Cyber Security – testing mechanisms for change

A research report prepared by TNS BMRB for DCMS

September 2016

TNS BMRB
DCMS Cyber Essentials Scheme

JN260136173

Contents

1. Executive Summary

Cyber crime is a growing threat to UK businesses of all sizes, as well as the public and Government. Businesses can incur a range of costs from a cyber attack including financial costs and reputational damage. The government has introduced measures to help businesses protect themselves against cyber crime. Previous research has shown that there are numerous barriers to positive behaviour change in this area and previous efforts have often not been successful. DCMS is working to develop further measures to enable and encourage businesses to take action to protect themselves against this growing threat.

DCMS commissioned TNS BMRB to conduct research to explore effective mechanisms for increasing business action on cyber security. Specifically, this research tested likely business responses to the introduction of five possible options DCMS are currently considering among other possibilities: (1) mandatory breach reporting and reduced fines for those who have followed approved codes; (2) mandatory cyber health checks; (3a) the requirement to include cyber security risks in Annual Reports (large businesses); (3b) the requirement for businesses to publish information on their website about cyber security risk management (SMEs); and (4) reductions in cyber security insurance premiums for those who have advised requirements in place. The research explores businesses views on the likely impact and effectiveness of these five options.

Qualitative research was conducted with 30 businesses, comprising of 20 tele depths and 10 face to face interviews each lasting 45-60 minutes. The sample included 6 large, 10 medium and 14 small and micro businesses. Businesses were recruited across a range of levels of engagement with cyber security, attitude to risk, and confidence in this area. The findings on barriers and facilitators to behaviour change support those reported in an earlier phase of this research, evaluating the government's Cyber Essentials scheme.[1]

1.1. Driving behaviour change

This research suggests that an approach which combines support and penalties could serve as a stronger call to action and be more likely to drive behaviour change than pursuing these approaches in isolation or approaches with deferred benefits or which are seen only as burdensome 'tick box' exercises. Businesses tended to be aware of threat of cyber crime and therefore responded well to options which encouraged improving protection measures in practice. Businesses were asked which of the options was most likely to persuade them to take greater action to tackle cyber threats. No clear single option emerged as being most likely to drive action. Businesses often chose a variety of combinations and were able to express reasons for and against why they thought each would be effective. However, overall, mandatory breach reporting and reduced fines (option 1) and the mandatory health check (option 2) were seen as the most likely to be effective overall. We note that whilst a similar number of businesses chose these two options in the prioritisation exercise, they were not always chosen in combination.

[1] In 2016 TNS BMRB conducted an evaluation of the Cyber Essentials scheme – a scheme designed to help businesses protect themselves from basic cyber threats.

Business' detailed responses to each of the options suggest that a pincer movement created by combining the two most popular options, the mandatory breach reporting and reduced fines and mandatory health check, could be the most effective approach to changing behaviour. Combining these two creates a carrot and stick approach. The health check actively creates the opportunity to make changes and offers support and guidance to assist with this, whilst the mandatory breach reporting and fines present penalties for those who do not take this up. The health check could be presented as a way to support businesses to make changes to enable them to access the reduced fines. Meanwhile the annual and website reporting and reduced insurance premiums served as weaker drivers of action.

Businesses generally reacted positively to the health check and perceived it to be potentially helpful and supportive. It is important to understand this finding within the wider context of business' response to the threat of cyber crime and understanding of the solutions available. As was found in the evaluation of the Cyber Essentials Scheme conducted by TNS BMRB, cyber crime and security is an area which can be perceived to be scary and complicated and is one where businesses can lack knowledge and confidence and do not know who to trust. A mandatory government health check was seen to be able to provide welcome reliable evidence and advice. Being able to also publish their health check score could also differentiate businesses and give customers confidence.

Meanwhile, whilst tending to report that it would drive action, businesses generally reacted negatively and fearfully to the proposal for mandatory breach reporting and increased fines. Businesses tended not to be aware of the current potential level of fines and increasing them (up from the current £500,000) was seen to be punitive and scary, and potentially able to close down SMEs. Businesses were also concerned about the reputational risks associated with mandatory breach reporting (i.e. losing customers). However, these penalties served as a strong call to action with businesses reporting that they would be forced to act quickly in response. Businesses tended to say that they thought there should be no fines rather than reduced fines for those who had approved codes in place.

A small number of businesses in the sample expressed a preference for the reduced insurance premiums. This option was sometimes received positively because, like the health check, it was seen to add value to the business rather than just creating administrative burden or financial cost. This option has the potential to save businesses money that already have cyber insurance and protection measures in place. Whilst some businesses expressed a preference for this option, it served as a weak call to action. This preference tended to be driven by the opportunity to save money rather than to improve cyber security measures. However this option was less popular than options 1 and 2 because there are too many unknowns (e.g. the cost of cyber insurance, the level of reduction, and what the requirements would entail) and the option's credibility was negatively affected by cynicism about the insurance industry more widely.

The options for annual and website reporting were widely seen to serve as weak calls to action. They were perceived to be bureaucratic and to introduce unwelcome administrative burden which would simultaneously be less likely to drive real change. Businesses saw these as box ticking exercises which they would want to complete as quickly as possible rather than an opportunity to protect their business, and there were risks reported around the potential use of templates.

1.2. Common principles

Despite mixed views about the individual options and a variety of views on which option would be most effective, a set of common principles emerged. These factors were seen to be able to encourage businesses to review their protection measures and drive change:

- Mandatory options were a stronger call to action.
- Combining options was seen as likely to be more effective.
- The level of fines cited was perceived to be ‘scary’ – fines and reductions served as a strong call to action. Businesses expected to receive no fine if they had followed approved codes.
- There is currently low awareness of the potential level of fines – raising awareness of current and future fine levels could drive change.
- Risk to reputation by making information (scores or breaches) public was a strong call to action.
- Businesses responded positively to options which offered them support and advice to review their systems and make changes.
- Initiatives which added value to the business itself (through advice, savings, financial incentives, or the opportunity for differentiation) were viewed positively.
- Making high level scores available to customers / investors which could differentiate businesses in their marketplace was received positively - however businesses wanted to avoid making too much information or detail public which could be used by competitors or cyber criminals.
- Options viewed as bureaucratic or imposing a heavy administrative burden were off putting.
- Businesses were sceptical about the effectiveness of options where templates could be used to satisfice and which were seen to lack oversight.

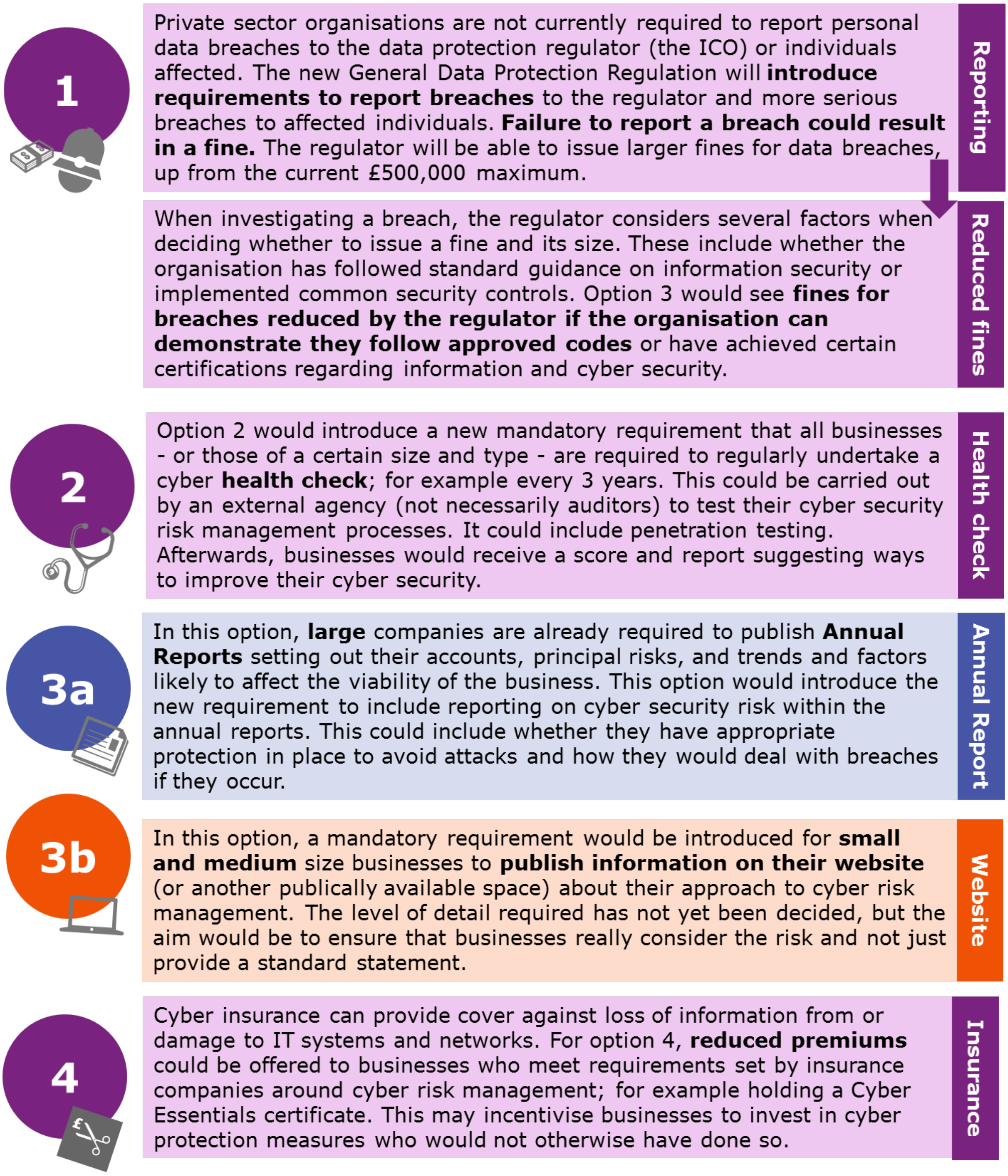
2. Introduction

2.1. Background and options

Cyber crime is a growing threat to UK businesses of all sizes, as well as the public and Government. The 2016 Cyber Security Breaches Survey reported that 24% of all businesses and 65% of large businesses experienced a breach in the last year.[2] Businesses can incur financial costs, damage to systems and loss of data, lose time, and suffer reputational damage from an attack. The government has already introduced a range of measures to protect UK businesses from cyber threats[3], including the Cyber Essentials Scheme evaluated by TNS BMRB in early 2016[4]. The evaluation supports findings from other research that convincing businesses to take action against cyber crime is not easy and recent efforts to improve cyber security practices among businesses have often not been successful.[5] Previous research has identified numerous barriers to positive behaviour change. Almost half of UK businesses have not undertaken any action in the last 12 months to identify cyber security risks, with the proportion increasing amongst micro businesses.[6]

