cost of certifications.
- **International alignment (5%)**: As for the previous question, a small proportion of respondents highlighted the need for solutions to be aligned internationally.

Increasing responsibility and accountability for cyber risk management at the senior level

Suggestions on the requirements and solutions that would ensure that, at a senior level, organisations take responsibility and accountability for effective cyber risk management were provided by 69 respondents. This was asked as an open question, with responses coded into themes, including:

- **Regulation (45%)**: Almost half suggested additional regulation. This included suggestions of mandating accountability including board members being directly accountable for cyber security or having a Chief Information Security Officer on the board, establishing director liability and compelling organisations to provide additional information through corporate reporting. A small proportion suggested that this could be achieved through extending existing regulation (6%), such as GDPR.
- **Improved understanding (14%)**: Some suggested increasing responsibility and accountability could be achieved by improving understanding and knowledge, particularly through cyber risk training for Board members.
- **Industry led enforcement (3%)**: A small proportion suggested that increased responsibility and accountability at a senior level could be achieved through industry initiatives such as organisations requiring their suppliers to comply to standards, and membership bodies and professional association requirements.

A final open question asked respondents what more Government and/or industry could do to help to stimulate investment in effective cyber risk management. Input was provided by 63 respondents, with responses coded into themes. Suggestions provided to this question were similar to responses to other questions throughout the Call for Evidence, particularly the need for additional regulation.

A third of respondents suggested implementing new or extending regulation (30%); a quarter of respondents (24%) thought that investment could be stimulated through the creation of new standards and frameworks or the increased promotion of existing standards and frameworks; and 16% suggested the use of financial incentives, for example, grants to cover accreditation. Other recommendations included building capability through the provision of cyber security education and training (14%), additional advice guidance and support (14%) and the need for products to be secure by design (3%).

Summary of ‘future policy and regulatory interventions’

This section highlighted the main solutions that organisations currently use for assuring and standardising the information used in cyber risk management, including the Government’s existing implementation of Cyber Essentials, General Data Protection Regulation (GDPR), the Network and Information Systems Regulations (NIS) Cyber Assessment Framework, and industry standards and frameworks such as ISO certifications and NIST.

Despite the existence and use of these standards and frameworks, many respondents agreed that more information is required around outlining what comprises effective cyber risk management, the full potential impacts that might be experienced from a cyber attack and additional threat information. It was suggested this additional assured information could be created and made available with improved standards and frameworks, either new or existing.

However, the Call for Evidence findings highlighted that there is also support for organisations to be required to take more responsibility and accountability for effective cyber risk management through the implementation of additional regulation, either to increase responsibility and accountability at the senior level or more generally to stimulate investment in effective cyber risk management.

Next steps

As put forth in the Call for Evidence, the development of policy interventions that help support recovery and future resilience of organisations across the UK will be most effective when done in partnership and with an understanding of what works, so it is important that a wide range of views from organisations of all sizes and sectors is captured in the development of new policy interventions. If we want to see sustained cultural change across organisations, we need to ensure that this work engages all organisations that influence and set market standards and act as drivers for corporate governance, risk management and business continuity.

DCMS will continue to progress the development of new interventions, and we will set out further detail on policy proposals in this area over the coming months, as set out below.

Next steps include:

- **Further in-depth analysis of all evidence** provided through the Call for Evidence, alongside other key pieces of evidence such as the recently published Cyber Security Breaches Survey 2020. New research on the impact of GDPR on security outcomes, and on a framework to analyse the full costs of cyber incidents is being published alongside with this publication. The findings, including full analysis of the sources of evidence provided in submissions to the Call for Evidence will be considered as part of DCMS' ongoing policy development process.
- **The development of new policy interventions**. DCMS will use the findings from the Call for Evidence, along with the evidence and insights obtained through consultation and wider stakeholder engagement, to scope and analyse policy options. This will focus on what action we can take in the immediate term to support organisations through the economy's recovery, as well as longer term perspectives on the role of the UK's regulatory framework in helping achieve a better standard of cyber security across the economy.
- **Ongoing engagement with key industry and Government stakeholders**. To inform the design of new policy interventions, DCMS will engage with key industry stakeholders, regulators and relevant Government departments. This engagement will seek input on the prioritised policy interventions and test whether these interventions will provide the necessary internal and external drivers to create a stronger rationale for cyber security prioritisation and investment.
- **Publication of a policy statement and future policy recommendations**. 2020 presents a number of opportunities for shaping the future direction of Government support for business cyber resilience within the broader agenda of enabling digital and tech to help us recover and grow as a nation. We will be utilising forthcoming fiscal events including the Comprehensive Spending Review and opportunities such as the publication of a new digital strategy in the Autumn to shape a refreshed strategic approach to cyber resilience, one that reflects the new post-Covid reality.

