Cyber Essentials Scheme – process evaluation and communications testing

DCMS
2016

TNS BMRB
DCMS Cyber Essentials Scheme

JN260136173

Contents

1. Executive Summary

Cyber crime is a growing threat to the UK public, businesses and Government. The government-backed Cyber Essentials scheme aims to be a low cost, achievable and light touch way for businesses to protect themselves against cyber threats. However, adoption of the scheme has not been as rapid as anticipated. Current evidence shows that businesses face numerous barriers to improving their security practices, and government efforts to improve security practices in the UK and elsewhere have not necessarily had the desired impact.[1]

DCMS commissioned TNS BMRB to conduct research to; (a) understand how to support increased adoption of the Cyber Essentials scheme and (b) ensure it is easy to use. Qualitative research was conducted with a total of 63 businesses over three strands, comprising:

- a process evaluation, consisting of 30 depths interviews with businesses certified under the scheme, exploring their experience of the process and identifying areas for improvement
- message testing, consisting of 4 focus groups of SMEs who have not been certified, to understand their views on key communications about the scheme
- remote website testing, conducted with 11 SMEs not certified under the scheme, to explore responses to information provided on the website.

1.1. Current motivations for undertaking Cyber Essentials

Cyber Essentials was designed to appeal to businesses wanting to protect themselves against cyber threats. The aim was that, once certified, businesses would use the badge to differentiate themselves as a secure business. However, these were not the main motivations reported by businesses who had signed up to the scheme. Rather, current motivations tend to be financially or business driven. Businesses tended to report that they had undertaken the scheme because it was a mandatory requirement in government procurement. Amongst the audience for the scheme, there was a high concentration of cyber security, IT and other consultants who were motivated to complete the certification in order to expand their offer and sell Cyber Essentials to other businesses, often alongside other products (e.g. penetration tests and scans). Businesses only cited protection from cyber crime as a reason to become certified if they had already suffered a breach or after deep engagement with Cyber Essentials (e.g. after having attended a course or conference).

1.2. Current barriers to engagement with Cyber Essentials

Echoing previous evidence in this area, businesses in the research did not necessarily perceive cyber crime as a relevant threat to them – and tended to discount the likelihood that they were personally at risk. They are therefore not actively seeking solutions to cyber crime, and are more likely to ignore messaging encouraging them to take action. In addition to this, SMEs often lacked knowledge and confidence about cyber security, perceiving it as a highly technical area and an increasingly crowded marketplace in which they do not know who to trust. The

[1] Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Maria Bada, Angela M. Sasse and Jason R.C. Nurse 2015; Using behavioural insights to improve the public's use of cyber security best practices, Summary report, Government Office for Science, 2014.

topic can drive fear and anxiety for these businesses. Awareness and recognition of the Cyber Essentials scheme was also very low.

Businesses certified through the scheme pointed to a number of possible improvements, in terms of how the scheme is presented, and around the process of certification itself. At the sign up stage, some businesses were confused about the nature of the scheme, and reported that the benefits and value of the scheme were not clearly communicated. They also reported that the current one page structure of the website is difficult to navigate. Some businesses reported finding the language used technical, and the jargon used on the website and in the supporting documents as difficult to understand. Once they had made the decision to become certified, some businesses still lacked clarity about the costs, process and requirements of certification.

During the completion process, some businesses encountered difficulty selecting a Certifying Body (CB) because of the amount of information provided and the growing number of providers, with which businesses (outside of the cyber and IT sectors) were unfamiliar. Some less confident businesses encountered difficulties completing the questionnaire, due to perceived ambiguity about how to respond. Meanwhile, businesses reported receiving varying levels of service from their CBs, with some providing less support and assistance than others which could serve as a barrier to successful completion.

Businesses tended to perceive the scheme to be good value for money. However this was within the context of businesses undertaking the certification in order to bid for and win new business (e.g. where the certificate was a mandatory requirement for a government procurement process) or as a business opportunity for cyber security and IT consultants. Value was not determined on the basis of the perceived quality of the scheme, its ability to protect against cyber threats, or its cost compared to that of an attack.

1.3. Risks and opportunities

There is currently low awareness of the scheme and of the badge, presenting a key barrier to sign up and undermining the value of the badge as an effective market differentiator. However, the fact that the scheme was government backed was highly attractive to businesses, who struggled to know which companies or products they could trust in the cyber security marketplace.

Currently, CBs create their own questionnaires (based upon a standard questionnaire) and respondents reported that they found different length versions available (ranging from 30-100+ questions). Businesses also reported variation in the types and levels of evidence they were required to submit. Given some businesses approach the scheme as a ‘tick box exercise’ to be completed for procurement purposes, this could be creating a race to the bottom for the shortest questionnaire. Businesses reported questionnaire length influencing their choice of provider. This also poses a potential risk to the credibility of the scheme if the accreditation is perceived to lack consistency or rigour.

Businesses reported experiencing varying levels of support from their CBs which can drive varying levels of satisfaction with the scheme. This can also be perceived to contribute to some businesses failing the first time where businesses feel they have not been given enough or appropriate support completing the questionnaire and information about what is required to pass. Businesses have different support needs when completing the certification, depending on their levels of knowledge and confidence about cyber security and IT more widely. Varying levels of service present a risk to the scheme where those with greater needs receive less support than they need or expect, as this can damage the reputation of the scheme.

In addition to CBs, there is a growing number of cyber security and IT consultants operating in this market, with evidence that some are using Cyber Essentials as a way to upsell products to businesses who have little understanding of the area. This presents a potential reputational risk to the scheme if businesses later realise they have been upsold unnecessary products or services. However, another implication of their involvement is that businesses in fact opt for greater levels of protection than they would through basic implementation of the Cyber Essentials measures. Further, such consultants could represent effective messengers or ambassadors for the scheme, if harnessed appropriately.

1.4. Recommendations

The research produced recommendations for ways in which the process, website and messaging can be improved to further engage businesses and increase uptake of the scheme. A summary of these recommendations, which respond to the barriers and risks outlined above, is provided in section 4.8.

The research suggests that the benefits of the scheme should be made clearer upfront so that businesses understand the value of the scheme. The cost, process and requirements should be clarified up front as businesses require this information to proceed. To help businesses make informed choices, greater clarity should be provided about the difference between the Plus and Basics accreditation. A summary table should be provided which allows businesses to quickly compare CBs and a feedback system developed to provide information about varying levels of customer service. Improvements could be made to make the scheme easier to complete for non-experts; such as guidance about how to use answer codes and the reduction of jargon.

In addition to the points above, the website could be improved by also improving the structure so that it is not all on one page; providing a tailored report after completion of the questionnaire; adding contact details; and including additional quotes and case studies from a wider range of businesses.

The messaging for the scheme could be improved to attract a wider audience and boost the credibility of the badge. The research found three key messaging principles: convince businesses that cyber crime is a real, relevant and urgent threat; convey what Cyber Essentials is and how it addresses this threat; and outline the costs and requirements clearly.

Beyond this, the research found that messages need to be tailored to three key groups: those who think an attack won’t happen to them; those who are worried and unsure; and businesses who assume they are covered. Businesses who think it won’t happen to them tend to be micro and smaller businesses, in low risk sectors and are less likely to trade online and have no or limited IT function. Businesses who are worried and unsure tend to be small businesses, medium risk sectors and may trade online and have some IT function. Businesses who assume they are covered tend to be medium size businesses, from higher risk sectors who trade online and have an IT team.

2. Introduction

2.1. Background

Cyber crime is a growing threat to the UK public, businesses and Government. The 2016 Cyber Security Breaches Survey reported that 65% of large businesses and 24% of all businesses experienced a security breach in the last year.[2] Businesses can incur financial costs, damage to systems and lose data, and also suffer from loss of time and reputational damage from cyber attacks. The government has introduced a range of measures working to protect UK businesses from cyber threats.[3]

The government-backed Cyber Essentials scheme has been designed to outline the basic measures that businesses can take to protect themselves against cyber threats. Aimed primarily at SMEs, the scheme offers a low cost, achievable and light touch way for businesses to protect themselves from the most common threats online. The scheme also aims to support consumers, investors and supply chain partners to choose businesses that take protection against cyber crime seriously, demonstrated through display of the Cyber Essentials badge.[4] The Cyber Essentials scheme sets out five basic cyber security controls businesses should have in place. Businesses become certified when they meet these requirements and have these five controls in place:

1) Malware protection [i.e. using anti-virus software]
2) Patch management [i.e. updating software]
3) Access control [restricting access to those who need it]
4) Secure configuration [setting up systems securely]
5) Boundary firewalls [to prevent unauthorised access].

The Government aims to rapidly increase uptake of the Cyber Essentials scheme, to maintain the high quality of the scheme, and to ensure it is easy to adopt and use. However, convincing businesses to take action and protect themselves against cyber crime is not easy. Evidence shows that recent efforts to improve cyber security practices among businesses have often not been successful or had the desired impact.[5] Almost half of all businesses in the UK have not undertaken any action in the last 12 months to identify the cyber security risks to their organisation, with the proportion increasing amongst micro businesses.[6] Previous research has identified numerous barriers to business' making positive behaviour change in this area, including:

- Habit and inertia – continuing current information security protocols;

[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 – Summary, HMG, June 2014

[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.

- High financial costs of security software and upgrades;
- Perceptions of the effort required to understand and implement changes – with low belief that these changes will translate into benefits;
- Downplaying risk and/or lack of belief in tangible, negative consequences;
- Low knowledge, understanding and confidence around cyber security;
- Over-estimating ability to understand and respond to security threats. 7

This research builds upon this evidence base to provide insight about ways to help encourage businesses to protect themselves against cyber crime.

2.2. Research objectives

DCMS commissioned TNS BMRB to conduct research to understand how to increase adoption of the scheme and to ensure it is easy to use. The research comprised of a **process evaluation** (strand A) and **communications testing** (strand B), comprised of **message testing** (strand Bi) and **remote website testing** (Strand Bii). The aims of these strands were to:

A. Understand how to improve businesses' experience of the application and certification process, as well as overall engagement in the scheme;

- Evaluate the **customer journey** for businesses who have signed up to the scheme, to identify areas for improvement:
    - Businesses' experience of the scheme, from first hearing about it through to achieving certification – motivations, barriers, influences on decisions, etc
    - How businesses implemented the standards, how Certifying Bodies (CB) were chosen, and businesses' evaluation of the support and services provided through the CB
    - Financial and time/resource costs, and how these were considered against the perceived benefits of certification
    - Whether businesses would encourage others to sign up
- Collect **quotes from businesses** about the experience of taking part in the scheme, to be used in communications

Bi. Understand how best to communicate the scheme and cyber security more widely, to increase businesses' take-up of the Cyber Essentials scheme;

- Develop and test effective **communications** to encourage sign up to the Cyber Essentials scheme, and promote cyber security more generally, to understand:
    - the messages that are most compelling for businesses
    - how information about the scheme (e.g. cost, the controls involved, and the two levels offered) influences businesses' perceptions of it and their decision to take part
    - the right balance of content between reasons to sign up to the scheme and descriptions of the scheme.