DCMS is reviewing further measures that encourage businesses to protect themselves against the growing threat of cyber crime. This research explored businesses responses to five potential mechanisms, which DCMS is considering among other possibilities, to increase business action on cyber security. The research particularly focused on impact and effectiveness of each of the five options outlined below in Figure 2.1. Options 1, 2 and 4 were tested with all businesses in the sample. Option 3a was only tested with large businesses (250+ employees) and Option 3b with small and medium businesses (1-249 employees). The options take a range of approaches to changing behaviour, including regulatory change and the introduction of penalties and incentives.

[2] Ipsos Mori, Cyber Security Breaches Survey 2016.
[3] https://www.gov.uk/government/news/chancellor-sets-out-vision-to-protect-britain-against-cyber-threat-in-gchq-speech
[4] Cyber Essentials Scheme – process evaluation and communications testing (July 2016, TNS BMRB)
[5] Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Maria Bada , Angela M. Sasse and Jason R.C. Nurse 2015
[6] Ipsos Mori, Cyber Security Breaches Survey 2016. 51% of all businesses had taken some form of action to identify cyber security risks in the last 12 months (such as regular health checks, risk assessments or internal audits); decreasing to 42% amongst micro businesses.



1

Reporting

Private sector organisations are not currently required to report personal data breaches to the data protection regulator (the ICO) or individuals affected. The new General Data Protection Regulation will **introduce requirements to report breaches** to the regulator and more serious breaches to affected individuals. **Failure to report a breach could result in a fine.** The regulator will be able to issue larger fines for data breaches, up from the current £500,000 maximum.

Reduced fines

When investigating a breach, the regulator considers several factors when deciding whether to issue a fine and its size. These include whether the organisation has followed standard guidance on information security or implemented common security controls. Option 3 would see **fines for breaches reduced by the regulator if the organisation can demonstrate they follow approved codes** or have achieved certain certifications regarding information and cyber security.

2

Health check

Option 2 would introduce a new mandatory requirement that all businesses - or those of a certain size and type - are required to regularly undertake a cyber **health check**; for example every 3 years. This could be carried out by an external agency (not necessarily auditors) to test their cyber security risk management processes. It could include penetration testing. Afterwards, businesses would receive a score and report suggesting ways to improve their cyber security.

3a

Annual Report

In this option, **large** companies are already required to publish **Annual Reports** setting out their accounts, principal risks, and trends and factors likely to affect the viability of the business. This option would introduce the new requirement to include reporting on cyber security risk within the annual reports. This could include whether they have appropriate protection in place to avoid attacks and how they would deal with breaches if they occur.

3b

Website

In this option, a mandatory requirement would be introduced for **small and medium** size businesses to **publish information on their website** (or another publically available space) about their approach to cyber risk management. The level of detail required has not yet been decided, but the aim would be to ensure that businesses really consider the risk and not just provide a standard statement.

4

Insurance

Cyber insurance can provide cover against loss of information from or damage to IT systems and networks. For option 4, **reduced premiums** could be offered to businesses who meet requirements set by insurance companies around cyber risk management; for example holding a Cyber Essentials certificate. This may incentivise businesses to invest in cyber protection measures who would not otherwise have done so.

Figure 2.1: Options for testing

2.2. Objectives

DCMS commissioned TNS BMRB to conduct research to explore effective mechanisms for increasing business action on cyber security, by testing businesses' likely responses to five possible options including regulatory change, the introduction of incentives, and other interventions. Specifically, the objectives of this research were to:

- Determine the **likely impact** on businesses, and potential scale of impact;
- Understand any **practical difficulties** with the options tested;

- Uncover any **unintended consequences**;
- Understand whether (and which) incentives are **likely to persuade** businesses to take (greater) action to tackle cyber threats.

2.3. Method

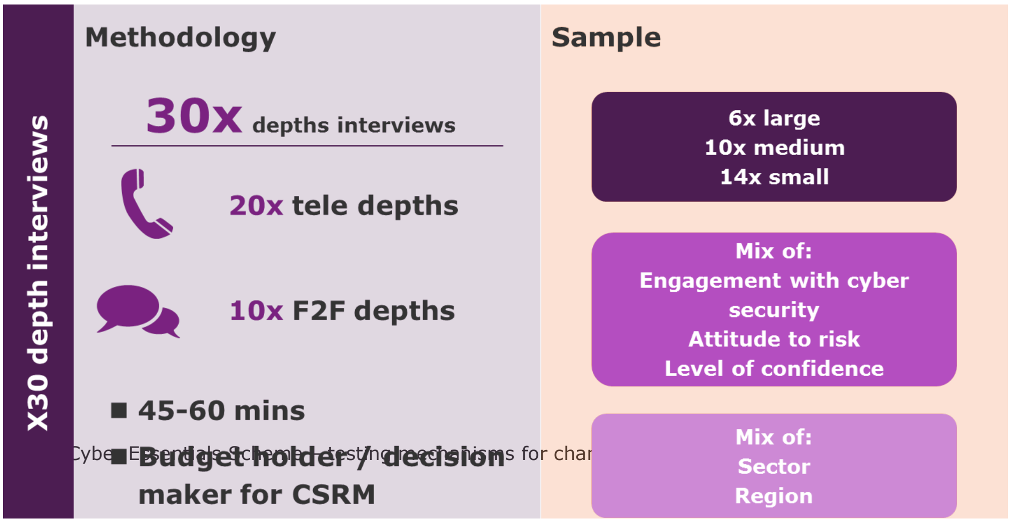
A qualitative approach was taken to address the research objectives, summarised in Figure 2.2 below. Thirty depth interviews were conducted with businesses of a range of sizes across the UK. This included 20 tele depths and 10 face to face interviews, each lasting 45-60 minutes. Most interviews were conducted via telephone in order to minimise burden for busy individuals, and 10 were conducted face to face with larger businesses. Interviews were conducted with the budget holder and decision maker for cyber security risk management in the business. This tended to be the CEO or MD in micro and small businesses, finance director in medium sized businesses, and finance director or risk manager in large businesses. Respondents were offered the opportunity for an IT or information security manager or other appropriate person to join the interview if they felt someone else could help provide more detailed information, and this was taken up in one instance.

The interviews were structured around the option testing. First, respondents provided some background about the business and their decision making processes for cyber security risk management (CSRM). They then described their attitude towards cyber crime and their current risk management strategy before exploring spontaneous facilitators and barriers to change. The bulk of the interview focused on testing respondents' reaction to each of the five options. The stimulus material was read out by the researcher who then probed on overall response; how the business would respond and any barriers or challenges raised; anticipated cost and impact on the business; how effective they thought the option would be; and whether the respondent had any suggestions for improvements. A prioritisation exercise was then conducted, asking respondents to compare the options and assess which they thought would be most effective in encouraging them to review and improve their cyber security protection measures. The full topic guide is provided in Appendix 6.2.

2.4. Sample

Respondents were recruited using free find methods. A range of business sizes were recruited to ensure a range of views was considered. This included 6 large businesses (250+ employees), 10 medium businesses (50-249 employees) and 14 small and micro businesses (1-49 employees). Businesses were recruited across a range of levels of engagement with cyber security, attitude to risk, and confidence in making decisions in this area because these factors were found to be relevant to behaviour in the evaluation of the Cyber Essentials Scheme. Businesses from a range of sectors and regions were recruited to include a variety of experiences. Respondents were given a £60 incentive to thank them for their time. The full break down of the achieved sample can be found in Appendix 6.1.

Figure 2.2 Summary of method and sample



2.5. Analysis and reporting

All interviews were recorded using digitally encrypted recorders and the audio was used for analysis. Respondents' responses to each option were charted against key themes for the research objectives and analysed against sub groups. A brainstorm including all members of the research team was conducted. The data was analysed for themes and trends, including the prioritisation exercise. The data was interrogated alongside data from the evaluation of the Cyber Essentials Scheme and the findings from this research regarding behaviour change are consistent with and build upon those from the evaluation.

Verbatim quotes are included to illustrate key findings in the report.

3. The Current State of Play in Cyber Security Risk Management

This chapter explores the current state of play with regards to cyber security risk management (CSRM). Section 3.1 explores businesses' perceptions of the risk cyber crime poses to them before Section 3.2 outlines the range of measures businesses reported currently having in place. Section 3.3 reports on the nature of businesses' decision making processes for CSRM and the implications of this for DCMS. Section 3.4 explores spontaneous facilitators and barriers to change which were reported before the options were introduced. Sections 3.5 reports on businesses' views on the guidance currently available and section 3.6 on their attitude to the proposition to share information about incidents.

