Department for
Digital, Culture,
Media & Sport

# Cyber Security Incentives and Regulation Review 2020: Call for Evidence

4 November 2019

# Foreword


Matt Warman - Minister for Digital and Broadband

This Government is committed to making the UK the best place to start and grow a digital business. We're providing the public and businesses with faster broadband, improved digital skills and stronger data protection laws. We're also tackling online harms and facing the challenges of the digital revolution in an effective and responsible way.

This is all part of the Government's digital strategy - and good cyber security is at the heart of that strategy. Having the right cyber security measures in place helps organisations protect their business, their data and their customers - and enables them to seize the opportunities of a connected world. Strong and secure businesses create jobs, attract investment and generate growth in our digital economy.

Our *National Cyber Security Strategy*[1]*,* supported with an investment of £1.9 billion, has made great strides in helping to achieve these aims. We want all organisations to be effectively managing their cyber risks, with the appropriate investments in place to improve their resilience. But despite significant Government and industry action over the course of this strategy, including the world-class guidance and support developed by the National Cyber Security Centre (NCSC), our research shows that many businesses of all sizes are still failing to adequately protect themselves against cyber attacks and data breaches, with over a third of UK businesses suffering a cyber breach or attack in 2018.[2]

Companies are getting better at assessing their cyber risks and 96% of FTSE 350 firms now have a cyber security strategy in place. But less than half (46%) have a dedicated cyber security budget and only 57% have a cyber incident response plan they test on a regular basis. Over three quarters (77%) of these leading firms furthermore fail to recognise the cyber risk across their diverse supply chains.[3] We need to understand what more can be done to improve and incentivise investment in effective cyber risk management across the UK economy.

[1] HMG National Cyber Security Strategy 2016-2021
[2] DCMS Cyber Security Breaches Survey 2019
[3] DCMS FTSE 350 Cyber Governance Health Check 2018

This is why we are reviewing the current spectrum of Government interventions, to understand the impact of action taken to date, and where Government and industry need to go further. This Call for Evidence is a key first step in testing our understanding of the barriers that remain; and to seek input on where we should be focusing work to develop a new programme of activity.

Our work will be most effective when done in partnership and with an understanding of what works, so it is important we receive a wide range of views from organisations of all sizes and sectors. This isn't just about the cyber security community. 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 drivers for corporate governance, risk management and business continuity.

Future-proofing our digital economy is an absolute priority for this Government. Good cyber security is a crucial part of this and is key to our mission of making the UK the safest place to live and work online.

**Matt Warman**
Minister for Digital and Broadband
Department for Digital, Culture, Media and Sport

# 1. Introduction

A key focus of the Government's current *National Cyber Security Strategy 2016 – 2021* is ensuring all organisations in the UK are effectively managing their cyber risk so that the UK economy is safe, secure and prosperous.

The *2016 DCMS Regulation and Incentives Review* concluded that the General Data Protection Regulation (GDPR) and the European Directive on Security of Network and Information Systems (NIS Directive), had the potential to drive improved cyber security behaviours. However, the review recommended their impact would necessarily be subject to regular review following their implementation in 2018. It further noted that this assessment may lead to the need for consideration of further Government action to achieve the improvement in cyber risk management required, whilst being cognisant of not placing unnecessary burdens on business.

Since 2016 the Government has made significant progress on tackling cyber threats and improving the resilience of the UK society and economy, both through the implementation of the GDPR and the NIS Directive, and notably, the establishment of the world-leading National Cyber Security Centre (NCSC). Whilst evaluation of the impact of Government activity on cyber security and resilience outcomes is ongoing, we believe that these efforts have not been sufficient to drive the necessary improvement in organisational cyber risk management, and to ensure the economy as a whole is adequately protected.