Bii. Understand how to improve the Cyber Essentials website.

- Test reactions to the Cyber Essentials **website**, to smooth the user journey, including exploration and testing of:

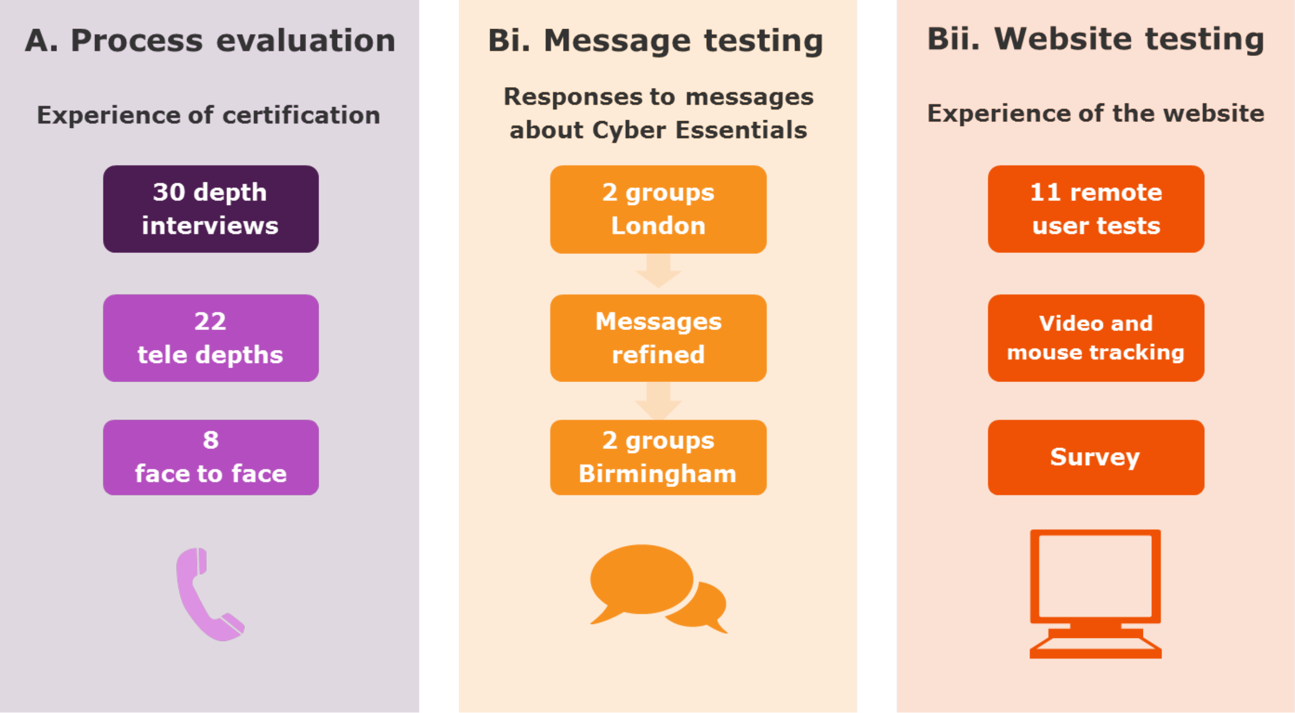
[7] Using behavioural insights to improve the public's use of cyber security best practices, Summary report, Government Office for Science, 2014.

- the content (text, messages, branding)
- layout, formatting, and logical ordering of information
- tools on the page, including the self-assessment questionnaire, the scrolling industry quotes, the downloadable documents.

2.3. Methodology and sampling

A multi-method approach was adopted to address the research objectives, summarised in Figure 2.1 below.

Figure 2.1: Summary of methodology



2.3.1. Process evaluation

Thirty depth interviews were conducted with businesses who were certified under the Cyber Essentials scheme. These explored decisions to adopt the scheme and experiences of certification. Interviews lasted one hour, and were a mixture of 8x face to face and 24x telephone interviews, including one paired depth with respondents who had shared responsibility for implementing the scheme. The face to face interviews were intended for businesses that had experienced a more complex certification process. Interviews were structured around a 'journey mapping' exercise, which involved talking through the experience of the scheme from start to finish, mapping satisfaction at each point. Interviews were recorded using digitally encrypted recorders and transcribed for analysis.

Sampling

Respondents were recruited from sample requested from the Accrediting Bodies, provided through DCMS. Respondents in the sample were offered the opportunity to opt out of recruitment. A range of business sizes were included, including 3 large businesses, but the sample was weighted towards smaller businesses who were more prevalent in the sample. A range of sectors were included, including IT and cyber security consultants (forming a relatively large proportion of the sample). A range of experiences of the scheme were included, however businesses tended to report few difficulties or complexity with completing the scheme at the recruitment stage. Respondents were given a £50 incentive to thank them for their time (£70 for paired depths).The achieved sample can be found in Appendix 6.4.

2.3.2. Message testing

Four 90-minute focus groups convening 22 SMEs in total were conducted to test and develop messaging about the scheme. The groups tested business' responses to headline messages about cyber crime; key messaging for the scheme; a leaflet and online ad. The stimulus materials used can be found in appendix 6.6.

The groups were iterative in design, with two rounds of testing to allow revision of the messages in the interim. After the first phase, a topline was provided to DCMS with recommendations from TNS BMRB as to what should be changed for phase 2. Messages that had been less successful at engaging businesses were removed or adapted, and a number of new messages were developed by DCMS to test in the next phase (e.g. including case studies). The messages tested, including how these were adapted between phases, can be found in appendix 6.6.

Sampling

Respondents for this strand were recruited using free find methods. The groups were split by size, with two groups of small businesses and 2 groups of medium sized businesses. Businesses were recruited across a range of sectors and levels of engagement with cyber security, e.g. some who had recently taken action to protect themselves, and some who had not taken action but intend to do so, including some who had been on the Cyber Essentials website but who had not progressed to certification. Phase 1 was conducted in London and Phase 2 in Birmingham. The groups were conducted two weeks apart. Respondents were given a £60 incentive to thank them for their time. The final achieved sample can be found in appendix 6.4.

2.4. Remote user testing

Eleven remote website testing sessions were conducted with SMEs in order to provide granular feedback on the Cyber Essentials website. Respondents completed the session from their office or home computer, in their own time, taking around 30 minutes to complete. Respondents were guided through a series of tasks: (a) their first impressions of the website and anticipated next steps, (b) feedback on specific aspects of the website e.g. their response to the questionnaire; and (c) responding to a series of follow up questions in an exit survey to evaluate their experience of the website. Respondents were asked to adopt a 'thinking aloud' approach, providing verbal feedback continuously during their session. Web-cam videos were collected from each user's session, recording their response during each task as well as their activity on the website itself. The topic guides and stimulus material for each of the strands can be found in appendices 6.5 and 6.6.

Sampling

Respondents were recruited using free find methods. Respondents were recruited in North and South England, the Midlands and Scotland. The sample was split by size of business, sector, and on existing knowledge of Cyber Essentials, to explore whether responses to the website depend on expectations and appetite for information and guidance in cyber security. Respondents were given a £60 incentive to thank them for their time. The final achieved sample can be found in appendix 6.4.

Participation in the research was voluntary, confidential and anonymous. Fieldwork took place between between May – June 2016.

2.5. Analysis

All interviews and focus groups were audio recorded and transcribed. The remote testing sessions produced audio and video files and the survey responses. This data was charted against key themes for the research objectives so that this could be analysed against sub groups. A brainstorm including all members of the research team was conducted. The data was analysed for themes and trends.

2.6. Structure of the report

Many findings were consistent across the three strands and were supported and triangulated across the three methods. In the report, it is indicated where findings are drawn from only strand A, Bi or Bii. The structure of the report broadly follows the methodology, with chapter 3 reporting findings drawn predominantly from strand A (process evaluation) and chapter 4 reporting findings from strand B (message and website testing).

Verbatim quotes are included from all three methodologies and attributed to the businesses size and sector to illustrate key findings.

3. Current barriers and motivations for engaging with the Cyber Essentials Scheme

This chapter explores the barriers and motivators to becoming certified with Cyber Essentials, in terms of how businesses hear about the scheme, their reasons for becoming certified, and their experience of the process of certification. Section 3.1 explores the characteristics of the current audience for the scheme and the implications of this. Section 3.2 explores businesses' experience of the scheme: at the point of sign up and at each stage of the certification process. Section 3.2.4 explores the perceived costs, benefits, value, and impact of the scheme. Section 3.3 presents recommendations derived primarily from the process evaluation and remote testing strands.

Key findings

Businesses' motivations for becoming certified with Cyber Essentials were rarely about protecting themselves against cyber crime, or differentiating themselves as a business that takes cyber security seriously. In practice, motivations amongst early adopters of the scheme have been to (a) satisfy mandatory government procurement requirements or (b) enable them to sell the scheme to other businesses, leading to a relatively high concentration of expert cyber and IT consultants in the audience. Low awareness of the scheme outside of the cyber and IT sectors is also a clear barrier to take up. This is supported by evidence from the 2016 Cyber Security Breaches Survey which found only 6% of businesses are aware of the Cyber Essentials scheme.

On the whole, businesses found much of the certification process simple and efficient (see quotes in appendix 6.3), though they reported some challenges that may serve as barriers to take up for other businesses. At the point of sign up, lack of clarity about the cost, process and requirements was sometimes confusing and frustrating for businesses. Complex language and technical jargon were off-putting, particularly for those who lacked knowledge and confidence in this area. Businesses were confused by the number of Certifying Bodies (CBs) and found it difficult to make meaningful comparisons between them. Experience showed that CBs provided different levels of support, and approached certification in different ways, which raised questions about standardisation and the consistency of the scheme.

The scheme was considered to represent good value for money. However, this is within the context of businesses undertaking the certification in order to bid for new business or as a business opportunity for consultants. As such, value was not being weighed against the threat of a cyber attack, or compared to other cyber security schemes.

3.1. Current audience

3.1.1. Ways businesses have heard about the scheme

Amongst the sample, businesses tended to have heard about the Cyber Essentials Scheme through government procurement processes where the certificate was a mandatory requirement to bid for contracts or retain clients (including the MoD, DfE and NHS). Knowledge thus tended to cluster in sectors where these contractual requirements were being introduced.

Some businesses had heard about the scheme through other specialist channels. Some had been informed by their IT suppliers who already provided them with other services. Meanwhile, some businesses had heard about the scheme at a conference or course, including those run by local councils and professional bodies (e.g. chambers of commerce), or the cyber security industry.

IT providers and those working in the cyber security industry had become aware of the scheme through industry news and channels. Some respondents reported that the scheme had been anticipated for some time within the industry.

> *"Yes I knew about it a few years ago; I was told that it was going to be the next big thing … everybody's been talking about it for two years, it's been a hot topic." (Strand A, 1-49, cyber security consultant)*

Strands A and B suggest that there is generally low awareness of the scheme among businesses outside of the cyber security sector. This not only presents a barrier to take up, but undermines the value of the Cyber Essentials badge, if it is unrecognised by other businesses.