The findings in this chapter support those from the evaluation of the Cyber Essentials Scheme. Cyber crime is perceived to be a growing threat, but is not yet seen to be a relevant threat by some businesses. Businesses reported having a range of measures in place and a wide range of monthly spends, with spend on cyber security linked to the perceived level of risk. Decision making processes varied in large and small businesses, but overall they were often siloed and required senior sign off, meaning there are multiple access routes for communications. A range of facilitators and barriers to change were reported. Businesses said experiencing an incident and rising awareness of the risk due to media coverage of incidents drive change, whilst habit, cost and competing priorities act as barriers. Businesses felt that there is currently a lack of accessible guidance available and some were unsure who to trust and where to look for reliable information. There were mixed but strong views about whether businesses would be prepared to share incident information.

3.1. Business perceptions of the risk cyber crime poses

The interviews began by exploring participants' understanding of cyber crime and the risk this poses to their business. This provided key context to help understand what was driving business' responses to the options. Businesses were aware of cyber crime and saw it as a growing threat. However, as was found in the Cyber Essentials Scheme evaluation, despite growing awareness, some businesses did not necessarily perceive cyber crime to be a relevant threat to them.

> *"We've never had any attempt to get information off us. I don't think the information we hold is anything valuable for anyone …it's not a massive thing for us." (Automotive, 1-49)*

This was particularly the case for some smaller businesses and micro businesses who thought larger businesses were more likely to be the target for cyber crime. Some businesses perceived their sector to be low risk, seeing the threat as more relevant to sectors such as banking and finance. Some businesses did not see cyber crime as relevant because they; (a) did not perceive themselves to be an online business (usually meaning they did not primarily trade online despite having a web presence) or (b) did not perceive themselves to hold large quantities of personal information (PI) (despite holding at least staff information and presumably some customer and client information). As in the Cyber Essentials Scheme evaluation, some respondents assumed other people were dealing with the threat of cyber crime. Smaller businesses could assume their bank was dealing with the risk whilst medium and large businesses could defer responsibility to their IT teams without necessarily checking the risk was being managed.

> *"We're quite low risk…we're a small company…we have thousands of invoices…that information isn't really useful to anybody…I can't see why anybody would want to get hold of that." (Logistics, 1-49)*

> *"It has crossed our minds because we do a fair bit of orders and things like that but we probably expect Global payments to contact us because they have all the information about card details." (Retail, 1-49)*

However this was not universal and cyber crime was a high priority for some of the businesses in the sample. In particular this included businesses who had experienced an attack or attempted attacks (across all three business size groups), larger businesses, service providers, those trading primarily online, those who perceived themselves to hold large quantities of PI or sensitive commercial data, and higher risk sectors (e.g. e-commerce, consultancy, healthcare and recruitment and importing). It was also a higher priority for businesses making regular international transactions, those with greater knowledge about the topic and higher awareness of media coverage of incidents. Increased media coverage of incidents and their implications was driving concern about the reputational damage cyber attacks can cause for some businesses.

> *"If we have a problem with data being stolen or misplaced, then that would obviously have a negative impact on our brand and reputation. Customers may decide not to use us." (Automotive, 250+)*

3.2. Current protection measures in place

Participants were asked to describe the protection measures they currently have in place. Businesses in the sample reported a range of measures, similar to those reported in the Cyber Essentials Scheme evaluation, and a wide range of spends from £100 to £20,000. Businesses in the sample reported having the following measures in place: anti-virus software, firewalls, passwords, and encryption; ISO certifications; intrusion detection, remote monitoring, anti-hacking software; penetration testing and scans; choosing banks offering protection measures; seeking reviews and advice from consultants; using merchant services including protection measures; and having staff policies in place.

The types of measures businesses have in place differ by their characteristics. Some businesses tended to have greater measures in place. This notably included larger businesses (250+ employees and larger medium size businesses), service providers (e.g. e-commerce, financial services and consultancy), those perceiving themselves to trade primarily online or hold large quantities of PI (e.g. payment information) or commercially sensitive data (e.g. about contracts and suppliers), and higher risk sectors (e.g. finance, logistics and consultancy). These factors could also overlap rather than be in isolation. These businesses tended to have measures such as anti virus software and firewalls, intrusion detection, penetration testing, remote testing, and encryption in place, have policies in place, upgrade regularly, hold relevant accreditations (e.g. ISO) and could have external IT support.

Some types of businesses tended to have fewer and less sophisticated measures in place. Businesses that perceived cyber crime to be a lower risk, smaller and micro businesses, those not perceiving themselves to be an online business or to hold large amounts of PI, and lower risk sectors (e.g. manufacturing, retail and automotive) tended to have fewer measures in place. They also tended to have less sophisticated measures in place; e.g. firewalls and anti virus software but not penetration testing or comprehensive policies and procedures).

Whilst there is growing awareness of the threat cyber crime poses, some businesses lack knowledge about the options available and their relative cost and effectiveness and confidence in choosing between them. This reflects findings from the evaluation of the Cyber Essentials Scheme.

3.3. Decision making processes for cyber security risk management

Participants were asked to describe how decisions about CSRM are made in their business. Processes varied between large and small businesses, but decisions were often siloed, made by a small number of people and required senior sign off. In some businesses (e.g. manufacturing, construction and automotive and those who saw cyber crime as low risk), these decisions were a low priority compared to other more pressing concerns (commonly sales and targets). Decisions were described as tending to be trade off exercises involving the cost of the measures and the potential cost of the risk. Attention paid to cyber security was also constrained by budgets and other priorities. Some respondents reported that the potential impact of measures on sales and customers as well as staff was considered (e.g. where measures were seen to increase burden for staff or customers).

> *"It's that eternal struggle really. Usually what happens I come up with some ideas of where we need to spend money and normally IT is not on that radar to be honest because my focus is on building sales and marketing and all that other stuff..." (Manufacturing, 50-249)*

Large and larger medium businesses more often had a more formalised strategy and review processes in place. Implementation and review tended to be carried out by the IT or compliance team who advised senior staff on this issue. However measures and changes needed to be signed off by the finance director, MD or board. Some participants described how senior staff would sometimes need convincing that measures and changes were necessary and why, and IT staff would need to present their case about why this was necessary for the business, with varying degrees of success. In unsuccessful cases, this could be because senior managers viewed other areas as greater priorities for spend.

Small and smaller medium businesses tended to have fewer measures in place. In these businesses, fewer people were involved in the decision-making and implementation and these could be quite isolated from other aspects of the business. In some small businesses, senior staff with varying levels of knowledge and confidence made the decision (with advice from IT consultants, online tutorials and board members) and implemented the measures. However some small and medium sized businesses outsourced implementation to IT consultants.

These discussions reveal that there are two potential entry routes for organisations wanting to communicate with businesses about cyber security: via senior financial decision makers and implementers (internal IT teams and external IT consultants). It may be helpful for communications be tailored to their interests to maximise effectiveness.

3.4. Spontaneous barriers and facilitators to improving protection measures

Before the option testing, participants were asked for their spontaneous views about what factors and situations might prompt them to consider reviewing and improving their cyber security measures and the barriers to change. A range of facilitators and barriers were reported reflecting those raised and reported in the Cyber Essentials Scheme evaluation.

In terms of facilitators, businesses across all the size groups commonly said that experiencing a damaging attack (e.g. the loss of a website) or regular attack attempts (e.g. phishing emails) would prompt them to review their cyber security measures. However this means that businesses would be leaving it too late until after potentially high costs have been incurred. Some businesses said that changes in the business can prompt review in this area, for example increasing the amount of trade conducted online, installing new systems or upgrading technology (e.g. moving to cloud storage). Businesses also mentioned external stimuli such as tendering and procurement processes and requests for information and standards from clients. Some businesses said that greater awareness of cyber crime and its implications could prompt review (e.g. via media coverage and information about incidents). Information from trusted sources was also seen as a potential driver of change, for example word of mouth about incidents in the sector and advice from trusted or proactive IT consultants. As stated above, large businesses were more likely to have IT and/or risk management teams with cyber security coming under their remit and for reviews to be formally scheduled. Whilst they were more commonly proactive than smaller businesses, larger businesses also reported that an attack would prompt them to review their measures. One respondent also mentioned that statutory changes could drive change.

> *"I don't know anything else that would but if we got attacked over the internet then I'd look at the cyber security, which is probably a little bit like shutting the gate after the horse has bolted." (Business Services, 250+)*

> *"I know as much as I need to know to protect what we have as a business. If we started procuring, making financial transactions online I may have to take it a step further." (Construction, 50-249)*

Businesses also reported a range of factors which can act as barriers to change, which again reflect those found in the Cyber Essentials Scheme evaluation. Habit and culture around cyber security practices (or lack thereof) can be difficult barriers to overcome. In particular this includes an attitude that cyber crime is not relevant or low risk to some business' size, sector or operations. Communications also need to overcome the assumption that someone else (such as banks or IT teams) are dealing with the threat. In order to change behaviour it is important that cyber security is regarded as an important priority that can compete with others in the business, and challenges around resources (namely time and cost) are overcome. A 'block in the chain' can also prevent progress; a business described how one senior manager refused to engage with the issue or listen to advice from other staff as he did not see it as a priority for the business. Changing behaviour in this area also needs to address low awareness of the issue as well as low knowledge and confidence among some businesses about cyber crime and IT more generally as well as protection measures, costs and where to go for help and advice. Some businesses were also concerned that some security measures could create burden for customers and staff and therefore potentially lose the business sales and staff time (e.g. adding requirements to purchasing processes or putting staff policies in place).

> *"We're a pretty laid back company. Things like that aren't brought up particularly unless I bring them up...There are more important things in other people's minds. Day to day running, contracts, winning deals. I think they think you've got an anti-virus system and something blocking someone hacking in and they think that's it. It's OK." (Vehicle Sales, 250+)*

> *"We're conscious of not burdening the team too much … It's trying to keep things, the administration burden as low as possible." (50-249, Construction)*

3.5. Business perceptions of current guidance on cyber security

Businesses were asked for their views on the current guidance and information that is available about CSRM. Businesses reported feeling that there is currently a lack of accessible information available about the risk and solutions. They do not know who to trust and where to look for reliable information.