As we approach both the end of the current National Cyber Security Strategy and mark two years since the implementation of key legislative vehicles intended to improve cyber security outcomes, DCMS is now conducting a further Cyber Security Incentives & Regulation (I&R) Review to assess where existing incentives and support, such as advice and guidance from the NCSC, have delivered the greatest improvements, and where there are observable impacts of the existing regulatory framework. This Review will consider which additional incentives and regulation would most effectively support the economy to overcome the remaining key barriers without placing unnecessary burdens on them effectively managing cyber risk as part of broader business continuity and operational resilience risk management.

# 2. Open Call for Evidence

This Call for Evidence seeks further evidence to inform the Review and gather evidence to underpin future policy development, including potential new cyber security interventions and regulations, if deemed appropriate. Specifically, it seeks input on our assessment of both the remaining barriers, and mitigating action that is still required to normalise the integration of cyber security within operational risk management across the UK economy.

Whilst the I&R Review will seek to capture the broad range of barriers to effective cyber risk management, this Call for Evidence focuses on specifically understanding what drives the current commercial case for investment in cyber security, as detailed below. We therefore welcome input from organisations that influence and set market expectations, who include but are not limited to membership bodies, consultancies, auditors, insurers, investors, corporate and risk governance bodies, regulators and other regulatory bodies such as professional associations. However, submissions are not limited to these organisations and we encourage submissions from all types of organisations and sectors.

Please take this opportunity to shape our future work by submitting your input online or by emailing your responses to the questions in this consultation to: cyber-review@culture.gov.uk, preferably in Word format. We recommend reading this document in full before completing the online questionnaire.

When you are ready to submit your response, please follow the survey instructions. Once submitted, you will no longer have access to your response. Partial responses will be recorded and included in the analysis. If you wish your partial response to be deleted and not included in the analysis, please email cyber-review@culture.gov.uk. Please note that in doing so, we may require you to provide us with some of your responses to the survey (identifying information), e.g. your organisation's name, to ensure the correct response is removed.

If you are unable to submit via email you can post your response to Cyber Security Incentives and Regulation team, DCMS, Room 4.47, 100 Parliament Street, Westminster, London, SW1A 2BQ. If you are responding by email or in writing, please clarify:

- If you are responding on behalf of an organisation or in a personal capacity;
- Which questions you are answering (there is no need to respond to all of the questions if they are not all relevant to you);
- Whether you are willing to be contacted (if so, please provide contact details); and
- Whether you prefer for your response to remain confidential and non-attributable (if so, please specify).

We would also welcome any information, studies, reviews, statistics, grey literature, measures or metrics which you feel are relevant to the development of incentives and

regulations for UK cyber security. Please send these via email to cyber-review@culture.gov.uk. Please do not provide responses that heavily reference existing Government surveys such as the Cyber Breaches Survey and the FTSE 350 Cyber Governance Health Check. If the documents you send relate particularly to any of our individual questions, please state this in your response.

If you have any issues submitting evidence in the above formats, or any questions, please contact us at cyber-review@culture.gov.uk.

This Call for Evidence will close at 23:59 on Friday 20 December 2019. A summary of the evidence gathered will be published as part of the formal, public consultation of the Cyber Security Incentives and Regulation review in 2020.

# 3. Effective cyber risk management

Recent high profile cyber incidents and data breaches, such as those experienced recently by British Airways and Marriott International, or 2017's Wannacry cyber incident, highlight the extensive impact that cyber attacks pose to both individual organisations and to the UK economy and national security. Following these attacks, the Information Commissioner's Office (ICO) announced that it intends to impose fines of £183 and £99 million for breaches of data protection law. Yet these fines are just one aspect of the potential impact experienced by organisations when they suffer a cyber attack.