> *"I'd never heard of it, to tell you the truth. Literally, they were the first client to approach me and say they needed it as a requirement for their continued support of [X client] and to get it sorted - so I looked into it, and that was the first time I'd come across it." (Strand A, 1-49, IT consultant)*

> *"I suppose [the badge] just gives reassurance but it only gives reassurance if it's well publicised and promoted out there... At the moment it's just as it is on the paper: it's just a sentence. It doesn't really- it doesn't mean much, if that makes sense, because there's nothing behind it." (Strand Bi, 1-49, London)*

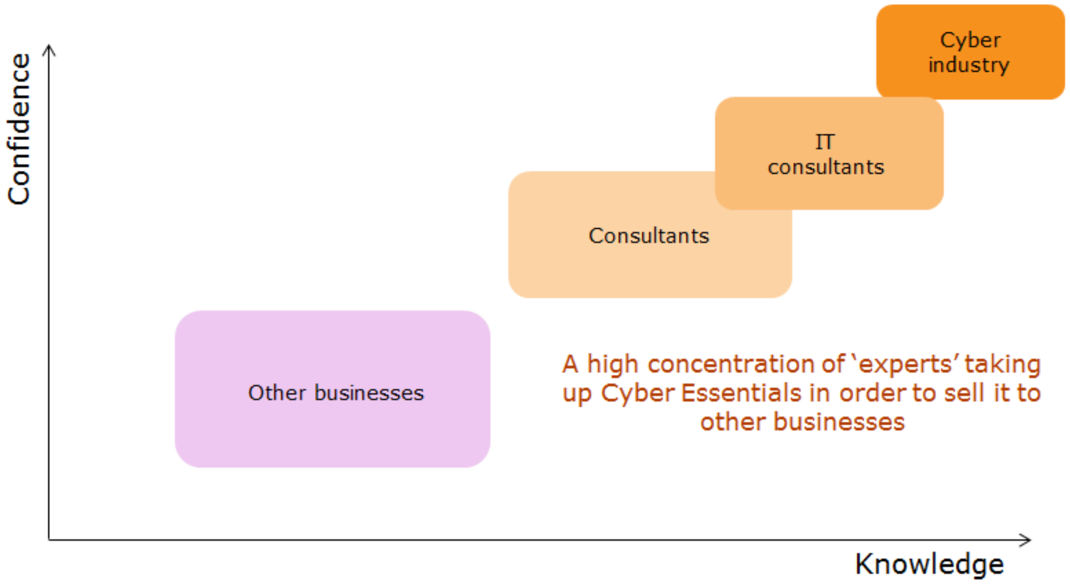
3.1.2. Audience Typology

The current audience has been shaped by early adopters in the industry and the requirement for the certification in procurement processes. This audience can be mapped against the dimensions of knowledge about cyber security and confidence in this area (see Figure 3.1 below). The current audience includes four main groups of businesses:

- **IT sector experts -** from the cyber security and IT industries who have high levels of knowledge and confidence about cyber security.
- **Experts -** other consultants, for example from the audit, risk management and information security sectors who have higher degrees of knowledge and confidence than some other businesses.
- **Non experts -** businesses from a range of sectors and of a range of sizes who require the certification in order to bid for government contracts.
- **Non experts -** businesses from a range of sectors who have undertaken the certification after engaging with the topic, for example to improve their security after an attack or as an alternative to the ISO accreditations.

The latter two non-expert groups tend to have lower levels of knowledge about and confidence around cyber security than the first two groups of expert consultants. This drives key differences in their experience of the process described in this chapter. Non experts include businesses of a range of sizes and from a range of sectors (listed in appendix 6.4). These businesses can lack knowledge and confidence in the area of cyber security and require assistance from experts to be able to engage with and complete the certification. Less confident businesses sometimes sought assistance from either their current IT provider or a new one. Less confident businesses tended to be sole traders and micro businesses and businesses operating in sectors they perceived to be less relevant to cyber security (e.g. education, environment and agriculture). The respondents themselves also tended to be older and less familiar with IT.

Figure 3.1: Current audience of the Cyber Essentials Scheme


Confidence
Cyber industry
IT consultants
Consultants
Other businesses
A high concentration of 'experts' taking up Cyber Essentials in order to sell it to other businesses
Knowledge

> *"I would probably come out in a cold sweat if somebody told me I had to start looking again at level two." (Strand A, 1-49, Education)*
>
> *"It meant nothing to me and the computer actually means nothing to me, I know how to start them up and I know how to shut them down … Obviously the work that comes down, I can open it up … My knowledge of computers- I would say quite a few of us, my generation of auctioneers, would be very similar to me." (Strand A, 1-49, Agriculture)*
>
> *"It's a language of its own, and I wasn't 100 percent confident with that language, so it was kind of getting my head round the questions." (Strand A, 1- 49, environmental consultancy)*

This context is important in evaluating the scheme. Cyber security, as well as IT more widely, was perceived as a highly technical, confusing area which can be a source of anxiety for some. Businesses who lack knowledge and confidence can feel somewhat vulnerable, exacerbated by the cyber security market becoming increasingly crowded. Businesses reported that in this sector, it can be difficult to know which suppliers are trustworthy and reliable when there are so many unfamiliar providers to choose from. The cyber security marketplace can be a confusing, overwhelming and scary place for some businesses. Ways to enable businesses to identify trustworthy providers and fair prices could help these businesses to feel more confident.

3.1.3. Current motivations

As Cyber Essentials was little-known or understood amongst the target audience, current motivations for certification were mainly financially and business driven, and the certificate was either a mandatory requirement in a procurement process or the business wanted to sell the certification to others. This is in contrast to the intended motivators for the scheme (outlined in chapter 1) and has implications for how businesses engage with the scheme.

A key driver of certification was Cyber Essentials being introduced as a mandatory requirement to bid for government contracts. In these cases, businesses felt they did not really have a choice, and often perceived the scheme to be a 'tick box exercise' which they needed to get through quickly. Others became certified as they believed Cyber Essentials would soon become mandatory in their industry, and wanted to 'get ahead of the curve'. This included a range of businesses in government supply chains. Some businesses knew their businesses already met the standards, particularly IT and cyber consultants. They therefore anticipated being able to complete the scheme quickly and not needing to make any substantial or costly changes (see case studies #3 and #4).

> *"It's something that we have to have in order to work for [a government department] and at the moment 80, 90 percent of our work is from [a government department]. We just went okay, well we are just going to have to pay for it and take the time to do it." (Strand A, 1-49, Design)*
>
> *"We would have lost a lot of business if we hadn't gone down this route" (Strand A, 50-249, Insurance)*
>
> *"It seemed like it was just ticking boxes … I knew our security was already tight so this was just a hoop to jump through to get them to continue the contract." (Strand A, 1-49, IT consultant)*

Cyber security and IT consultants had undertaken the certification in order to sell this alongside their current products. Some consultants from other sectors (e.g. information security and risk management) saw this as an opportunity to expand their offer and saw it as a new business opportunity.

> *"It was less about us getting the criteria to meet the network and more about if we get the accreditation, we're trained up as practitioners and it's a service we can offer out. It came out more from a revenue thing then a wanting to make yourself secure kind of thing." (Strand A, 1-49, cyber consultant)*
>
> *"...because Cyber Essentials was taking off it was like okay, it was more of a business opportunity and okay as a cyber essentials practitioner we could go and help other companies that say if they weren't so au fait with what would be required, we could provide them assistance to that company as more of a business opportunity." (Strand A, 1-49, cyber consultant)*

Some businesses undertook the scheme because they perceived it to be a cheaper alternative to the ISO accreditations, and in some cases, a first stepping stone towards achieving these more rigorous and well known accreditations. They were less likely to see the scheme as a tick box exercise and improving their cyber security as an iterative learning process.

> *"...finding out about Cyber Essentials made me think well let's not kind of bite off more than we can chew, let's start with the basic first to get that accreditation under our belt and then if the need arises we can go to a more advanced level…I guess Cyber Essentials, I see that as like a step one of a longer process." (Strand A, 50-249, Recruitment)*
>
> *"I thought it was good, as an entry level, because I also know…so for example ISO 27001 is quite an expensive scheme." (Strand A, 1-49, Other)*

A number of businesses were motivated by a desire to protect their business from cyber security threats. However, this tended to be after suffering a cyber security breach (see case study #1) or after deep engagement with Cyber Essentials (e.g. via a conference, QG training course[8] or recommendation). These businesses were therefore already on a journey looking for cyber security solutions.

On the whole, however, businesses rarely cited the risk of breaches and protecting themselves from cyber crime as the reason they had become certified. No businesses cited differentiation via the badge in their marketplace as something which had motivated them. This may be linked to low awareness of the badge. However, some did acknowledge that they now publicise their accreditation.

> *"We put the Cyber Essentials logo in the back of all our proposals and tenders, we've got a paragraph that says you know we've achieved this … We use it as a unique selling point." (Strand A, 1-49, environmental consultancy)*

3.1.4. Risks and opportunities

The current audience and their motivations for becoming certified present both risks and opportunities to the scheme. As described, aside from the experts, businesses tended to lack knowledge and confidence in this area and required support to complete the process. Other businesses like this could potentially be vulnerable to upselling from certifying bodies and IT consultants, and the research found some evidence of this taking place. Some consultants reported observing other companies doing this, and businesses in the sample reported (knowingly and unknowingly) experiencing upselling. For example, some businesses assumed penetration tests and scans were a compulsory part of the Basic accreditation after being sold them as part of a Cyber Essentials 'package'. This scenario may present a risk to the scheme's reputation if businesses discover that they have paid for products or checks that are not necessary to gain certification (see case study #5).

> *"The first two … didn't really offer it, they were using it as a sales tool to offer penetration testing, … so when you ring up they basically say, 'Well, we can do this, but we don't, we do it as part of a more formal package', and then they up-sell from there, so rather than the £300 just for the certificate, they were offering sort of £5,000-£6,000 packages for full penetration testing … which they threw the Cyber Essentials in as like a freebie." (Strand A, 1-49, IT consultant)*

However, this situation also presents opportunities. Some businesses may be happy to pay for additional tests and scans, where they are aware these are not a compulsory part of the certification but recognise the added value these products offer in improving their cyber security. Even if unaware, these practices may result in businesses putting in place more rigorous security measures than they may have done otherwise. Some businesses were also happy to pay for consultants to either guide them through the process, or complete it on their behalf, depending on their skills and needs. Consultants are arguably already playing a key role as messengers informing businesses about the scheme and its benefits, as well as helping them to implement the requirements. Their contacts and expertise could be harnessed to further promote the scheme to a wider range of businesses and increase uptake.

> *"We look at it as a bit of a loss-leader but it's also assisting people." (Strand A, 1-49, IT consultant)*

> *"In order to win the business, the practitioners are having to reduce their daily rate to attract that market. So the practitioners aren't really that interested in training [businesses] because it's not worth any money...they're trying to add it to an additional*

[8] QG Business Solutions are a business consultancy in the procurement standards market. They offer one day training courses which prepare businesses to undertake the Cyber Essentials certification, amongst other services (including the ISO standards). They also accredit certifying bodies for the scheme.