> *"It's very poor from the banks…very poor from our regulatory bodies…there's a knowledge void." (Law, 250+)*

Businesses reported finding that there is a lack of proactive guidance and information on this topic, particularly regarding best practice and solutions. They felt there was a lack of guidance available from the government and ICO, suggesting that they would consider these to be reliable and welcome sources. Information that was available was often found to be confusing and inaccessible due to the use of technical language and excessive jargon. There was also a particular lack of guidance about the cost and effectiveness of different solutions to help businesses make decisions. Businesses also reported a lack of training available in this area.

> *"It's never really been put under my nose before … I don't know what government guidance there is…I think it's quite poor at the moment." (Healthcare, 50-249)*

Businesses said that they wanted to see more information and guidance available to them about this topic. They wanted to access information from trustworthy sources that is succinct, accessible and jargon free; relevant to their size and sector; and includes information about costs. Businesses thought that it would be useful to have information available during business set up, growth and when they are making changes to systems and technology.

3.6. Attitudes to sharing information about incidents

Businesses were asked whether they would be prepared to share information on cyber attacks with other businesses in their sector. There were mixed and strong views in response to this proposition. Some businesses were enthusiastic about sharing information, particularly large businesses that saw this as potentially useful. Some suggested case studies would be particularly helpful to make consequences more real and suggest appropriate solutions, as was seen in the Cyber Essentials Scheme evaluation. However businesses reported that they would only share within their sector, because they appreciated that this activity could help to protect the sector or industry overall and raise knowledge and awareness about the kinds of attacks and consequences they were at risk of. However businesses tended to say that they would require this to be anonymous and that they would likely only share a low level of detail.

> *"Whilst we are competitors, ultimately we share a common interest in protecting our names and industry and it's better to do it together than individually." (Automotive, 250+)*

Some businesses reacted negatively to this proposition, particularly SMEs. There was particular concern that this could damage their reputation in the industry and among clients or customers. There was also concern that this would alert competitors who could use this information against them. Businesses were concerned about losing customers and clients, as well as potentially suppliers and partners. One business noted that they would not be able to share information due to confidentiality agreements.

“I wouldn't really want anyone to know I'd been breached….don't use that company, they get breaches of security, you know. It would be easy for them not to use your company. It could have a negative effect on your business." (Manufacturing, 1-49)

4. Testing mechanisms for change

This chapter presents the findings from the option testing. Businesses were asked for their overall response and feedback about the feasibility of each mechanism. Findings are presented about the impact and effectiveness of each option and businesses' suggestions for improvements. Section 4.1 reports on businesses' views on which options served as the strongest calls to action. Sections 4.2 – 4.6 report the detailed feedback businesses gave about each of the options in turn.

No single option emerged as being most likely to drive change. However the research found that the mandatory breach reporting and reduced fines (option 1) and mandatory health check (option 2) served as the strongest calls to action and businesses more often reported that these mechanisms would drive them to review and potentially improve their cyber security measures – albeit for different reasons which are described in Section 4.1. Whilst some businesses expressed a preference for reduced cyber insurance premiums (option 4), this served as a weak call to action. The annual and website reporting (option 3) were seen as bureaucratic burdens which added little value to businesses and were the weakest drivers of action.

4.1. Summary of overall responses

After reviewing each of the options in detail, businesses took part in a 'prioritisation' exercise and were asked whether any of the options were likely to persuade them to take greater action to tackle cyber threats. They were asked to compare the relative effectiveness of each and select which they thought would be most likely to encourage change.

No single clear option emerged as most likely to encourage change and respondents commonly struggled to pick one option. Businesses tended to choose a variety of combinations and were able to see strengths and weaknesses in each, and expressed reasons why multiple options would be effective. However overall, as is illustrated in Figure 4.1, mandatory breach reporting and reduced fines (option 1) and the mandatory health check (option 2) emerged as most likely to drive change. These were the two options which businesses saw as the most likely to persuade quick action, albeit for different reasons, across different business sizes and sectors. Whilst similar proportions of businesses in the sample selected these two options in the prioritisation exercise, they were not always chosen in combination (i.e. some respondents choosing option 1 or 2 opted for this in combination with 3 or 4). **We note that whilst these figures are given to indicate a sense of how the sample fell out, these are illustrative qualitative rather than quantitative sample findings and cannot be generalised to the wider business population.**

Figure 4.1 Summary of business' overall responses

Option	Large businesses	Small / medium businesses
#1 Reduced fines	3 🟢	12 🟢
#2 Health check	3 🟢	13 🟢
#3a Annual reporting	1 🔴	
#3b Website reporting		5 🔴
#4 Reduced insurance premiums	2 🟠	7 🟠

(Key: Green = stronger support, Amber = medium support, Red = weak support).

Businesses tended to react negatively to the information about mandatory breach reporting and increased fines. They were commonly unaware of the current level of fines they could face, and were often shocked and scared by these (particularly SMEs). The fines were perceived to be high and punitive and businesses reported that these levels could close the business. Commonly, concerns arose about reputational risks associated with mandatory breach reporting (i.e. loss of customers and clients). However, these types of penalties served as a strong call to action with businesses reporting that they would be forced to act quickly.

> *"The system of the fines. It really scares me. It could have a major impact on your business and we're not talking small fines …that would definitely say this needs to be done and now." (Manufacturing, 1-49)*

Meanwhile, businesses generally reacted positively to the health check, perceiving it to be potentially helpful and to add value to the business by helping them understand and address risks (particularly those with low knowledge and confidence). This should be understood within the wider context described in section 3.1, that some businesses lack knowledge and confidence about cyber security and do not know who to trust for advice. A mandatory government health check was seen to potentially be able to provide welcome reliable evidence and advice.

> *"The health check … that's going to give you the direction…if you've got…an independent report saying you're way behind, you've got to do something." (Hospitality,50-249)*

Annual and website reporting served as weak drivers of change. They were perceived to be bureaucratic and to introduce unwelcome administrative burden which would be unlikely to drive real change. Businesses tended to see these as box ticking exercises to complete as quickly as possible rather than opportunities to engage with the risk of cyber crime (particularly those who saw cyber crime as lower risk). Some businesses expressed a preference for the reduced insurance premiums (particularly those with greater measures in place). This option was sometimes received positively because, like the health check, it could add value by saving the business money. However this mechanism served as a weak call to action because it was non mandatory so could be avoided, and the preference tended to be driven by the opportunity to save money rather than to improve cyber security measures.

The following sections review each of the options in turn, presenting the option as it was introduced to respondents, and assessing the reported feasibility, impact and effectiveness of each.

4.2. Option 1: Mandatory breach reporting and reduced fines

The new General Data Protection Regulation will introduce requirements to report breaches to the regulator and more serious breaches to affected individuals. Failure to report a breach could result in a fine. Fines for breaches could be reduced if the organisation can demonstrate they follow approved codes.

4.2.1. Overall response and feasibility

Overall, the fear of fines and reputational risk from mandatory breach reporting served as strong calls to action for businesses (across all sizes and sectors) to review their security measures. Across all sizes, businesses identified both positives and negatives about this option. The fact that this option was mandatory was viewed positively as it was seen as an opportunity to raise awareness of the importance of protecting data and the imperative to put cyber security measures in place. Large businesses who perceived themselves to hold large quantities of PI particularly felt that the regulatory nature of fines could drive culture change within their business. This is because fear of fines would motivate board members to make cyber security a priority within the business, and therefore invest in cyber security measures.

> *"The more that can be done to bring to people's attention the need to protect data and the sensitivities around it and the importance of it, the better." (Automotive, 250+)*

Amongst SME's, using certifications to potentially reduce fines was seen as an attractive option as they could also be used to differentiate their business within their market by showing clients and customers that they are taking cyber security seriously, particularly in tendering processes. SMEs also highlighted the benefits of mandatory breach reporting, as they felt it could raise awareness of the level and types of cyber threats among businesses of the same size and sector. In turn, SMEs felt this would lead to an improved understanding of the threats and how best to protect themselves. Mandatory breach reporting was also perceived to be beneficial to customers as businesses understood they have a right to be informed if a breach has taken place which involves their data.

> *"As much reporting as your business can give is only going to be beneficial to yours and other businesses." (Import/ Export, 50-249)*

However mandatory breach reporting to individuals affected raised concerns for large businesses for fear that their customers could lose confidence in them. This was an added concern for businesses that outsource their IT, as an attack on their external supplier's systems could lead to a loss of customer confidence in them, particularly if they display the supplier's logo on their website. This raised questions and concerns about who would take responsibility for reporting and paying the fines, and whether this would be the business or the IT supplier.

> *"We still have a big ecommerce by [IT Provider] and a logo on our website. If our customers see that they're going to lose confidence and think I'm not shopping there." (Retail, 250+)*

SMEs raised concern and questioned whether they could get a fine for non-reporting if they were not immediately aware that they had been breached. Therefore questions were raised around how this option would be enforced and regulated. Some respondents also questioned why businesses would be punished for the crimes cyber criminals commit and saw this as unfair. It was seen as particularly punitive and unfair when fines, even reduced fines, would be given to businesses that have put measures in place. Businesses wanted to see the government taking action against cyber criminals as well, rather than the burden being on them. Other concerns were raised around IT consultants charging more to support businesses with their cyber security as a result of this option becoming mandatory, because businesses who lack IT knowledge and confidence would need their help and support to comply.