At an economy-wide scale, the 2017 Wannacry cyber incident highlighted the potential breadth of impact of cyber attacks, affecting one third of hospital trusts, with over 19,000 appointments cancelled.[4] Cyber incidents thereby increasingly pose risks to the growth of the UK economy (being hindered by the collective costs of cyber attacks on organisations of up to £27bn annually, and an opportunity loss due to a lack of trust in technology solutions) and potential harm to individuals and society more broadly.[5]

While there is currently no standardised definition and approach to effective risk management of cyber threats for organisations of all sizes and sectors, the NCSC have developed guiding principles and good practice, outlined in:

- Advice and guidance, particularly the Board Toolkit and the Small Business Guide;
- GDPR security outcomes;
- The Cyber Assessment Framework (CAF) and CAF Guidance; and
- Accreditation or certification products such as Cyber Essentials.

These pieces of guidance emphasise the importance of a spectrum of risk management mitigation activities. Given the vast majority of organisations in the UK today rely on digital technology to function, cyber risk management must be integrated into operational resilience and business continuity risk management. The guidance and advice issued to date therefore covers not only technical security measures but also practices including governance processes and organisational culture.

Despite improvements in cyber security practices and behaviours, the *Cyber Security Breaches Survey* and *FTSE 350 Cyber Governance Health Check* show that many organisations, large and small, are still not taking the necessary steps within their operational risk management to protect against cyber threats and prepare themselves for cyber incidents. In 2018, only around 60 percent of organisations took actions to identify cyber security risks to their organisation.[6] Nearly one in two FTSE 350 companies,

[4] National Audit Office, Investigation: WannaCry cyber attack and the NHS 2018
[5] Home Office, Understanding the Costs of Cyber Crime 2018
[6] DCMS, Cyber Security Breaches Survey 2019

furthermore, are led by Boards that still lack a comprehensive understanding of their critical information, assets and systems.[7]

Part of the barrier to investing in cyber risk mitigation lies with cyber security being viewed as an IT-specific issue and an objective in itself, rather than an enabler of business continuity and operational resilience. As an objective in itself, cyber security offers little commercial incentive. However, as an essential means of protecting personal data, intellectual property, online transactions or the technologies exploited to implement innovative business models, it is an enabler of the everyday operations of most businesses today. Seen as such, cyber security becomes a business management challenge, which requires a strategic and whole-of-organisation approach.

Boards and senior leaders therefore play a critical role in determining how cyber security is integrated across all business operations through informed decision making and better targeted investments. Alongside Boards, other organisations, including the investment community, insurers, audit firms and consultancies amongst others, have a critical role across the economy in holding organisations to account, and in doing so, and stimulating an improved appreciation of the importance of appropriate  risk management practices.

Without additional incentives and regulation to encourage improved practices, the current resources and guidance tools are likely not sufficient to realising the full integration of cyber mitigations into operational risk management across the UK economy. The I&R Review will therefore assess how government should intervene directly without placing unnecessary burdens on business, as well as support and stimulate industry, to help to address barriers to effective cyber risk management.

[7] DCMS, FTSE 350 Cyber Governance Health Check 2018

# 4. Questions

This Call for Evidence seeks evidence in relation to the following four categories:

- Barriers to effective cyber risk management;
- Commercial barriers and incentives for investing in cyber security;
- Access to the right information for effective cyber risk management; and
- Areas of focus for future policy and regulatory interventions.

You are not required to respond to every question should they not all be of relevance to your submission.

## Section 1: Barriers to effective cyber risk management

Through research and engagement undertaken to date, DCMS believes the main barriers to organisations undertaking effective cyber risk management to be three-fold:

### Barrier 1 - Inability

- Even where organisations are engaged and willing to undertake cyber risk management, there exists for some organisations an inability to act which can be caused by, but is not limited to:
    - Not knowing how to protect themselves and others from the harm caused by cyber incidents. Organisations may not fully understand the risks they face or which of the numerous tools and frameworks are appropriate to manage their cyber risk.
    - Lacking the capability to effectively manage cyber risk, including not having adequate technical expertise or access to sufficiently trained or skilled staff; and
    - Lacking the capacity, including limited financial resources, to access specialised services and products.