> *service to existing products that they sell or additional services that they sell." (Strand A, 1-49, information security consultant)*

3.2. Businesses' experience of the scheme

Businesses tended to find much of the certification process simple and efficient (see quotes in appendix 6.3). However, they reported facing some challenges during sign up and certification which serve as barriers to take up and can negatively affect businesses' experiences. These barriers presented a greater challenge to businesses that lacked knowledge and confidence, and typically smaller businesses and those from sectors less directly related to IT. Some of these businesses found it easier to pass the entire process to an IT consultant, as is described in the quote below, and therefore engaged less themselves with the scheme. These section now describes businesses experiences of each stage of the sign up and certification process.

> *"Being a complete, total technophobe … I just sort of read about what it was and then downloaded the questionnaire that you had to fill in. Then to be honest from then on … the IT guys that we use generally filling it in and trying to explain to me what on earth it all meant, but a lot of it was slightly over my head about servers and various things like that that I basically didn't understand, but they would then tell me what we had, so that I could fill the form in … some of them I just didn't even understand the question, but obviously the IT guys did … I was still in quite a fog as to what on earth I was really doing." (Strand A, 1-49, Education)*

3.2.1. Signing up

Initial impressions of the website

The overall format and design of the website was seen to be basic and not reflective of a government website. Some businesses reported finding the website difficult to navigate with the long single page format making it harder to find the information they were looking for. Splitting the website into different tabs or pages more clearly could help ease these issues, rather than users needing to scroll down the page. Further information could then be provided on the webpages rather than in downloads. Information needs to be succinct and targeted at businesses and their needs, rather than provided in uploads of policy documents which is how the documents were perceived. Too much text was reported to be both time consuming and off putting. Businesses wanted to be able to quickly and easily gather information on the scheme without spending too much time looking for it.

After an initial assessment of the website and scheme, businesses tended to find it interesting and relevant to them. However smaller businesses could report feeling the scheme seemed less relevant to them and more relevant for medium/large businesses. Presenting the benefits of the scheme could help to clarify this. Being a government backed scheme was of particular interest to participants as they felt it was a trust-worthy scheme due to this association. Businesses responded positively to the HM government logo when this appeared on any materials for the scheme and businesses in the remote testing responded positively to seeing this in documents (though it is not currently included on the Cyber Essentials website).

> *"At no point did I feel the scheme was very clear but I did gather that the website was meant to provide information on what to think about. I didn't feel Cyber Essentials wanted people to sign up at any point."* (Strand Bii, 1-49, Healthcare)

Businesses responded positively to and were engaged with the industry quotes often finding these credible and reputable and appreciated the variety of sources. The quotes highlighted that reputable companies care about their business and customer data which is why they are using the scheme. However, as most quotes were from CEO's of large businesses, some participants from smaller businesses felt it may not be relevant to them. Further quotes are likely to be well received from a wider range of sectors and businesses of different sizes, particularly some smaller businesses to appeal to micro and small businesses. Businesses reported video testimonies are also likely to be well received and engaging.

> *"There's a lot of reading involved, I'm not sure if a video at this stage would be a lot more engaging and show more authenticity."* (Strand Bii, 1-49, Leisure).
>
> *"This says to me it's big organisations doing this…is there anything from small firms?"* (Strand Bii, 1-49, Online Media)

Some businesses questioned why there were not contact details for those who have questions or difficulties. As participants generally found the website fairly difficult to navigate and fairly confusing amongst all the text there was a tendency to look for a contact number so they could speak to someone to help and explain the processes. Adding a chat function and/or email contact address for those with queries about the scheme and requirements would likely be well received – for those having difficulty accessing or understanding the website.

Decision making process

Businesses described how the decision was made to become certified. Two approaches were revealed: either the final decision was made by senior management first who handed the work down to IT managers, or IT managers escalated up to senior management. Handing down occurred where senior managers decided to become certified in order to bid for work and would delegate the work to someone else to find out more information and sign up. Alternatively, escalating up was the approach that tended to be taken where other motivations were driving action (such as personal development), with staff and IT managers playing 'information seeker' and completing all the ground work in terms of finding out more about the scheme, benefits, features and processes, which they would then present to senior management for sign off. This could be due to personal development or hearing about the scheme at a course or conference.

> *"The senior managers were on board as long as they don't have to do the work themselves then they yes, they are keen to get it done and get it in place."* (Strand A, 250+, Charity)

The benefits of the scheme which were presented were in line with the motivators discussed above – becoming accredited was mandatory to bid for government contracts, or the expectation that it would become mandatory and forced down the supply chain. It was presented as a low cost way to retain the ability to bid for high cost contracts and for some would require little effort as their business' security standards already met the requirements.

The perceived low cost of the scheme also influenced some businesses' decisions about the value of the scheme and whether to sign up, particularly those undertaking the scheme as an alternative to the ISO accreditations.

Barriers, risks and opportunities at sign up

Businesses reported that there is currently a lack of clarity about the nature of the scheme, process and requirements and costs at the sign up stage. This serves as a barrier in a context where businesses already have low confidence about the subject matter. Respondents from both strands A and Bii highlighted the difficulty in finding the cost of the scheme on the Cyber Essentials website as this was not provided upfront. In order for participants who had become certified to find out the cost, they had to speak to someone from either the Accrediting Bodies (ABs) or Certifying Bodies (CBs). When businesses were made aware of the costs they tended to consider this to be low and represent good value for money. However, the initial lack of clarity around costs at the start of the process acted as a barrier to sign up, and meant that businesses could be unaware of upselling if this took place. Some businesses in strand B inferred that the lack of transparency about cost meant that the scheme would be expensive and designed for larger businesses rather than SMEs.

> *"It's taken me a while to find out what the costs are…in a way that's put me off a bit."* (Strand Bii, 1-49, Online Media)

Businesses reported that the requirements for the scheme were confusing and not clearly laid out. Businesses across all strands said that this meant they found it difficult to understand what was required of their IT systems in order to be awarded certification. This confusion around requirements was even shared by some IT consultants:

> *"I claim to be an expert in this field with 30 years of experience and I had to look quite closely at the requirements … Other companies approaching this cold would have some difficulties."* (Strand A, 1-49, Cyber security consultant).

Businesses were also unclear about the process they would need to go through, with the selection of ABs and CBs being particularly confusing. This was driven by there being different approaches to the certification process and ABs and CBs selling different packages. As there was not a clear upfront indication of the process, some business had to telephone CBs to gain greater clarity.

Businesses also reported a lack of clarity regarding the distinction between the Basic and Plus certificates and what the added value of Plus was.

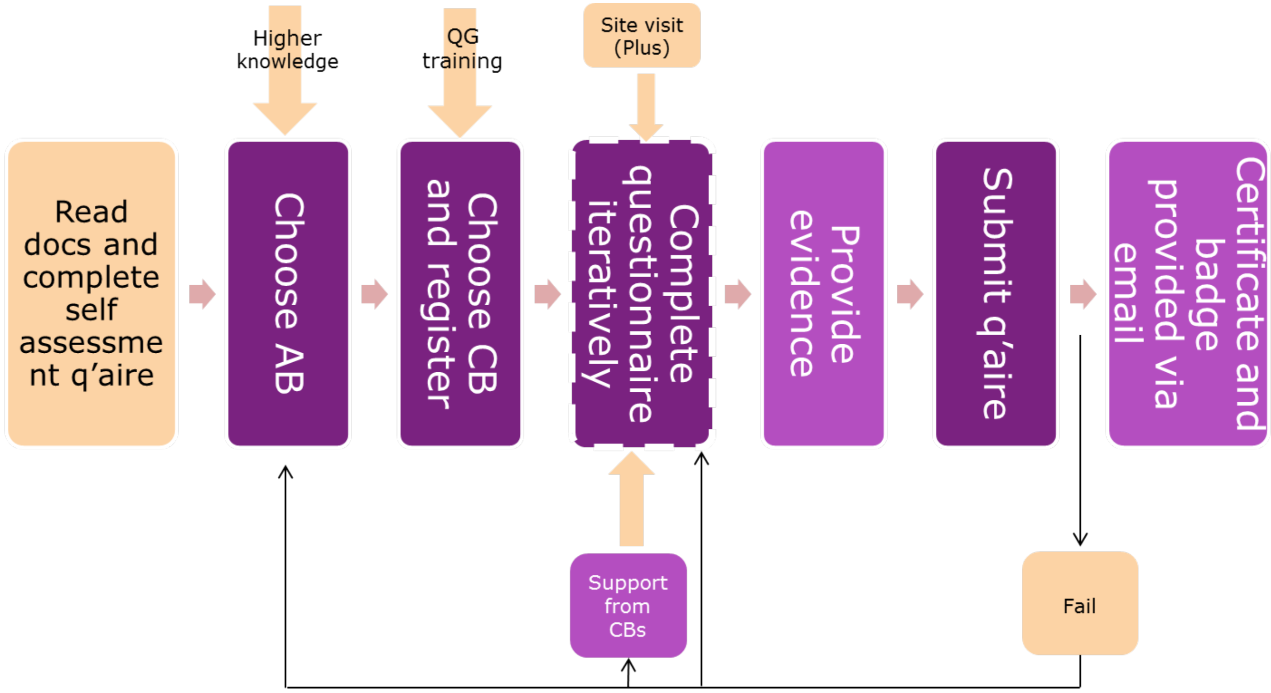
> *"We've achieved the [Basic certificate] so, and that appears to be as much as anybody has ever asked us for ... So, in order to get me to spend money, I would need to have a reason for it." (Strand A, 50-249, Recycling and Waste Management)*

> *"There's a cyber essentials plus, does that make it more secure? In that case, how much more does that cost and what does that say about the cyber essentials … Why is one not as good as the other. If this is a government initiative surely I'd imagine that you'd want 100% protection." (Strand Bii, 1-49, Other)*

3.2.2. Completing the certification

Overall, businesses were generally positive and tended to find the process fairly simple and efficient. However, non-experts lacked confidence at key decision-making points, often exacerbated by the lack of clarity up-front about the steps of the process. Figure 3.2 below illustrates the certification process as described by our participants.

Figure 3.2 – Diagram of the certification process



Businesses tended to start the process by reading the documents and completing the self-assessment questionnaire. However, those with high levels of knowledge and confidence about cyber security and the sector could skip this step and move straight to choosing an AB. Business who undertook the QG training (QG being an AB) moved straight to choosing their CB.

Getting started

Having made the decision to become accredited, respondents took on the role of 'information seeker'. For experts, finding the information required to complete the process was generally considered fairly easy and straightforward. The first part of the process requires businesses to read documents and complete the self-assessment questionnaire on the website. Participants appreciated that the documents were free to download. Some, including IT specialists, found the information provided was useful, particularly where it provided a good checklist of what they needed to do to increase their business' cyber security. Businesses were engaged by and found diagrams included in the documents helpful and accessible as these summarised complicated information.