> *"If I don't report it, how would they know that I've been breached? How can it be policed?" (Business Services, 1-49)*

4.2.2. Cost and impact

Costs were largely seen in terms of the fines themselves which were perceived to be high and scary for businesses, but also in terms of the effects of reputational damage such as loss of sales. Businesses felt that fines should be proportionate to the nature and circumstances of the cyber-attack as well as the size and turnover of the business (particularly those who saw cyber crime as a higher risk). Considerations of costs also included the price of additional measures and implementing and maintaining these. This option was considered to be potentially more expensive than others for SMEs, as the strong call to action meant budgets would be affected as they would invest more money and time in implementing cyber security measures. Those with lower IT knowledge and confidence would also have to pay for external advice and support. This cost was of greater concern for the micro businesses and sole traders in our sample and they suggested financial support should be provided by the government if this option was to become mandatory.

4.2.3. Effectiveness

Fines, both increased and reduced, were seen to be strong drivers for businesses to take action to review and improve security measures (particularly those with less confidence and fewer measures in place). Large businesses felt this option would only be effective if the government raised awareness about fines, as currently businesses across the sample had little knowledge about current levels and impending changes (particularly among those who saw cyber crime as low risk). Mandatory breach reporting was also a strong driver to action as businesses were concerned about reputational damage, which could have an effect on relationships with clients and consumers and ultimately the business's survival and success (particularly from the service sector). There was some scepticism around how this option would be regulated, and respondents questioned how the ICO would know businesses had been breached. This caused concerns that businesses might hide attacks to escape what were perceived to be high fines.

> *"It would make me act immediately because I want to make sure all my information is protected, covered and I don't want to get fined." (Manufacturing, 1-49)*

> *"How would anyone know you'd been breached? ...How would they know if I didn't tell them?" (Vehicle Sales, 250+)*

4.2.4. Suggestions for improvements

- Many respondents said that fines should not be issued to businesses that have put cyber security measures in place and have followed approved codes, rather than fines just being reduced.
- SMEs would like more advice and clarity around the requirements of approved codes (particularly those with lower confidence).

4.3. Option 2: Health check

In this option, a mandatory requirement would be introduced that all business - or those of a certain size and type – would be required to regularly undertake a cyber health check (e.g. every 3 years).

4.3.1. Overall response and feasibility

Overall, a wide variety of businesses tended to respond positively to this option. They saw the cyber health check as helpful, supportive and a benefit to the business by providing reliable advice and guidance (particularly those with lower confidence and who saw cyber crime as a higher risk). Businesses of all sizes welcomed this option as they could access information, advice and feedback from a trustworthy external agency on how to improve their systems, which was of particular value to businesses that lacked IT knowledge and confidence. Even amongst businesses that had more sophisticated measures in place and those who felt knowledgeable and confident in this area, this option could provide reassurance that the business had sufficient security in place. The outputs from this option (a report and score) were also viewed positively as they could be used as a sales tool particularly in tendering processes to demonstrate to clients and consumers that they are taking cyber security seriously (across business sizes). An additional benefit reported by SMEs was that they could compare their scores with other businesses in their sector to get a sense of where they stand in the market. Businesses generally agreed that due to the fast paced nature of the cyber industry, health checks should happen more frequently than every 3 years to protect against cyber threats.

> *"It would allow you to show some credibility and to be able to demonstrate to your customers that you've gone through this audit, health check process." (Automotive, 250+)*
>
> *"We've never had anything like that done before and would be good to know the results and a score, to have a scan on out servers and systems." (Retail, 1-49)*

However, some businesses raised concerns as they felt this option was not applicable to their business size or sector (particularly smaller businesses, lower risk sectors and those who saw this as a lower risk). This was particularly the case for businesses who did not perceive themselves to hold large quantities of PI and some smaller businesses[7]. Some businesses in the sample did not perceive themselves to hold PI and this could mean they saw cyber crime as less relevant to them which could serve as a key barrier to taking action to protect themselves. This included large and medium businesses who would presumably at least hold details about employees and therefore we infer that some businesses can mistakenly perceive themselves not to hold PI. These businesses implied that they could be resentful if the report or score from the health check was publicised and felt it should only be made public for businesses dealing with large amounts of PI, such as the financial sector.

> *"I would be highly resentful… it's really no one's business so why should it be made public unless you are dealing with public data." (Manufacturing, 250+)*

Large businesses were also concerned about the report or score being made public as the information provided could be an advertisement to cyber criminals. If a business's score was low and the report outlined in detail where they lacked security, this could create opportunities for cyber criminals to attack their systems. SMEs were also concerned that having someone external come in and check their systems could be disruptive and intrusive, particularly if the health check meant shutting down their systems and disrupting work and sales.

4.3.2. Cost and impact

Estimated costs of the health check varied between business sizes. Large businesses estimated that the health check would cost up to approximately £2,000, whereas SMEs estimated the cost to be between £100 - £1,000. Smaller businesses were more likely to expect costs to be in the lower hundreds (£100-300) whereas medium businesses expected to pay more (£500-£1,000). Businesses reported that this option would entail additional costs such as buying new security measures and staff time for implementation.

Micro businesses and sole traders reported this cost as a burden to their budget. Additionally, the businesses who felt they did not hold large amounts of PI and saw cyber crime as lower risk were more negative about the mandatory nature of this option as they didn't see it as relevant to them and were less open to the added costs to their business. However, businesses that hold large amounts of PI and already take cyber security seriously and had more sophisticated measures in place felt that the benefits of the health check could outweigh the costs, particularly if it identified weaknesses in their systems to help protect the business.

Some businesses with lower knowledge and confidence were concerned about and less aware of the cost of external consultants.

4.3.3. Effectiveness

Similar to Option 1, the mandatory nature of the health check was a strong call to action for businesses to improve their cyber security as they would want to ensure they had the correct measures in place before having the health check and receiving a negative score. Publishing the score would serve as a strong call to action. Participants expressed that a report being made public would incentivise immediate action to improve their cyber security measures to avoid a negative report being published which could affect relationships with clients and consumers. Businesses perceived the report itself to potentially be helpful and to be able to drive change, if it gave detailed guidance about areas where the business was at risk and specific advice about how to address this. The report was seen to be particularly useful by respondents who lacked knowledge and confidence in this area and did not know who to trust for advice. The health check report could therefore also drive change after its completion as well as in preparation for the check itself, if it is designed to be accessible and helpful.

> *"If we had to do that we'd make sure that our risk profile was good and we were up to speed with everything and secure and sorted." (Business Services, 250+)*
>
> *"You don't want anything negative about your business. You want people to believe you do everything right...I'd put all my effort into security." (Business Services, 1-49)*

4.3.4. Suggestions for improvements

- If this was to become mandatory, the government should provide clear guidelines about the requirements and process.
- The report should provide detailed feedback and advice to businesses, with next steps and solutions to improve their cyber security, including the cost of these solutions. The report should also be accessible to those with less knowledge.
- A traffic light system was suggested to help businesses prioritise budgets. This could also be used to influence decision makers within the company to spend more money on new measures.
- Smaller businesses would welcome financial help from the government if this became mandatory.
- Bronze, silver or gold certification could help businesses understand what level their cyber security is at and what they need to work towards, as well as helping to differentiate their businesses in their marketplace.
- The cost of the health check should be proportionate to business size, turnover and operations.
- Concerns about the role of consultants and upselling means that their role and requirements would need to be clarified.

4.4. Option 3a: Annual reporting

This option would introduce a new requirement for large businesses to include reporting on cyber security risk within their annual report. This option was only tested with large businesses (250+ employees).

4.4.1. Overall response and feasibility

Overall, large businesses responded negatively to this option and tended to see it as a weak call to action that was unlikely to encourage them to improve their cyber security protection. Large businesses tended to see this mechanism as bureaucratic and to impose unwelcome administrative burden and to provide little added value to the business itself.

Large businesses were able identify a small number of strengths. Some businesses (mainly those who saw themselves as holding large quantities of PI) agreed with the principle that businesses have a responsibility to their customers/clients to demonstrate how they hold their data securely and saw this as a means to do this transparently. Annual reporting has the potential to reassure and attract clients and investors. The report itself was perceived as something that could be useful for tendering processes. Some respondents said that the mandatory nature of the mechanism had the potential to raise awareness of the issue, particularly among senior members of staff, and to drive culture change if changes were required as a result.

> *"It almost forces people then to not ignore the potential problem because you have to report on it." (Retail, 250+)*

However, businesses identified a number of barriers and challenges. Annual reporting was viewed as bureaucratic and to impose unwelcome administrative burden. It tended to be perceived as a box ticking exercise to be completed as quickly as possible. Some respondents implied they would resent this approach because they could see few benefits to businesses themselves (particularly those not perceiving themselves to hold large quantities of PI). Businesses also raised concerns about being required to display too much detail about their security arrangements publically as this information could be used by hackers trying to penetrate the business.

> *"It's a layer of bureaucracy which we don't really need in a business." (Manufacturing, 250+)*

4.4.2. Cost and impact

The costs associated with this option were largely seen in terms of the resource which would be required to produce the statement for the annual report. Businesses assumed there may be some cost associated with time needed to check their measures and price of any new measures which may need to be implemented. Businesses suggested that those who are less knowledgeable may need to pay an external consultant to support this work.

4.4.3. Effectiveness

Large businesses generally perceived this option to be less effective than the others and unlikely to drive changes to security arrangements. This was primarily because the annual reporting requirement was perceived to be a box ticking exercise rather than an opportunity to engage with the topic. They raised concerns about satisficing and thought that businesses would only aim to meet the minimum requirement (particularly those who saw it as a bureaucratic burden). Businesses raised concerns about oversight and questioned who would check the accuracy of the statements businesses were providing and how this would be done. Businesses were also sceptical about whether anyone would actually read the reports, adding to the perception of this option an administrative burden.

> *"I'd draft a very, very bland, one line statement which satisfies the requirement and I would get on with something else as I don't see it as a priority at all." (Automotive, 250+)*

4.4.4. Suggestions for improvements

- The statement could be used for tendering processes to differentiate business when bidding for work which could add value to businesses.

4.5. Option 3b: Website reporting

This option would introduce a new requirement for SMEs to publish information on their website about their approach to cyber risk management. This option was only tested with SMEs (1-249 employees).