- Government efforts to date which have focused on improving the capability of UK organisations, have done so predominantly through voluntary support measures, including, but not limited to:
    - Guidance, communications campaigns such as Cyber Aware, and targeted advice, working with priority groups and sectors across the economy and society, and increased overall industry engagement on cyber security.
    - Programmes of investment that support the growth of the UK cyber security industry and help support emerging and innovative cyber security companies identify, develop and commercialise technology solutions.

- Programmes of work to develop cyber skills through strengthening and developing a pipeline of diverse talent for the UK's cyber security workforce, setting a vision through the *Cyber Security Skills Strategy* and establishing a new UK Cyber Security Council to progress a coherent and world-leading cyber security profession.

## Barrier 2 - Complexity and insecurity of the digital environment

- The digital environment within which many organisations operate has the potential to further compound existing inability to implement effective cyber risk management on the basis of its:
  - **Insecurity:** many elements of the digital environment are not secure by design, thus creating a wide range of vulnerabilities and risks to mitigate; and
  - **Complexity:** many organisations are also subject to risks resulting from high levels of interconnectivity with other organisations, resulting in increasing levels of dependency on others' cyber risk management.

- Current government initiatives exist in this space, and will remain a focal point of future intervention where there is potential to have industrial scale impact on risk reduction. These currently include:
  - The *Active Cyber Defence* programme, which seeks to reduce the harm from unsophisticated cyber attacks through a number of services such as making websites less attractive targets, helping public sector organisations take control of their email and preventing access to known malicious domains, and finding malicious sites and notifying the host or owner to get them removed;
  - Ensuring Internet of Things devices are secure by design and embedding standards more widely, such as the 2018 DCMS *Code of Practice for Consumer IoT Security* and ETSI *Technical Specification 103 645* published this year.

## Barrier 3 - Lack of a strong commercial rationale

- The third barrier to effective cyber risk management, and focus of this Call for Evidence, is categorised as the lack of a strong commercial rationale to stimulate investment in cyber risk management. We believe that this is due to:
  - Organisations finding it difficult to demonstrate compelling cases for return on investment on cyber security products, services and mitigation activities, particularly when often drawing on inadequate or hypothetical information to make these cases (as outlined in section 3 below);
  - Market drivers that could normalise investment in cyber security across the economy and lead companies to feel compelled to take up effective cyber risk management, such as strong consumer pressure and competitive advantage, have not yet formed in many sectors or across the economy as a whole; and
  - Cyber security often being perceived as an end in itself rather than a fundamental enabler of business operations, as mentioned above.

- Whilst 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 digital insecurities. Less explicit focus has been placed on exploring and addressing commercial rationales for investment in cyber security. The following sections of this Call for Evidence and majority of questions therefore focus on this third barrier: inviting evidence on potential reasons for whether and why there may exist a lack of strong **commercial rationale**, how this barrier can be addressed, and what can be done to increasingly normalise effective cyber risk management across the economy.

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?
    a. Barrier 1 - Inability *Open response*
    b. Barrier 2 - Complexity and insecurity of the digital environment *Open response*

# Section 2: Commercial barriers and incentives for investing in effective cyber risk management

When making cyber security investment decisions, it is rational for organisations to estimate the actual costs of investing and balance these against the potential benefits procured or impacts mitigated, informed by an organisation's particular risk appetite.

Although risk and investment decisions are often assessed through 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); and

d. *Mitigation activities and associated costs* (e.g. activities such as the implementation of cyber security controls or training which constitute effective mitigation).

We believe that, in the short to medium term, it is likely there will continue to be a lack of strong commercial rationale for investment in cyber security, as cyber security investment is not underpinned by clear, easily accessible or assured information on the above areas. When understanding the full impact of cyber incidents, an understanding of potential business continuity and operational resilience impacts is critical to a realistic assumption of costs.