> *"I think it was quite straightforward and simple and that's the way to keep it."* (Strand A, 250+, Vehicle Sales)
>
> *"Really helpful, I guess it was good in explaining in concise terms what Cyber Essentials scheme is, why it is important, so yes it was really, that's the information I was looking for.* "(Strand A, 50-249, Recruitment)

However a common theme within strands A and Bii, was that the documents were very lengthy, full of jargon and designed for the IT savvy. For non-experts the documents lacked clarity and were difficult to understand. As a result, these businesses may disengage from the process, or delegate it entirely to their IT providers. As the nature of the website is about cyber crime, some participants were unnerved by having to download documents and would prefer the information to be web based because this was seen as less potentially dangerous – particularly the FAQ's section.

> *"This is something I would have to get my IT guy to look at because this seems very complicated."* (Stand Bii, 50-249, Retail)
>
> *"I've been in the IT business a long time, I've got the knowledge and could work my way through, but if you were maybe a smaller company, I could see some of the issues you would be a bit confused."* (Strand A, 50-249, Insurance)
>
> *"Some of the guides are quite heavy, they're more focused towards tech people, which is not a deal breaker for me but I think if I had been a microbusiness or an SME with a more normal level of tech knowledge it might have been more off-putting"* (Strand A, 1-49, Cyber security consultant)

Businesses responded positively to the short self-assessment questionnaire on the website in both Strands A and Bii. Businesses suggested that it was a quick and easy way to assess whether their business was meeting the required standards. The questionnaire tended to encourage businesses to look further into the scheme so that they could address issues where they did not score so well. The questionnaire was a useful way of highlighting what their business was doing correctly when it comes to cyber crime and what else they need to be doing at a basic level. The research suggests some people knew less than they thought they did about their security arrangements, and the questionnaire therefore challenged their assumptions.

> *"I found the questions posed to be useful, topical and a way of assessing my organisation's cyber-readiness."* (Strand Bii, 50-249, Insurance Provider)
>
> *"There was a quick sort of, not quiz but I think they wanted to find out a bit of information, do you meet these requirements? That was useful to know so yes, that's probably lead me on to look more, look into it in further detail."* (Strand A, 250+, Charity)

Businesses also reported that they would like more information about how the score is calculated and a personalised report afterwards, advising on how they can address the issues which are flagged by the questionnaire so that it is clearer what businesses have to do to increase their cyber security and pass the scheme.

> *"The questionnaire was simple and did highlight the fact I didn't know enough about what we do as a business. This was embarrassing to say I am the MD and therefore I decided I would look in to this further."* (Strand Bii, 1-49, Healthcare)
>
> *"I've done the questionnaire, so it was helpful in terms of the summary, 7 out of 12, but what it wasn't clear about was so what are the 5 that I didn't score particularly well on, what would I do about them? "* (Strand Bii, 50-249, Leisure)

Choosing Basics or Plus

After seeking further information from the free downloads and self-assessment questionnaire, businesses had to choose whether to apply for the Basics or Plus certificate.

Some businesses reported difficulties choosing between the options where they found it unclear what the added value of the Plus certification was and what benefits this offers for the additional cost.

> *"The Plus didn't offer too much more except a bit of an internal scan, and to be honest we just wanted to get it through. There was no necessity for the Plus, there was a bit of an extra charge I think, but [DELETED] just wanted to get through so they could continue trading. So there was no requirement for it." (Strand A, 1-49, IT consultant)*

> *"I didn't understand the difference between Cyber Essentials and Cyber Essentials Plus. I've only recently just found out the difference … there's no differentiation as far as I can see on the website." (Strand A, 50-249, energy sector)*

> *"Cyber Essentials Plus is more involved, which would also mean that there would be some operational costs to get the certification." (Strand A, 1-49, risk management)*

Within our sample, the Basics certification could be chosen as a first step to become accredited before progressing onto Plus.

> *"I thought as it was the first time we'd done it, I thought the basic level was the best way to start off with….you have got to start at the beginning. What's the point in going for plus if you don't know the basics."* (Strand A, 250+, Vehicle Sales)

Additionally, government bodies only require Basics for procurement processes. Thus for businesses whose motivation was to be able to bid for government contracts, Basics was considered the easier and cheaper option. The Plus certification was considered a more viable option for larger businesses, those already holding accreditations, and experts.

> *"We didn't need any more than the level 1..... felt that was all I could handle at that time, because the bid itself is quite a big bid, so we were spending every hour of every single day doing it, so the Cyber Essentials to be honest for me at the time was a bit of another job that I have got to do, you know, this is jump through the hoops." (Strand A, 1-49, Education)*

Choosing an accrediting body and certifying body

Experiences of choosing an AB and CB varied depending on the type of business. Whilst cyber experts were able to navigate their options fairly smoothly, given their knowledge of the sector, non-expert businesses found this more challenging. Even after certification, some of these businesses were still unclear about the difference between ABs and CBs and the role they play in the process.

Non-expert businesses could find choosing a provider confusing and time consuming due to the growing number of certifying bodies and their unfamiliarity with these companies. These businesses chose an AB through the Cyber Essentials website by following the links to their homepages, and then found a list of CBs to register with on the AB's website. Confusion reportedly arose from the lack of clear cost information and clarity about their different offers. These businesses tended to assume that the process would be the same whichever CB they used and therefore did not compare. Those who did try to compare tended to find the process onerous.

> *"The list was very long and I also did not really know what I was looking for…I also assumed the price would be relatively similar for that sort of procedure. I hope that's right cause I did not really do price comparison." (Strand A, 1-49, Charity and Think Tank)*

> *"I had an initial conversation with 2 or 3 [CBs], they just seemed to have the best experience on the phone, they seemed quite responsive and receptive and they got back to me quickly … customer service plays a big part doesn't it." (Strand A, 50-249, Recruitment)*

The experience of choosing an AB and CB was different for IT and cyber experts. Their choice tended to be based on previous experience with providers, recommendations from colleagues, or personal contacts. Some IT consultants came through different avenues such as attending a Cyber Essentials practitioner course and would become accredited with the AB who was delivering the course, mainly Quality Guild. In contrast to other businesses, IT consultants had greater familiarity with the sector and were therefore more confident in comparing products and services regarding fees and obtaining value for money. Some questionnaires were recognised as more rigorous or difficult than others; however it was mainly experts who were confident enough to compare these at the outset of their journey. Some who recognised this were looking for the easiest route.

> *"Because one of our guys knew the person at the accreditation body, we just went with someone that one of us knew." (Strand A, 1-49, cyber security consultancy)*

Completing the questionnaire

Those who had been on a Cyber Essentials practitioner training course generally found the process of completing the questionnaire simple. The full day course gave participants a lot of information not only about the scheme but how to complete the questionnaire and what standard the answers were measured against. This meant that participants were well equipped when filling out the questionnaire for their own business, making the process simple and understandable.

However, participants who had not been on this training course – particularly non experts - could encounter some difficulties when completing the questionnaire. Respondents reported that the questionnaire answer codes could be vague, for example using *'always, sometimes, often, never'* scales. This drove dissatisfaction with the process because businesses lacked clarity about what these terms meant, or were anxious that putting the wrong answer could result in failure. Non experts could find the language and requirements in the questionnaire difficult to understand which could mean they needed the help of an IT consultant to complete it, driving up costs. Conversely, IT consultants found this process simple, quick and efficient; but they held expertise and also often already had systems which met the standards.

> *"You have to do your homework to answer all the questions. I rely quite a lot on our IT support company. Some of the questions in there, I wouldn't be able to answer myself. "* (Strand A, 1-49, Risk Analysis Consultancy).

Businesses who had conducted comparison were aware that questionnaires provided by the CBs vary and this had an impact on participants' experience of the process. Some questionnaires were longer or considered to be more complex than others. This was viewed negatively, particularly by consultants, as businesses expected a standardised questionnaire to be used for a uniform accreditation.

> *"It makes a bit of a farce of the fact that it's not really a standard, it's not a consistent standard anyway."* (Stand A, 1-49, Cyber Security Consultancy)

> *"Subsequently I'm aware that their people - the accreditation bodies ask different questions and personally I find that nuts. I don't understand why they're all asking different things; it should be one and standard for all."* (Strand A, 1-49, IT Consultancy)

'Plus Certificate' site visits

For businesses that completed the Plus accreditation, as well as completing the self-assessment questionnaire, they were required to have a consultant from their CB conduct an onsite visit and a scan to test the business' systems.

Businesses can face challenges at this stage. For example, during a visit a business had to set up a mirror system for the assessor to complete the test (instead of on their live systems due to the sensitive material they hold) which disabled their security and caused their systems to stop working. This issue, as well as not having any of their documents or policies checked by the assessor, was met with frustration. There is a risk that these types of negative experiences with assessors and their processes could affect the credibility of the scheme.

> *"There were some of the tests that he couldn't perform, and I remember being really, really gobsmacked by this – that we had to disable some parts of our security so that he could perform one of the tests." (Strand A, 1- 49, IT Consultancy).*

Submitting evidence

Businesses provide evidence for some of their answers to their questionnaire to demonstrate they have the right measures, policies or standards in place. Evidence usually consisted of policy documents, screenshots (e.g. of firewalls) and paperwork detailing IT security in place. Businesses did not tend to report difficulties collecting or providing the types of evidence required. However businesses, particularly experts, reported awareness of varying levels of evidence being required from different CBs. This drove dissatisfaction amongst some participants who believed there should be a standardised approach to evidence and that this could be a risk to the credibility of the scheme.

> *"I just said, well, do you want to review any of the documents? He said, oh, no; I don't do any of that part. And that actually made me a little bit annoyed only because I just thought, well, actually, I could have written anything on those documents. I could have just written the attached, you know, access control dot pdf. And would they have accepted it? And when I saw that, I just thought that doesn't give me any real assurance or how is that giving you assurance that I have these controls in place?"* (Strand A, 1-49, auditing)

> *"It varies across all the different certification bodies and I think this is really quite dangerous because I found out the other day that … the organisations that does it literally you just say yes to things and don't have to provide evidence and if that's the case that's pointless … I think that's really dangerous because if people are looking at that badge there are going to be people like me that have done it and its secure … and then there are going to be organisations like that one that's being used and … companies aren't secure … there's a real difference between compliance and ticking boxes." (Strand A, 1-49, cyber security consultant)*

Once the questionnaire is complete and evidence had been collected, businesses submit this to their CB via email. This tended to be an iterative process with businesses sending their questionnaire and evidence back and forth for review before the final submission and with CBs providing varying levels of advice and assistance on requirements and what evidence was required to demonstrate compliance.

Actions taken to complete the certification

Businesses in the sample tended to have taken some action and made some changes to their practices and systems in order to pass the accreditation. However these changes were generally considered to be relatively minor and not too burdensome. Businesses considered this to take minimal time and incurred little to no extra cost. For example, one business had to deliver all staff training on cyber security in which staff were taught about the systems in place and advised not to click on certain email links and go on to blocked websites.