4.5.1. Overall response and feasibility

Overall, as with the annual reporting, small and medium size businesses tended to respond negatively to this option, saw it as bureaucratic and of little value to businesses themselves. Whilst it was seen as achievable to SME's, it was often seen to be meaningless and thus unlikely to drive real change.

SME's identified some strengths of this option. Some businesses saw this option as very achievable and assumed it would not cause too much hassle, particularly those who already had measures (and more sophisticated measures) in place and held other certifications (e.g. ISO accreditations). As with annual reporting, some businesses felt that businesses have an obligation to reassure consumers and clients that they are holding their data securely and saw this as a way to provide transparency (mainly those understanding themselves to hold large quantities of PI and those who already had measures in place). Some businesses thought this option could provide valuable reassurance and confidence to customers and help to attract new business.

> *"If the public are buying things off the company, I think it's very good…a lot of people are concerned about buying things online." (Import/ Export, 1-49)*

However, on the whole, businesses perceived website reporting to be bureaucratic and impose an unwelcome administrative burden (or 'red tape') which provided little benefit or added value to the business (particularly those perceiving themselves not to hold PI or trade online). Businesses were sceptical and questioned whether any customers would actually read the statement, as people rarely read T&Cs. Consequently, respondents felt this option would be unable to provide differentiation. Some businesses implied they would resent this option becoming mandatory because they did not see it as relevant to their business, seeing it as relevant to other sectors (e.g. finance and banking).

> *"It's that eternal business versus the government red tape thing isn't it and business has enough red tape to cut through" (Manufacturing, 50-249)*

4.5.2. Cost and impact

The costs associated with this option were largely seen in terms of the time and resource required to write the statement, update the website, and potentially review measures. A small number of businesses noted that there may also be costs for some 'other' businesses with less protection measures in place associated with implementing new measures. For those with less knowledge and confidence, there could be costs for hiring an external consultant to review measures and write the statement. There was some concern among these businesses that consultants could charge higher fees if they knew this was mandatory.

> *"Just to make sure everything's correct, everything's right, I haven't missed anything. I wouldn't want to do it myself. I'd want to get help." (Retail, 1-49)*

4.5.3. Effectiveness

SMEs tended to see this option as less effective than others and as unlikely to drive real change. As with annual reporting, respondents thought that businesses were unlikely to do more than meet the minimum requirement. Businesses also reported that satisficing would be likely if businesses could copy and use a standard template and may not review their measures or take the requirement seriously. As with annual reporting, businesses questioned who would oversee this and check the accuracy of statements and whether customers would read the statements.

> *"It wouldn't mean anything...the very smallest businesses would do the minimum they have to. They would get it done as a statutory requirement, but it's meaningless." (Digital service, 1-49)*

4.5.4. Suggestions for improvements

- Businesses may do more than meet the minimum requirement if it was clear how this requirement was going to be 'policed' and that statements would be checked for accuracy.
- Businesses wanted to see a system that would assign them bronze, silver or gold status to help easily differentiate their business and give them different levels to work towards.

4.6. Option 4: Reduced cyber insurance premiums

In this option, reduced premiums could be offered to businesses who meet requirements set by insurance companies around cyber risk management; for example holding a Cyber Essentials certificate.

4.6.1. Overall response and feasibility

Some businesses responded positively to this option (particularly those who saw cyber crime as a higher risk); however this was due to the voluntary nature of the option and potential to save money rather than encouragement to take action and review and improve protection measures. This option was reviewed positively particularly among businesses that already had security measures (and more sophisticated measures) and cyber insurance in place as it was viewed as the easiest option. For these businesses, this option held value because they could protect their business by having good cyber security, and get reduced premiums, saving money as a result. This option was seen to be fair as respondents believed businesses should get a reduction for having good cyber security and was often compared to car insurance.

> *"It's like being a careful driver, you should get reduced insurance premiums, so yeah, why not?" (Food Industry, 50-249)*

SMEs particularly liked the idea (proposed in the stimulus material) of the Cyber Essentials Scheme as the certificate/ badge can be used to differentiate the business by being displayed on websites and used in tendering processes to show that the business is taking cyber security seriously.

However, this option was less attractive to businesses that do not currently hold cyber insurance and see cyber crime as a lower risk. It presents high barriers to entry as businesses would need to spend twice – on the policy and the new measures – in order to save. Some businesses did not believe they need to buy insurance due to the type of data they hold, believing themselves to be at low risk (where they did not see themselves as holding PI). Some businesses were concerned about how complex and demanding the requirements would be and were not convinced that paying £300 for Cyber Essentials would reduce their premium significantly enough to hold value. Businesses were also cynical about the insurance industry more widely, and were often not convinced that even with cyber security measures in place, insurance companies would pay out claims for breaches. Businesses would need reassurance from insurance companies that they would pay out before investing in cyber security measures.

> *"Knowing insurance companies they'd find a way round it. I know whenever you have a claim they look for ways they can get out without paying you." (Business Services, 250+)*

> *"I'm a wee bit cynical…the time to demonstrate consequential loss probably outweighs the reimbursement of the consequential loss." (Construction, 50-249)*

4.6.2. Cost and impact

Costs were reported for taking out a new cyber insurance policy where this was not already in place. However this option was seen as an opportunity for a saving by businesses who had insurance in place. Overall, the cost of the Cyber Essentials certification at £300 was considered to be reasonable. However there was scepticism about whether this would reduce premiums significantly enough to represent good value. Additional costs reported were for new security measures and time to implement them as well as staff time and resource to complete the Cyber Essentials certificate. Finding the time and resource for completing the Cyber Essentials scheme and implementing security measures was of greater concern to smaller businesses than medium and large businesses.

4.6.3. Effectiveness

While this option was viewed positively by some businesses and to add value by potentially saving businesses money, it served as a weak call to action as businesses would not be motivated to take immediate action. It was seen as a benefit rather than encouragement to review or increase cyber security measures. Preference for this option was driven by the opportunity to save money rather than review measures (particularly by those already holding cyber insurance and who had more sophisticated measures in place). The non-mandatory nature of the option would also mean it would be easy to avoid for many. Businesses of all sizes suggested that they would conduct a cost/benefit analysis to determine whether the reduced premiums would outweigh the cost of new measures. There was low awareness and take up of cyber insurance among businesses in our sample, and for those that did have insurance, they were generally unsure about what this covered. This effectiveness of this option was also damaged by the cynicism about the insurance industry outlined above which may prevent businesses taking it up.

> *"You would have to do the maths to it, you could either pay X amount higher premiums or X amount putting cyber security in place." (Retail, 250+)*

> *"It may incentivise you a bit more, but nothing major… you're always going to expect the security to be higher [than the premium reduction]"(Hospitality, 50-249)*

4.6.4. Suggestions for improvements

- Businesses who already had cyber insurance and held a lot of PI felt that cyber insurance should be a mandatory add on to existing business insurance with a discount if businesses have Cyber Essentials.
- Businesses need clarity on the level of discount and requirements for this option to be meaningful.
- Businesses would welcome reassurance from insurance companies that they would pay out if they suffered a cyber-attack.

5. Recommendations

This chapter presents recommendations on effective mechanisms for increasing business action on cyber security. Section 5.1 reports on businesses responses to the five options and which approach was seen to drive change most effectively. Section 5.2 discusses the challenges associated with each option.

The research found that there is merit in DCMS pursuing both ‘carrot’ and ‘stick’ approaches that offer support and incentives to businesses as well as penalties. In this research, mandatory breach reporting and reduced fines and the mandatory health check provided stronger calls to action, and if communicated in combination approaches such as these could more effectively drive change. Each of the five options presents risks and challenges if pursued in isolation.

5.1. Combining support, incentives and penalties to drive change

Businesses’ detailed feedback showed that mechanisms which employ support, incentives or penalties each have merit and can effectively drive change. Overall, the research suggests that a strategy which combines options tested in this research could serve as a stronger call to action and more effectively drive change and encourage businesses to review and improve their cyber security measures. The options tested in this research are among others DCMS are considering pursuing.

We recommend exploring whether it’s feasible to combine the options for mandatory breach reporting and reduced fines and the mandatory health check – approaches which combine the principles of support, incentives and penalties. An approach joining these principles could create a pincer movement and present an opportunity for support on a topic about which some businesses lack knowledge and confidence and would welcome advice, but punishes those who then do not take action. The health check could be presented as a way to support businesses to make changes to enable them to access the reduced (or removed) fines and could therefore be seen to add value to businesses for the cost of the check.

The health check generally received a positive response from businesses where it was seen to be helpful, supportive and offer added value. Businesses understood that they would need to pay for the check but perceived it to be able to add value. Some businesses welcomed advice and evidence from a reliable source, on a topic which can be perceived as complex and scary and where they lacked knowledge and confidence and did not know who to trust. Crucially, this option can be seen to support businesses to make changes, rather than punishing them. Businesses said that being able to publish their score could also differentiate them and give customers and investors confidence. However, feedback suggests that further response to this type of mechanism would depend on how checks are designed. The cost, frequency, requirements, and style of the report would all shape business’ responses. In particular, businesses wanted the report to include a score which they could publish but did not want to publish further detail as this could be used by competitors or cyber criminals. They wanted to report to be detailed and offer advice on next steps and the cost of appropriate measures to address risks. However they also wanted the report to be accessible. Businesses raised concerns about who would carry out the checks and the role consultants would play. We suggest burden perceived to be created by the mandatory nature of the health check, in terms of financial cost and disruption, could be offset by the check helping businesses to make appropriate changes to access reduced fines if a breach occurred.