A further enabler and driver of investment lies with consumer demand. A PwC survey found that consumers state they will take their business elsewhere if they do not believe an organisation is handling their data responsibly[8]. However, the recovery that businesses generally make after experiencing a cyber attack indicates consumers do not often respond this way. For example, TalkTalk's 2015 cyber attack reportedly resulted in the company losing over 100,000 customers, however, customer churn and new connections normalised again by the start of the following year.[9] From evidence available to date, we believe that consumer pressure is unlikely to drive increased or more effective investment in cyber security risk management over the short to medium term.

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] PwC, Consumer Intelligence Series: Protect.me, 2017
[9] The Guardian, TalkTalk counts costs of cyber-attack, 2016

8. In your experience, which of the following information is used by organisations to inform cyber security investment decisions? *Please select all that apply*
    a. Threat level
    b. Vulnerabilities
    c. Impact or harm of cyber incidents
    d. 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*

# Section 3: Access to the right information for effective cyber risk management

Access to the right information to inform risk management decisions and an ability to communicate effectively to decision makers, such as the board of directors,[10] 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 operations, potentially resulting in either under- or over-investment[11].

Through our research and engagement to date, we have identified three information-based issues:

- Some organisations often either do not draw on, find it difficult to engage with, or do not invest in information about **cyber threat** and their exposure.
- 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 customer base loss).[12]
- 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.

[10] FTSE 350 Cyber Governance Health Check 2018
[11] The Cyber Breaches Survey 2019 findings highlight a very high variance in organisations spending estimates which indicates that organisations are either underestimating or overestimating their spending.
[12] For example, only 16% of FTSE 350 companies report that their board has a comprehensive understanding of the impact of loss or disruption associated with cyber threats.

The complexity of organisations connected through supply chains further exacerbates the information failures outlined. The business operations of one organisation are increasingly dependent on others in their supply chain. Organisations struggle to effectively manage cyber risk in their supply chains as both vulnerabilities and mitigations in the chain of connected organisations are not known or understood, making it difficult for a business to determine its own true risk exposure.

10. How much of a barrier do you think each of the below issues are to organisations in managing their cyber risk effectively?
    a. Businesses do not have access to 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 make better 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*

# Section 4: Future policy and regulatory interventions

Future solutions to normalise investment in cyber security across the UK economy could focus on generating more useful information to inform cyber risk management decisions and investment, such as through the development of an **assured or standardised approach to defining and assessing** an agreed definition of effective cyber risk management or the cost of a cyber incident.

Once standardised information is created, the use of existing market processes and levers (for example, statutory audit or the use of cyber insurance) to assess, validate and assure this information could ensure it is **transparent, accessible and trusted.**

A revision to existing market processes and levers, however, might never fully address the lack of a return on investment for some types of organisations, where investment in cyber risk management is not a commercially beneficial choice. However, in cases where improved cyber risk management is required to protect the broader economy and society from harm, we may seek to consider the broader range of government interventions available to compel certain sectors or types of organisations to invest more in effective cyber risk management.

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 additional solutions 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 an 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 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*

# Section 5: Demographic questions

22. Are you responding as an individual or on behalf of an organisation?
    a. Individual
    b. Organisation

23. [if individual] Which one of the following statements best describes you?
    a. Cyber Security professional
    b. Employer of cyber security professionals or consumer of services provided by a cyber security professional
    c. Professional in another sector
    d. Academic
    e. Student
    f. Interested in a career in cyber security
    g. Interested member of the general public
    h. Other Free text

24. [if organisation] Which one of the following statements best describes your organisation?
    a. Organisation that employs, contracts or uses cyber security professionals
    b. Cyber security training provider and or certification/qualification provider
    c. A cyber security professional body
    d. Other form of cyber security professional organisation
    e. An academic or educational institution
    f. Organisation with an interest in cyber security
    g. Non-cyber security specific professional body or trade organisation with an interest in cyber security
    h. Other Free text

25. [if organisation] Which one of the following best describes the sector of your organisation?