> *"We handed out information booklets to each of them to read and, just make sure they're aware of what they were doing."* (Strand A, 1-49, Pharmaceuticals)

Other examples of actions taken were changing password procedures so that passwords are changed automatically every six weeks. Additionally businesses were required to tidy up and update other policies and document procedures to prove they were meeting the requirements.

Process for those who fail

The research indicates that some businesses do fail first time. The business which failed first time in the sample was given a report which outlined the areas they complied with and the areas they didn't comply with which ultimately led them to fail. They failed after having a vulnerability scan. The participant was surprised to have failed and felt that more support could have been provided by the CB in order to help them pass first time (see case study #2).

> *"There was very little explanation of what was actually going to happen. I think it was quite obvious that my IT knowledge is absolutely basic, and there was not any support there."* (Strand A, 1-49, Charity and Think Tank).

A re-application fee was paid to complete the questionnaire again and while they completed the process with the same CB, they could have started again and reapplied with a different AB and CB. The reapplication fee was communicated up front so they were aware how much it would cost to reapply and this was cheaper than going elsewhere and starting again.

Completing the process

Businesses reported different experiences of the end of the process. Generally, this was considered to be quick and simple with businesses receiving their certificate and badge as standard via email, with notes on how to advertise the scheme. However, others had different experiences such as not hearing back from their CB with their results and having to call them and having to send their certificate back multiple times due to the name being incorrect. Where this occurred it was considered anti-climactic and a further hurdle at the end of the process.

3.2.3. Service from CBs

Businesses reported that varying levels of support were provided across CBs and varying levels of satisfaction with them. While some businesses had received support throughout the process, particularly with filling in and understanding the questionnaire, others reported being left to fill it in by themselves.

Businesses who were positive about the level of support from their CB would often attribute this to having a point of contact and being able to ask questions. This was considered important particularly around the stage of the questionnaire process when businesses often needed clarification or extra support. These businesses were able to send the questionnaire back and forth with their CB, making iterations until the questionnaire was at the right level for final submission. This approach was valued as it helped to enable businesses to pass first time and was considered quick, easy and friendly (see case study #1).

> *"If there was something which was maybe a miss or wrong, by them reviewing it, they came back and said OK for us to pass it you need to go and look at your processes. So we wouldn't have submitted it and got a failure and then had to pay for submission again."* (Strand A, 50-249, Insurance)

Conversely, other businesses reported poor levels of support from their CB, particularly non-experts who felt more could have been done to support them through the process (see case study #2). However, businesses who had passed first time could also feel they had not received as much support as they expected or needed.

> *"You're paying out the best part of £500, there's no guarantee you're going to pass it and no offer of any technical support."* (Strand A, 1-49, Other, P12).

Some businesses are happy to receive less assistance, particularly experts. However they could be sceptical about the services provided by some CBs who would upsell their services to businesses with lower knowledge. These negative experiences from having little support from CBs and business awareness of high cost upselling can damage the credibility of the scheme, or likelihood of renewal.

3.2.4. Costs, benefits, and value of the scheme

Overall the scheme tends to be seen as good value for money. However, when weighing up costs and benefits, value tends to be understood in terms of the context of the new business opportunities the scheme presents. A few hundred pounds is seen as a minimal amount to pay to be able to win big contracts with government departments and not in terms of the value of protecting the business against cyber threats and breaches and the costs, financial and otherwise, that they might incur from this. Those who fail are less likely to see the scheme as good value, especially if they have to pay for upsold products in order to pass.

> *"In terms of value it's excellent, because for £300 I've managed to maintain my opportunity to do trade with [a government department]."* (Strand A, 1-49, Engineering)

Costs

Costs reported by participants were the initial price, upsold products (e.g. scans and penetration tests), consultancy time and business' own time. The initial price was seen to be fair because £300 was compared to the price of other more expensive accreditations, notably the ISO accreditations, and the value of new business which could be obtained as a result. Businesses tended to report paying £300-£350 +VAT for the Basic certificate, but some businesses reported £500-£800. They reported figures between £500-£1,500 for the Plus certificate. Businesses tended to report paying £1,000-£4,000 to consultants, although some have paid less than £500 and one business £7,000. It could be difficult for businesses to estimate how much time they had spent on the certification, and for some this was the first time they had tried to calculate time and cost spent. Businesses tended to estimate 1-4 days, but it could be 2-3 hours. Some businesses reported spending 10-14 days, and this tended to be larger businesses and those experiencing issues with Macs or other system issues.

> *"It's low, very low....Well, if we were looking for obtaining certification for the ISO 27001 framework, we'd be looking at 100 to 150 thousand k. So if you want to put that in a context."* (Strand A, 250+, Education)

Costs could be seen to be unfair when ABs and CBs were trying to upsell products and services which could add on extra hundreds or thousands of pounds to become accredited. This created negative views of the scheme among those who were aware that these extra products and services were not necessary as it was seen to be unfair that there wasn't a standardised system in place. Those who were aware of upselling could still see this to be good value where they appreciated the value of the products.

Businesses' time did not tend to be considered as an extra cost. This was less relevant to consultants and IT companies who would have been doing this kind of work anyway. However even IT managers within businesses did not consider their staff time as an extra cost as it is part of their job to make sure these systems and measures are in place and it wouldn't be the sole focus of their work anyway. Some smaller businesses and charities with less staff resource considered this as a burden when they had other priorities and tasks to do.

> *"It is part of the processes that we do anyway so I would have reviewed our IT processes at some point, whether it was with the cyber essentials in mind or not."* (Strand A, 250+, Vehicle Sales).

Benefits

As mentioned above, the perceived benefits of the scheme were usually focused around the new business opportunities that the scheme presents. IT consultants saw Cyber Essentials as a way of investing in their business because this is a product they can then offer to others. However, other benefits were reported from taking part in the scheme.

> *"As an enabler I can now offer it to my other clients. There is a value for us because effectively...we can offer it as a service, so helping our clients move towards it. That's a value."* (Strand A, 1-49, Managed Service Provider).

> *"It's another revenue stream because I can go and consult in it now because by getting certified myself and doing practitioner training I can now go and consult in that as well."* (Strand A, 1-49, Teaching and Consultancy)

An additional benefit reported by participants was that the Cyber Essentials scheme is cheaper than ISO and can act as a stepping stone towards it. Businesses were interested in gaining the ISO 27001 certification however due to cost and length, Cyber Essentials was seen as a cheaper and simpler option. Once they had completed the Cyber Essentials Scheme, businesses would have less to do for the ISO accreditation as their systems would already be at the correct standards. For other businesses, the ISO accreditation was not seen as appropriate for the size of their business and so Cyber Essentials was considered a more suitable option.

Some participants mentioned improved systems, knowledge and confidence from having taken part in the scheme. This was particularly those with low knowledge who had completed the scheme themselves; those who made more changes to their systems; and those who had previously suffered cyber-attacks.

> *"The immediate benefit was that it was a way to make sure independently that our network was up to snuff…of a suitable standard and secure."* (Strand A, 50-249, Scientific Research)

> *"I certainly feel more secure because it's sort of like unconscious incompetence, suddenly you go on some training and it becomes conscious incompetence and then you go and do something about it and then you like think okay I'm consciously competent now."* (Strand A, 1-49, Teaching and Consultancy)

Less commonly, some businesses mentioned the scheme to their suppliers and were now more aware of the cyber security of other companies they interact with. Having gone through the scheme and put the standards in place, businesses wanted to know that their suppliers were also doing the same so that by default they were less likely to receive a security threat. As a result, businesses could encourage their suppliers to sign up.

> *"We want to know that you've thought seriously about your protection because by default then we're getting less spam from the connection of you talking to us."* (Strand A, 1-49, Cyber Security Consultancy)

3.2.5. Impact of the scheme

When assessing the impact of the scheme, businesses were often not aware of whether any attacks had been prevented after becoming accredited with the scheme. The exception was for those who had suffered attacks in the past and could anecdotally say they had not had any further attacks so far. None of the businesses reported any impact on insurance premiums. Discussions about impact tended to focus on new business bids and wins. Some businesses mentioned that their staff were better informed and that practices had improved.

3.2.6. Risks and opportunities

Some of the barriers reported regarding the process evaluation have implications and pose risks to the future success of the scheme: most notably, the lack of clarity about costs, requirements, process and inconsistent levels of support and other inconsistencies in the process (particularly the length and complexity of the questionnaire). Given businesses' general lack of familiarity with the cyber security market, the lack of clarity about costs and the process means that businesses can be vulnerable to paying for non-mandatory products (e.g. scans and penetration tests). This can be done by both CBs themselves but also opportunistic consultants, who are aware that businesses need help to get through the process and offer their services as an extra source of revenue. This means that businesses with little knowledge in this area are paying for more than just the cost of the accreditation itself but also added extras which they are unaware of. This could potentially be risky for the scheme as they can damage its reputation and credibility within the industry and among businesses more widely. However, if greater transparency were encouraged around costings and products, then additional products and services could present added opportunities for businesses to improve their protection levels, where they choose to invest in this.

Additionally, a lack of consistent service means that businesses may be dissatisfied with the service from their CB. As mentioned previously, businesses reported different experiences and levels of support. Those with lower level knowledge can attribute their failings or difficulties with the scheme to being under-supported by their CB which leaves them feeling frustrated with the scheme. The cyber industry also finds the lack of consistency less credible, which may damage the scheme's reputation or mean these businesses will be less willing to recommend it to others.

However, there are also opportunities for the success of the scheme which have been reported. In a market place where businesses can be unsure of who to trust, government backing offers reassurance to businesses. This is a unique selling point of the scheme as it is viewed as a trustworthy source in a context where there are lots of unknowns.