The option for mandatory breach reporting and reduced fines – an option combining the principles of penalties and incentives - also served as a strong call to action for businesses to quickly take action to review and improve their measures – albeit for different reasons. Businesses reacted strongly but negatively. They tended not to be aware of the current potential level of fines they could receive and this as well as increasing the fines was perceived to be scary and have potentially damaging implications for businesses. Risks associated with mandatory breach reporting also raised concerns about reputational damage leading to loss of customers. Businesses reported that there should be no fines rather than reduced fines for those who have fully complied with approved codes. Raising awareness of the current levels of fines and impending changes could work to move this issue up the agenda of boards and senior staff.

Combining the principles of these two options into a coherent strategy which offers a carrot and stick approach and added value to businesses, could serve as a strong call to action and drive businesses to review and improve their cyber security. A strategy which offers support as well as penalties would need to be carefully communicated to businesses so that the incentives are clear. Communications should also be tailored separately to decision makers and implementers, identified as potential access channels in Section 3.3.

5.2. Risks and challenges associated with pursuing options in isolation

Businesses identified numerous risks and challenges associated with the principle of each of the five mechanisms. If the health check is pursued in isolation without the incentive of helping businesses demonstrate compliance with data protection regulation and receive reduced or removed fines in the event of a breach, then this mandatory check can be seen as burdensome and costly to some businesses, particularly those who do not see cyber crime as relevant to them and conversely those with greater knowledge and who already have measures and strategies in place and review these regularly. Organising the health check and complying with its requirements can be seen as burdensome and costly and having an external consultant conduct this can be perceived to be invasive and disruptive. Businesses also raised concern about this option providing information to competitors and criminals.

Some businesses saw the option for mandatory breach reporting and increased fines as punitive and heavy handed. This was particularly the case for businesses who thought the government should be focusing on tracing and punishing cyber criminals rather than businesses who are also victims of cyber crime. This response may be reduced if this approach is combined with additional support and advice. There is low awareness of the current levels of fines and therefore communications work would be required for this option to be effective. Business raised questions and concerns, particularly around how mandatory breach reporting would be policed. They questioned how the ICO would know a business had suffered a breach, and whether heavy fines may incentivise businesses to try to hide incidents. Businesses were also concerned about risks associated with suppliers, and who would pay the fine if suppliers were breached and suffering reputational damage by association with them.

Whilst some businesses expressed a preference for reduced insurance premiums, this mechanism served as a weak call to action because preference was driven by the opportunity to save money rather than improve security measures. This option was also a weak call because it was not mandatory and therefore easy to avoid. The mechanism’s effectiveness was further hindered by low awareness of and knowledge about cyber insurance. It also involved too many unknowns, particularly the cost of cyber insurance, level of reduction, and detail about cost and implications of the requirements. The credibility of the option was harmed by cynicism about the insurance industry more widely and scepticism about whether companies would pay out. This option also presents high barriers to entry: many businesses did not have cyber insurance and therefore would need to spend twice (on a policy and meeting the requirements) to save.

The annual and website reporting were perceived to be bureaucratic and burdensome. They were a weak call to action because businesses perceived them to be a box ticking exercise to complete as quickly as possible, rather than an opportunity to review their security measures. The options do not provide help and were often seen to offer little added value. They may be costly where businesses would need to seek external support to comply. Whilst some businesses said the statements could reassure customers and investors, they more often questioned whether anyone would read the statements. Businesses questioned who would check the accuracy of the statements. They raised the risk of satisficing as businesses would want to complete this quickly and could utilise templates. Businesses were also concerned that these public statements could provide information to competitors and hackers.

Overall, the principles of support, incentives and penalties in options 1 and 2 were seen to be stronger calls to action and more likely to drive meaningful change.

6. Appendices

6.1. Achieved sample

X30 interviews		**Completes**
	Face to Face	10
	Telephone	20
	Total	30
PRIMARY QUOTAS		
Size	1-49	14
	50-249	10
	250+	6
SECONDARY QUOTAS		
Engagement with cyber security (in the last 12 months)	1. Not taken or considered taking any action to increase our cyber security protection	8
	2. Has considered looking into taking action to increase our cyber security protection	15
	3. Has looked for information about taking action to increase our cyber security protection	2
	4. Has sought advice on taking action to increase our cyber security protection	
	5. Has taken measures to increase our cyber security protection	5
	6. Has updated our cyber security protection	
Attitude to risk		
	High	7
	Medium	17
	Low	6
Confidence		
	Very confident	6
	Quite confident	18
	Somewhat unconfident	6
	Not at all confident	0
TERTIARY QUOTAS		
Sector	Retail	3
	Manufacturing	3
	Financial services	1

	Scientific sectors	0
	Charity	0
	Insurance provider	0
	University	0
	OTHER – SPECIFY 11-Business services 11-enginerring 11-consultancy 11-recruitment & logistics 11-import/export x 2 11-Recruitment 11-Private Law 11-Automotive 11-hire equipment 11-photography 11-medical 11-Healthcare 11-law 11-Logistics 11-Healthcare 11-Food sector 11-Automotive 11-digital services 11-hospilality 11-Construction x 2 11-Fork lift Truck sales	23
Region	Greater London	7
	South East	1
	South West	4
	West Midlands	0
	North West	5
	North East	0
	Yorkshire and the Humber	12
	East Midlands	0
	East of England	1
	Scotland	0
	Wales	0
		30

6.2. Topic Guide and Stimulus

DCMS Cyber Essentials - Strand C – Testing mechanisms for change

Depth interviews: Topic Guide (45-60 mins)

Aims and objectives:

Explore effective mechanisms for increasing business action on cyber security. This will involve **testing likely businesses responses to options including regulatory change, the**

introduction of incentives, and other interventions. Specifically, the objectives of this strand are to:

- Understand any practical difficulties with the options tested;
- Uncover any unintended consequences;
- Determine the likely impact on businesses, and potential scale of impact;
- Whether (and which) incentives are likely to persuade businesses to take (greater) action to tackle cyber threats.

Methods:

- 20x tele depths and 10x face to face, 45-60 minutes interviews, at least 6 large businesses
- Respondents will be the budget holder and decision maker for cyber security risk management *(likely to be the CEO in small businesses, finance director in medium businesses, and finance director or risk manager in large businesses)*
- Option available for paired depths to include IT and information security managers

1. Introduction

- Introduce yourself and TNS-BMRB – an independent social research agency
- Research on behalf of DCMS (the Department for Culture, Media and Sport).
- This research is exploring your views on ways in which businesses can be encouraged to take greater action to protect themselves against cyber threats. We will be collecting business' views on 4 possible options for this.
- This research is voluntary - participation will not affect your current or future relationship with DCMS
- The research is confidential and anonymous – though fully anonymised transcripts of the session will be provided to DCMS
- The information provided will be used for research purposes only
- Length: 45-60 minutes
- Gain permission for audio recording

2. Background – 5 mins

This section scopes out background of the respondent, business and key players who may be involved in decision making about cyber security risk management. It will explore how characteristics of the business may influence strategy and decision making in this area. It will also explore the role of IT and cyber security consultants/advisers in this area where relevant.

- Respondent background
  - Role and responsibilities
- Role with regards to cyber security risk management (CSRM)
  - Explore how confident and comfortable they feel in this role
- Nature of the business and operations
  - Size, sector, history
  - Products / services
  - Large businesses – explore key areas of risk in the business

        - Small/medium - Whether they trade online; Whether they hold personal information – types and volumes; IT set up - use of IT products and services
    - Ownership / company structure
        - Where CSRM sits in this
    - Whether they make use of any external sources of advice/support for cyber security specifically (e.g. cyber security / IT consultants)

3. Attitude towards cyber crime and current approach to cyber security risk management– 5 mins

This section will begin to map the range of influences on CSRM. It will explore the respondent's understanding of cyber crime and security measures, and assess their knowledge and confidence in this area. It will explore their perception of the risk this threat poses to the business and attitude towards the issue. It will then explore the business' current strategy and approach to CSRM and the measures they have it place, who is involved and how decisions regarding investment and risk management are made. It will explore any changes recently made to change or improve protection measures and motivations for this.

- Explore understanding of cyber crime and cyber security measures
    - Assess knowledge and confidence in this area
- Respondent's attitude to and perception of the risk posed by cyber crime
        - Their view on the organisational attitudes/perception of the risk of cybercrime: amongst board; more widely
        - Level of priority within the business; at senior/board level
        - Whether / what they hear from their investors about cyber security; to what extent they think this factors into decisions to invest
        - To what extent they are aware of/examine cyber security of suppliers – why/why not
        - What they think might encourage them to do so in future

- Current CS protection measures in place (respondent to briefly list)
    - (Estimated) cyber security spend
    - Current CS risk management 'strategy' – how defined/formalised this is
    - Any changes / improvements which have recently been made – explore what triggers and motivated these changes
- Decision making process (for strategy and investment)
    - Who is involved and their roles / degree of involvement - (explore profiles of decision makers and their attitudes)
    - How decisions are made
    - Factors that influence decisions (e.g. costs, time, reputation, risk, competing priorities etc)
    - Barriers to increasing security measures

4. Spontaneous drivers of change – 5 mins

This section will explore spontaneous drivers of and barriers to change and improving cyber security protection.

- When, if at all, are measures reviewed, and reasons for this

- What factors / situations might prompt them to consider reviewing their CS protection measures
  - What they think would encourage the board to take an increased interest in cyber security
- Whether they think culture change about cyber security is possible (e.g. all staff aware of necessary steps to protect themselves)
  - What they think is necessary to effect culture change
- Any expected changes in the future - regarding cybercrime and cyber security protection measures
  - Explore internal/external changes
  - How they think the company might react to these changes – and why
  - How decisions would be made

  Researcher note: note where changes to data protection legislation (described in option 3) are raised spontaneously – though do not ask

5. Testing options – 40-45 mins

This section will explore businesses' responses to the four options. A high level summary of the principle for each option will be introduced. The researcher will read out an agreed statement/explanation communicating the way in which each option would operate.