This work will evaluate the work HMG has done to date on supporting businesses to improve their levels of digital resilience, reflecting on the impact advice and guidance has had alongside the sufficiency of existing regulation, including GDPR and the NIS Regulation. This future policy statement will further propose policy interventions that will support organisations to develop a compelling case for investment in cyber security and encourage organisations across the economy to take more responsibility and accountability for cyber risk management over the course of the future National Cyber Security Strategy.

Annex: List of call for evidence questions

1. To what extent do you agree that the barriers outlined ((1) inability; (2) complexity and insecurity of the digital environment; and (3) lack of a strong commercial rationale) are the main barriers to organisations undertaking effective cyber risk management? Single response (Strongly agree, slightly agree, neither agree or disagree, slightly disagree, strongly disagree)

2. Are you aware of any other key barriers to effective cyber risk management that are not captured in the 3 barriers highlighted? Single response (Yes/No)
3. [If Yes at Q2] Please provide any evidence or examples you have of other key barriers to effective cyber risk management. Open response
4. What evidence do you have for how Government and/or industry could help address the following two barriers, in addition to the existing interventions outlined? Barrier 1 - Inability Open response Barrier 2 - Complexity and insecurity of the digital environment. Open response
5. How much of a barrier is a lack of commercial rationale to organisations managing their cyber risk effectively? Please answer for each of the organisation sizes below. Single code/matrix (Not a barrier, Somewhat of a barrier, Moderate barrier, Severe barrier) / (Micro organisations (Less than 10 employees); small organisations (10-49 employees; medium organisations (50-249 employees); large organisations (250 or more employees))
6. [If moderate barrier/severe barrier for any organisation size] What are the reasons for a lack of strong commercial rationale for the following organisations to invest in cyber security? [organisation sizes selected at Q2] Please provide evidence to support your answer. Open response
7. [If not a barrier/ somewhat of a barrier] What evidence do you have that there is a strong commercial rationale for the following organisations to invest in cyber security? [organisation sizes selected at Q2] Please provide evidence to support your answer. Open response
8. In your experience, which of the following information is used by organisations to inform cyber security investment decisions? Please select all that apply Threat level Vulnerabilities Impact or harm of cyber incidents Mitigation activities and associated costs
9. [For those selected at Q8] In your experience, how is this information used by organisations to inform cyber security investment decisions? Please provide any evidence you have for how this information is used. Threat level; Vulnerabilities; Impact or harm of cyber incidents; Mitigation activities and associated costs; Open response
10. How much of a barrier do you think each of the below issues are to organisations managing their cyber risk effectively? a. Businesses do not have or draw on the right information about the cyber threat or their own cyber risk posture; b. The direct and indirect impacts of a cyber attack are not fully recognised by the organisation; c. There is no agreed definition of effective risk management; Single code per option (Not a barrier, Somewhat of a barrier, Moderate barrier, Severe barrier).

11. What information would allow organisations to better make investment decisions in cyber security? Please provide evidence to support your answer. Open response

12. What are the barriers preventing organisations from creating, collecting or accessing this information currently? Please provide evidence to support your answer. Open response

13. Is there evidence of anything in the market currently effectively addressing these information transparency barriers? Single response (Yes/No/Don’t know)

14. [If yes] Please provide evidence of how the market is currently addressing these information transparency barriers? Open response

15. What solutions do organisations currently have for assuring and standardising the information used in cyber risk management? Please include evidence or examples. Open response

16. Do you think that a solution for assuring and standardising the information used in cyber risk management is required? Single response (Yes/No/Don’t know)

17. [If yes] What types of information should be assured or standardised? Please select all that apply a. What ‘good’ looks like and how effective businesses are at managing their cyber risk; b. The impact (costs) of a cyber incident; c. Threat identification; d. Other (please specify).

18. How can Government or industry create a solution(s) that provides this assured or standardised approach to defining and assessing the key information underpinning cyber risk management? Please include evidence or examples from other areas. Open response

19. What approaches could Government or industry take to make this information for cyber risk management more transparent, accessible and trusted? Please include evidence or examples. Open response

20. What is required to ensure that, at a senior level, organisations take responsibility and accountability for effective cyber risk management? Please describe how this responsibility and accountability will stimulate action to manage cyber risk within an organisation. Open response

21. What more do you think Government and/or industry could do to help stimulate investment in effective cyber risk management? Please include any examples or evidence of how industry in other countries have helped to stimulate investment in effective cyber risk management. Open response

↑ Back to top