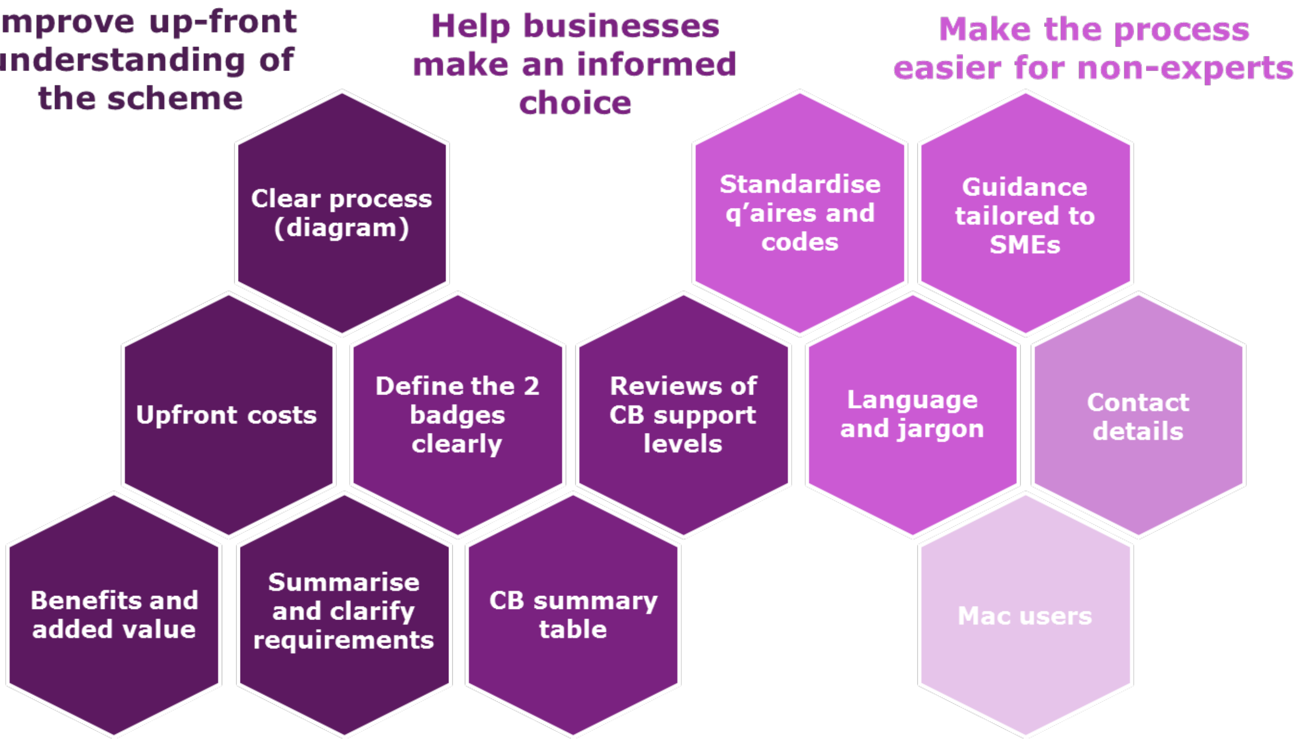
The iterative feedback from CBs when completing the questionnaire gave businesses the opportunity to learn more about cyber security. Being able to reflect on the feedback and make changes before submitting the final questionnaire made the process more engaging, educational and flexible. It also allowed businesses the opportunity to improve their IT systems, further protecting themselves from cyber threats. This was possible to a greater degree where businesses were able to complete the process themselves rather than relying on IT consultants, which serves as further reason to simplify the scheme (or at least the supporting documents) to make it more accessible for non-experts.

> *"I think it's been a useful experience. I think it's been helpful in getting our business on track with IT security." (Strand A, 50-249, Recycling and Waste Management)*

3.3. Suggested improvements to the scheme

The research found that there are some key areas where improvements could be made which could further engage businesses and increase uptake. Improvements could address the risks outlined above and protect the reputation and credibility of the scheme. The recommendations are summarised in Figure 3.3 below.

Figure 3.3: Summary of recommendations


Improve up-front understanding of the scheme
Help businesses make an informed choice
Make the process easier for non-experts
Clear process (diagram)
Standardise q'aires and codes
Guidance tailored to SMEs
Upfront costs
Define the 2 badges clearly
Reviews of CB support levels
Language and jargon
Contact details
Benefits and added value
Summarise and clarify requirements
CB summary table
Mac users

3.3.1. Suggested improvements to the completion process (process evaluation)

Improve up-front understanding of the scheme

Businesses' understanding of the scheme is important because it shapes their initial impression of the scheme, influences whether they sign up or not, and sets their expectations for the process ahead (in turn shaping their level of satisfaction).

> *"… marketing is always poor from that side so if you were to market it better that would, or market it at all that would help … By showing companies why they need it and why it's a good product and why it's cheaper than everything else and the training, by pointing out the benefits of it, they don't do that at all … in a business there's got to be a benefit otherwise you're spending money and time on doing something that you're not going to get any benefit from." (Strand A, 1-49, cyber security consultant)*

- Clarify the value and benefits of the scheme to businesses upfront , including how they can protect themselves from cyber threats
- Clarify costs of the scheme upfront – not only the cost of the certificate, but including an indication of associated costs and resources which will likely be required. This will support more informed decision making about the likely cost of accreditation, as well as differences between offers from CBs or other providers.
- Improve upfront understanding of the scheme by:
  - using consistent descriptions and language about what the scheme is
  - using an infographic or process diagram to summarise the process of certification, indicating the length of time each stage is likely to take, where businesses might wish to seek support (e.g. from consultants or IT services), and the form that support could take
  - providing a 'check list' to outline the requirements in simple language

- Signposting to further information (i.e. more technical information about the requirements and what is required to implement these at the practical level) can then be provided for those who want this, and for IT providers carrying out the process on behalf of businesses.

  "I would prefer a flowchart approach which made it clear which steps were required to achieve one of the badges and then what I could use the badges for." (Strand Bii, 50-249, Other)

Help businesses to make informed choices

Improvements could be made to the materials and website which could help businesses make more informed choices during the process. Helping businesses make informed choices could help them gain greater value from the scheme and increase satisfaction with it.

- Provide greater clarity about the difference between Basics and Plus
  - Outline the added value and benefits of Plus
- Outline clearly the difference between ABs and CBs - and explain their role in the process for businesses
- Provide a comparison table or tool (in the style of a comparison website) which enables businesses to compare CBs and select the one which is most appropriate for their needs
  - This should include costs of Basic and Plus, additional products and services they provide, length of questionnaire (if this is not standardised or where there are additional optional questions), and an indication of the level of support provided
  - Include customer service reviews and scores/ratings (this may help to improve the level of service being provided overall if CBs are aware feedback is being left publically)

Improve the completion process for non-experts

Businesses, particularly consultants from the cyber security sector, reported dissatisfaction and concern that CBs currently use different length questionnaires, different answer codes and require different types and levels of evidence. Standardisation and more guidance about answer codes could help some businesses complete the process with less assistance from IT consultants, therefore increasing their learning about cyber security and their systems during the process. Making the process simpler and clearer could make the scheme more engaging for businesses as well as reducing anxiety and confusion and improving overall experience.

- Standardise the questionnaire
  - Standardise the length of the core questionnaire
  - Allow CBs to add extra questions to help businesses improve their cyber security as long as this is transparent
  - Standardise evidence requirements and set out instructions clearly
  - Communicate any changes to the cyber security industry to reassure those concerned about the rigour of the scheme
- Standardise approach to answer codes
  - provide guidance on what is required to pass and model answers for how to fill in the answer codes (businesses tended to prefer open answer codes)
- Provide options for greater support from CBs for non experts
- Simplify the language used in materials, on the website, in documents and the questionnaire
  - this should be jargon free and in plain English as far as possible
  - Reduce the amount of text used where possible

    - Do not use policy style documents

Other improvements to the website

The website testing (strand Bii) showed there are other aspects of the website that are working well and engaging businesses to sign up and continue with the scheme. The findings of the website testing reflected all of the suggestions above, and also revealed the following:

- Split the website into different tabs or pages rather than users needing to scroll down the page.
    - Further information could then be provided on the webpages rather than in downloads.
- The website could set out clearly the benefits and added value of the scheme to businesses through case studies of a variety of businesses from different sectors and sizes
    - this could also be done by video to try and reduce text on the page.
- Businesses expressed that they would like the HM Government logo to be displayed more clearly on the webpage to shows it's affiliation with government and increase trust of the website, in a marketplace where businesses are unsure who to trust.
- Provide a tailored report after completing the questionnaire on the website with further explanation of what businesses have to do to increase their cyber security and pass the scheme.
- Further quotes are likely to be well received from a wider range of sectors and businesses of different sizes
    - particularly some smaller businesses to appeal to micro and small businesses. Video testimonies are also likely to be well received and engaging.
- Adding a chat function and/or email contact address for those with queries about the scheme and requirements would likely be well received.
- Less text / more images
    - too much text is both time consuming and off putting.

4. Recommendations for improving messaging and engaging a wider audience

This section explores ways in which to improve the effectiveness of communications about Cyber Essentials to engage a wider audience with the scheme, with implications for communicating with businesses about cyber security more generally. It outlines findings derived primarily from the communications testing with businesses that had not completed the certification and usually had not heard of the scheme. The recommendations are strongly supported by findings from the other strands and build upon the findings outlined so far. Section 4.1 explores perceptions of cyber crime and the risk this poses to businesses; section 4.2 presents three key messaging principles; then section 4.3 outlines a typology of businesses and their different messaging needs; before the chapter presents findings regarding language, tone, imagery and the leaflet and online ad specifically. It finally makes recommendations about preferred communication channels. The chapter then summarises recommendations derived from across all three strands of the research.

The communications testing revealed three key messaging principles: businesses need to be convinced that cyber crime is a real and relevant threat; understand what Cyber Essentials is and what it offers to address this threat; and understand the cost and requirements. Beyond these three principles, messages can be tailored to engage businesses based on their size, level of knowledge about cyber crime, and their perception of the risk this poses to their business.

4.1. Perceptions of risk

The message testing groups began by exploring participants' understanding of cyber crime and the risk this poses to their business and UK businesses more widely. Participants were also asked about their understanding of protection measures, what measures they have in place and whether and how they have looked for information about this topic. This provided key context to help understand what was driving business' responses to the messages and materials.

Businesses were aware of cyber crime and characterised it as a growing threat to UK businesses. High profile cases of cyber attacks were mentioned spontaneously (e.g. Talk Talk), and businesses mentioned hearing it increasingly reported in the press. Some small businesses had personally experienced single cyber attacks, such as e-mail hacking. Some medium size businesses reported being aware that they suffer cyber attacks on a regular basis, including malware and phishing attacks on a weekly basis, attacks from global locations, and in one case being hacked by a competitor.

> *"We always seem to be every week now seem to be getting sort of these dodgy emails – phishing. There's malware; spyware … it's just on the general increase." (Strand Bi, 50-250, London)*

> *"I think I've known it as a threat; I've seen it on the news that it can be a threat. But I think just sitting down here and talking about it has just put that seed in there." (Strand Bi, 50-249, Birmingham)*

Though awareness was high, understanding of cyber crime varied amongst businesses, and tended to be higher amongst the larger SMEs. Respondents defined cyber crime as any crime which takes place online for financial gain. It was mainly associated with data theft and breaches, password attacks, theft of personal and financial details and hacking (including of social media accounts among small businesses). Medium size businesses also mentioned staff stealing data. Small businesses associated images or icons of padlocks with secure websites and some said they look out for this reassuring symbol as a symbol of 'cyber security'. Businesses were also aware of some basic cyber security measures.[9]

> *"It's not your area of expertise is it? It's like you need somebody that knows what they're doing." (Strand Bi, 1-49, Birmingham)*

> *"You know that little lock, if that's on a website, then I think it's quite secure, I think that links up for me to be cyber protected." (Strand Bi, 1-49, London)*

Despite growing awareness and experience of attacks, businesses did not necessarily perceive cyber crime to be a relevant or pressing threat to them and their business. This was particularly the case amongst sole traders and micro businesses, who perceived themselves as too small to attract the attention of cyber criminals compared to larger firms. Other businesses felt that their sector excluded them from risk, associating banking, finance and IT as the sectors most likely to be targeted for cyber attacks. Businesses that did not trade online also downplayed their risk, despite using networked computers or other online tools. Meanwhile, some medium size businesses did not engage with the threat of cyber crime because they assumed this was something their IT team or IT consultant would be dealing with (despite not actually having confirmed this was the case). These individuals tended to have almost completely divested responsibility for cyber security to others.