Moderator to explain that we would like to test various options the government is considering to encourage businesses to take greater action to protect themselves from cyber crime.

The core questions below have been merged into each of the testing sections but please ensure these core topics are covered for each option.

Core questions

Researcher to explore these questions after reading out each of the options below and then follow up with additional/tailored prompts specific to each option. Researcher to use prompts flexibly but ensure the following areas are covered:

- Overall response to the option
  - Whether it raises any questions or concerns
- What their next steps would likely be
  - What changes would need to be implemented (how would decisions be made, who would be involved, how would they assess the benefit to the business)
  - Whether budgets would be affected
  - Whether they would need to seek advice and assistance (where they would look for this and why)
  - *Researcher to explore any unintended consequences*
- Barriers and challenges presented
  - Any practical difficulties envisioned
- Costs to the business
  - Explore costs and burden in depth
  - Explore components of cost and whether this is perceived to be high/low (Financial, time, and explore any other costs/burdens)
- Perceived benefits

    - To the business, sector/ industry, UK business more widely
- Likely impact on the business
    - At board level – would this highlight the issue to the board
    - Culture change more widely
    - Assess the scale of any impact
- Whether they envisage this option would improve levels of cyber security /encourage them to increase their measures; how effective it would be
    - Why / how, or why not
- Would they suggest any changes to make this option more effective for their business

Options and additional prompts:

Option 1a: Add risk reporting to Annual Reporting requirements
ASK LARGE BUSINESSES ONLY (250+)

In this option, large companies are already required to publish Annual Reports setting out their accounts, principal risks, and trends and factors likely to affect the viability of the business. This option would introduce the new requirement to include reporting on cyber security risk within the annual reports. This could include whether they have appropriate protection in place to avoid attacks and how they would deal with breaches if they occur.

- Overall response to the option
    - Whether it raises any questions or concerns
- Explore (briefly) any existing annual reporting requirements, including any that relate to cyber security (high level/detailed)
        - If not why not, and what might encourage them to do so (i.e. other than mandation – competitors, board interest, following breach, etc.)
        - If existing, what information is included in the report (check against the list provided)
- What their next steps would be
    - What changes would be required and whether budgets would be affected
- Any barriers or challenges
- Costs and burden to the business - Estimation of time/resource required to report this on an annual basis (e.g. would they seek external support; does it overlap with any existing protocols)
    - Explore whether they have the skills to identify risks and whether they would seek external help
- *List information that may be required in future* – does this information already exist
    - Explore whether providing a list of what would be required would be helpful
    - Whether they would need help with this

Information that may be required:

- *How risks are being communicated to boards and at what frequency*
- *How sensitive and critical data are being protected*
- *Whether the company's cyber security strategy been evaluated (whether third parties are involved, how they evaluate their supply chain)*
- *Whether incident management processes are in place*

- Likely impact on the business
- Explore what would encourage them to do more than the minimum required (standard reporting)
- Whether this option would improve their cyber security
- What information they think would be helpful to report – in terms of data they consider to be useful
    - Anything they would be less comfortable with reporting
- Whether they think this would differentiate their business – do they expect investors will be interested in this information / will be able to compare; why/why not

Option 1b: Require businesses to display a statement on their website
ASK SMALL AND MEDIUM BUSINESSES ONLY (1-49, 50-249)

In this option, a mandatory requirement would be introduced for small and medium size businesses to publish information on their website (or another publically available space) about their approach to cyber risk management. The level of detail required has not yet been decided, but the aim would be to ensure that businesses really consider the risk and not just provide a standard statement.

- Overall response (any concerns)
- Explore (briefly) any existing requirements to provide statements on their websites, including any that relate to cyber security (high level/detailed)
    - If existing, impact of this on the business
    - If not why not, and what might encourage them to do so (i.e. other than mandation – competitors, board interest, following breach, etc.)
- Explore whether they see any value in providing this information to consumers
- What their next steps would be (any changes needed and whether budgets would be affected)
- *List information that may be required in future* – does this information already exist

Information that may be required:

- *How risks are being communicated to boards and at what frequency*
- *How sensitive and critical data are being protected*
- *Whether the company's cyber security strategy been evaluated (whether third parties are involved, how they evaluate their supply chain)*
- *Whether incident management processes are in place*

- Barriers and challenges
- Explore whether they have the skills to identify risks and whether they would seek external help
    - Explore whether providing a list of what would be required would be helpful
- Costs to the business
- Impact on the business
- Explore what would encourage them to do more than the minimum required (standard templating)
- Whether they think this would differentiate their business – do they expect investors or customers will be interested in this information / will be able to compare; why/why not

Option 2: Introduction of a mandatory cyber security health check (top down, board led culture change)
ASK ALL

Option 2 would introduce a new mandatory requirement that all businesses - or those of a certain size and type - are required to regularly undertake a cyber health check; for example every 3 years. This could be carried out by an external agency (not necessarily auditors) to test their cyber security risk management processes. It could include penetration testing. Afterwards, businesses would receive a score and report suggesting ways to improve their cyber security.

- Overall response
- Current security evaluation process
- Any areas of audit/health checks for business currently – how costs/benefis of these are weighed up
- If required to have a health check, what would they expect from this to maximise usefulness for the business (i.e. guidance, feedback, or advice they think would need to be part of the process)
    - Whether they would see this as providing any additional value over and above what they currently do
    - Where would they seek advice and information
- What a 'good' and useful approach to health checks would look like for businesses
    - Explore views on what the consequences of a negative report should be and their response to this idea of this being made public
- What their next steps would be (changes and whether budgets would be affected)
- Barriers and challenges
- Costs to the business
    - How much would they expect to pay (if every 3 years)
- Impact on the business
- How much do they think it would influence their measures

Option 3: Introduction of a mandatory data breach reporting and reduced fines for improved cyber security measures (influencing investment decisions, avoiding reputational risks, changing relationship with customers)
ASK ALL

Definition data breach: "a breach of security leading to disclosure of personal data"

- Explore awareness of what happens currently should a breach occur
    - Expectations of fines, and estimation of the level of fine (average, maximum)

Private sector organisations are not currently required to report personal data breaches to the data protection regulator (the Information Commissioners Office) or individuals affected. The new General Data Protection Regulation will introduce requirements to report breaches to the regulator and more serious breaches to affected individuals. Failure to report a breach could result in a fine. The regulator will be able to issue larger fines for data breaches, up from the current £500,000 maximum.

- Explore awareness of these changes among businesses
- Overall response and concerns
- What their next steps would be (changes and whether budgets would be affected)
- Barriers and challenges
- Costs
- Impact on the business
  - Explore how this might influence decisions on cyber security
  - Explore how far significantly increased fine levels would influence decisions on cyber security; and/or encourage them to take additional measures
  - Expectation of impact on relationship with consumers
- Whether/how mandatory breach reporting would change they way they think about:
  - the reputational risks of a data breach
  - the financial risks of a data breach
- Whether fines/other financial penalties been introduced to other areas of their business; how have these been responded to

When investigating a breach, the regulator considers several factors when deciding whether to issue a fine and its size. These include whether the organisation has followed standard guidance on information security or implemented common security controls.

Option 3 would see fines for breaches reduced by the regulator if the organisation can demonstrate they follow approved codes or have achieved certain certifications regarding information and cyber security.

- Would a reduction in fines for data breaches, offered for good cyber security behaviour change their approach to cyber security; why/how or why not
  - If they were offered reductions in these fines for having undertaken certain certifications and following approved codes, how likely would they be to take these and what would this depend on
  - Explore what level of certainty over the reduction would be required for them to invest in security measures
  - Where they would look for information, advice and guidance

Option 4: Reduction of insurance premiums for cyber security protection measures (trade-off between reduced premium and increased measures)
ASK ALL

- Explore awareness of current coverage for cyber attacks under existing insurance; type and level of cover (first party, third party) (and other risks)

Cyber insurance can provide cover against loss of information from or damage to IT systems and networks. For option 4, reduced premiums could be offered to businesses who meet requirements set by insurance companies around cyber risk management; for example holding a Cyber Essentials certificate. This may incentivise businesses to invest in cyber protection measures who would not otherwise have done so. *Moderator to read out description of Cyber Essentials scheme if unknown:* The Cyber Essentials scheme checks whether your business meets 5 basic cyber security requirements. You become certified when you meet these requirements. Certification costs start from £300.

- Overall response and concerns

- What their next steps would be (changes and whether budgets would be affected)
- Barriers and challenges
- Costs
- Impact on the business
  - In principle, whether they have a preference for paying higher premiums vs spending on cyber security measures (i.e. transfer of the risk)
- Whether this wouold change their approach to cyber security risk management
- Explore any other areas of their business where they receive insurance reductions for actions taken – how this was introduced

6. Prioritisation – 5-10 mins

In this section, respondents will be asked to reflect on the four options and carry out a prioritisation exercise.

- Explore whether any of the four options is likely to persuade them, and the business, to take greater action to tackle cyber threats
- Explore relative effectiveness of each, and reasons for views:
  - Top down / board led culture change
  - Greater public awareness of companies' measures
  - Advice from external experts
  - Reduced fines
  - Financial incentives – savings in exchange for increasing levels of protection
- Whether there are any other options / ideas which would persuade them to take actions and engage with the issue of cyber threats
- What they think about current guidance/information
  - Would they like more information about what constitutes best practice
  - Anything specific they think would be useful for businesses
- Would they share information on attacks with other businesses in their sector
  - Would they find information sharing useful
  - Would this encourage them to implement changes

7. Close

- Any final thoughts / questions
- Explain incentive process (£60 BACS transfer)
- *Moderator to explain that DCMS may wish to conduct some follow up work once these ideas have been developed further. This will likely take place in September, and will probably be a short (c. 20 minute) telephone interview.*
  Moderator to request (written) consent for re-contact for F2F (check signature sheet and report any opt-outs to research team) and verbal for telephone
- Thank and close