a. Agriculture, forestry & fishing
b. Production
c. Construction
d. Wholesale and retail; repair of motor vehicles
e. Transport & Storage (inc. postal)
f. Accommodation & food services
g. Information & communication
h. Finance & insurance
i. Property
j. Professional, scientific & technical
k. Business administration & support services
l. Public administration & defence
m. Education
n. Health
o. Arts, entertainment, recreation
p. Other services

26. [if organisation] Including yourself, how many people work for your organisation across the UK as a whole? Please estimate if you are unsure.
    a. Under 10
    b. 10–49
    c. 50–249
    d. 250–999
    e. 1,000 or more

27. [if organisation] What is the name of the organisation you are responding on behalf of? Free text

28. Are you happy to be contacted to discuss your response and supporting evidence? [YES/NO]

29. [f yes] Please provide a contact name and email address below.

# 5. Privacy Notice

The following is to explain your rights and give you the information you are entitled to under the Data Protection Act 2018 and the General Data Protection Regulation ("the Data Protection Legislation"). This notice only refers to your personal data (e.g. your name, email address, and anything that could be used to identify you personally) not the content of your response to the survey.

## 1. The identity of the data controller and contact details of our Data Protection Officer

The Department for Digital, Culture, Media and Sport ("DCMS") is the data controller. The Data Protection Officer can be contacted at dcmsdataprotection@culture.gov.uk.

You can visit the DCMS website to find out more about how DCMS uses and protects your information.

## 2. Why we are collecting your personal data

Your personal data is being collected as an essential part of the Call for Evidence process, so that we can contact you regarding your response and for statistical purposes such as to ensure individuals cannot complete the survey more than once.

## 3. Our legal basis for processing your personal data

The Data Protection Legislation states that, as a government department, the department may process personal data as necessary for the effective performance of a task carried out in the public interest. i.e. a Call for Evidence.

## 4. With whom we will be sharing your personal data

Copies of responses may be published after the survey closes. If we do so, we will ensure that neither you nor the organisation you represent are identifiable, and any responses used to illustrate findings will be anonymised.

Qualtrics is the online survey platform used to conduct this survey. They will store the data in accordance with DCMS instructions and their privacy policy can be found here: https://www.qualtrics.com/privacy-statement/

If you want the information that you provide to be treated as confidential, please be aware that, under the Freedom of Information Act (FOIA), there is statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this, it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information, we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.

## 5. For how long we will keep your personal data, or criteria used to determine the retention period.

Your personal data will be held for two years after the survey is closed. This is so that the department is able to contact you regarding the result of the survey following analysis of the responses.

## 6. Your rights, e.g. access, rectification, erasure

The data we are collecting is your personal data, and you have considerable say over what happens to it. You have the right:

- to see what data we have about you
- to ask us to stop using your data, but keep it on record
- to have all or some of your data deleted or corrected
- to lodge a complaint with the independent Information Commissioner if you think we are not handling your data fairly or in accordance with the law.

You can contact the ICO at https://ico.org.uk/, or telephone 0303 123 1113. ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

## 7. Your personal data will not be sent overseas.

8. Your personal data will not be used for any automated decision making.

9. Your personal data will be stored in a secure Government IT system.

# Annex: List of 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?<br>a. Barrier 1 - Inability *Open response*<br>b. 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.<br>*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*<br>● Threat level<br>● Vulnerabilities<br>● Impact or harm of cyber incidents<br>● 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.<br>● Threat level<br>● Vulnerabilities<br>● Impact or harm of cyber incidents<br>● Mitigation activities and associated costs<br>*Open response* |
| 10. How much of a barrier do you think each of the below issues are to organisations managing their cyber risk effectively?<br>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<br>c. There is no agreed definition of effective risk management<br>*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*<br>a.What 'good' looks like and how effective businesses are at managing their cyber risk<br>b.The impact (costs) of a cyber incident<br>c. Threat identification<br>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* |