> *"I think because I'm a small business I just think there's always somebody bigger out there to, you know what would they really want to take, apart from my banking really?" (Strand Bi, 1-49, Birmingham)*

> *"You think it's never going to happen to you. You hear it all the time but it's never close to home." (Strand Bi, 1-49, London)*

> *"I think it's whether you think you should take them...Because we've got an IT company who's supposed to look after this for me." (Strand Bi, 50-249, Birmingham)*

Given the widespread downplaying of risk, actions taken to increase cyber security were generally minimal. Generally assuming that IT teams were taking care of the issue, medium sized businesses tended to have nominally sought information, sometimes from government sources and websites, though had not engaged with it deeply. Businesses across all strands of research reported that information about the topic was overwhelming and often conflicting, and that they didn't know who to trust. Businesses often suspected that companies offering cyber security support could in fact be phishing operations masquerading as legitimate businesses.

Smaller businesses, particularly sole traders and micro businesses, tended to perceive themselves as too busy to take action on cyber crime, with a great deal of competing priorities

[9] The following measures were commonly mentioned: anti-virus software, firewalls, secure passwords, logging out of programmes, not allowing others to use your personal computer or accounts, protecting your screen in public, and protecting removal media (among medium businesses).

on their time and fewer staff to delegate to. They had sometimes assumed that installing anti-virus software was adequate protection for them and were unlikely to have further measures in place. Small businesses worried that they did not know enough about the topic, but were unsure about where to turn for advice.

> *"It have other things to do, it's not the number one thing on my agenda." (Strand Bi, 1-49, London)*

These findings echo previous research exploring reasons why businesses do not take greater action to protect themselves from cyber security threats.[10] Despite being aware of the threat, SMEs in this research did not perceive the threat to be relevant to them, and were not taking personal responsibility for this issue. This was in part due to the fact that media coverage predominantly focuses on high profile breaches of large businesses, but also because businesses lacked the knowledge or confidence to make decisions about appropriate support. Any messaging about cyber security should take this as a starting point and attempt to overcome businesses' assumptions of safety, as well as provide guidance and reassurance.

The implications of businesses' attitude to risk are explored below, in terms of the ways in which SMEs responded to messaging about cyber crime and the Cyber Essentials scheme.

4.2. Principles for cyber security messaging

In the strand Bi focus groups, the following were tested with small and medium sized businesses:

- headline messages about the threat of cyber crime;
- key messages regarding the Cyber Essentials scheme;
- a leaflet and online ad about the scheme.

Messages included a mix of those already used to communicate about Cyber Essentials, and some developed specifically for the research. These were adapted following phase 1, based on feedback about which messages which were seen to be more or less engaging.[11]

The message testing revealed three key messaging principles to more effectively engage businesses with the scheme and issue: (1) businesses need to be convinced that cyber crime is a real and relevant threat; (2) messages should clarify what Cyber Essentials is and what it offers; and (as outlined in the previous sections) (3) messages should clearly communicate the cost and requirements of the scheme.

4.2.1. Convince businesses cyber crime is a real and relevant threat

Before businesses will pay attention to any specific messaging about the scheme, messaging first needs to convince businesses that cyber crime is a real and urgent threat to them. Messages that were most effective included those that:

- prompted businesses to imagine an attack happening to them, by providing tangible examples of attacks and details of the impacts (e.g. messages 7, 9, 11 and 12 in phase 2)
- conveyed the level of threat (e.g. message 1 in phase 2)

[10] Using behavioural insights to improve the public's use of cyber security best practices, Summary report, Government Office for Science, 2014.

[11] The messages and stimulus material shown to businesses can be found in Appendix 6.6. The research found that small and medium size businesses responded slightly differently to the messages presented to them. A high level summary of their responses can be found in Appendix 6.1.

- presented cyber crime as a threat to businesses of similar sizes to them (e.g. message 8 in phase 2)
- presented cyber crime as a threat to sectors outside those typically associated with cyber crime (IT, banking and finance, etc.) (e.g. messages 3, 11 and 12 in phase 2).

Tangible examples of the impact of an attack were effective at engaging businesses, particularly messages or case studies concerning the financial costs, loss of time and reputational damage an attack can cause.[12] Loss of reputation was particularly compelling for small businesses, some of whom said they relied on this amongst relatively small networks. Citing the impacts of an attack made the threat seem more real to businesses, and was found to be much more effective than describing the nature of the threat (particularly when this is done in technical language). Explaining the nature of the possible crimes was less powerful in part because businesses already tended to have some awareness of this, but also as they were often confused by some of the descriptions, which were seen as too technical (e.g. message 2 in phase 2 which described a Distributed Denial of Service attack).[13]

> *"I think it wouldn't alarm me enough, I think, because it doesn't necessarily spell out great danger in terms of, doesn't specify how bad the attack is."[14] (Strand Bi, 1-49, Birmingham)*

Effective messages conveyed the level of the threat to businesses. As stated, businesses tended to discount the level of threat they (personally) faced. Some of the figures included in the testing were impactful and engaged businesses because they were surprisingly high and induced fear. This notably included the message: *"1 in 4 businesses experienced a cyber breach / attack in the past 12 months".* This message and scaling worked well across sizes and locations because the format "1 in 4" was both memorable and more relatable than averages and percentages – for example businesses understood that this meant at least one of them in the group. Businesses were slightly less engaged by percentages indicating the level of threat, and were more likely to question the provenance or details of the statistic.

> *"25% of businesses experience that, that's a hell of a lot. So yes, you would question it, what type of businesses, could it be me?" (Strand Bi, 1-49, London)*

> *"It's better to have one in four, one in six, one in nine.... Because you're relating to small numbers, so 60% of what? 50% of what?" (Strand Bi, 50-249, Birmingham)*

Messages should also show businesses that cyber crime is relevant to 'businesses like them', that is of similar sizes or sectors – for example message 8 in phase 2 *("New Government research shows 51% of medium-sized businesses detected one or more cyber security breaches in the last 12 months").* The testing found that businesses engaged with case studies which are as tailored as possible, to demonstrate that their type of business is at risk. For example, small and micro businesses were less convinced by case studies about medium sized businesses, and vice versa – and all found large business case studies harder to relate

[12] (1) A cyber attack can cause disruption, loss of time, loss of company and client data, put off customers, be a barrier to growth and causes damage to a business' capacity to trade and reputation as well as having financial costs. It could also be reported in the local media. Attacks could breach the Data Protection Act and lead to fines from the Information Commissioner. (2) A cyber attack in October 2015 meant Talk Talk saw the personal data of nearly 160,000 customers being accessed. They lost 101,000 subscribers in the third quarter and took on fewer new customers after temporarily shutting down online sales channels. The attack cost £42 million and Talk Talk saw their full year profits more than halve. (3) A rival company collected information about a small manufacturing company via social media, malware in emails and a stolen laptop. They used this to access the company network and steal information about a bid. They used stolen intellectual property to produce a lower bid and the company lost out on the contract. Without the contract, half of the employees were made redundant.

[13] 16% of small businesses were hit by 'Distributed Denial of Service' attacks in the last year – which cause your website to go offline, preventing customers from accessing your website and making purchases. The attack could also prevent staff from accessing the internet, sending/receiving emails and accessing company data held online.

[14] 1 in 4 businesses experienced a cyber breach / attack in the past 12 months

to. Case studies and examples should therefore be from a wide range of sectors, circumstances and different size businesses.

Conversely, businesses tended to dismiss messages that described cyber crime in general rather than specific terms.[15] Businesses were also sceptical of messages using percentages and averages, finding statistics easier to reason with or argue against than individual examples or case studies (e.g. message 4 in phase 2 – *"59% of businesses expect there will be more security incidents in the next year than last"*). Businesses responded less well to these kinds of messages, were more likely to question their source, and were less able to see the threat as relevant to themselves.

4.2.2. Convey what the Cyber Essentials Scheme is and what it offers

Messaging about the scheme then needs to convey what the scheme is and what solution it offers businesses to address the threat which has been outlined.

The current messaging about Cyber Essentials caused some confusion about the nature of the scheme. After reading all the messages, including the leaflet introducing the scheme, some small businesses thought Cyber Essentials was a piece of software they could install, similar to anti-virus software. The additional explanatory messages about the scheme included in phase two largely worked well to avoid this confusion[16]. However some businesses in phase two again questioned whether software was provided in response to mentions of 'freely available software' in the leaflet. Without clear and consistent information about the scheme, businesses may make assumptions about what it is. Misinterpretation may lead to disappointment if businesses confuse the offer; for example when businesses realised that Cyber Essentials was not a piece of software they were less enthusiastic about the scheme. This is within a context where businesses perceive it to be difficult to address cyber crime and may not feel confident taking action themselves – they were less enthusiastic about having to take more of an active role in implementing the scheme.

> *"It's informative but not active… it informs you but it won't do it for you." (Strand Bi, 1-49, London)*

As described in chapters 2 and 3, messaging also needs to set out clearly what the process and requirements are for the scheme, to set expectations and outline the solutions the scheme offers to address the threat of cyber crime effectively. Businesses reported that they were unsure what the benefits of the scheme were to them. As in the other strands, they were confused about the process and requirements and requested further information about this. As well as more information about the scheme and its nature, message 13 was added in phase two: *"The Cyber Essentials scheme checks whether your business meets 5 basic cyber security requirements. You become certified when you meet these requirements".* This worked well and also served as a call to action because businesses wanted to check whether they met the requirements in response to this.

Across all communications about Cyber Essentials, consistent terminology regarding the requirements should be employed as far as possible. Businesses were confused about the difference between 'essentials', 'steps' and 'requirements' and why there were sometimes five and sometimes ten of these. The nature of the scheme and its key requirements should be

[15] For example: (1) Cyber crime is a growing threat to UK businesses – criminals target customer data, company finances, and the safety and integrity of IT systems. (4) By taking action on cyber security you can protect customer data, company finances and the safety and integrity of IT systems.

16 (13) The Cyber Essentials scheme checks whether your business meets 5 basic cyber security requirements. You become certified when you meet these requirements.

described consistently, rather than trying to describe different elements at once and using similar terminology.

> *"Just set out nice and plain....Yes what you need to have, there's the 5 steps, and you just think, right I can … that's simple to do." (Strand Bi, 1-49, Birmingham)*

The messaging crucially also needs to set out clearly the benefits to businesses themselves of completing the certification. Businesses reported that currently the benefits are not clear from the materials or on the website and therefore messages do not convey the value of the scheme to businesses. The benefits should be up front to make clear how the certification will be useful and valuable to businesses, to drive sign up. Messages focussing on growth (message 19), for example, worked well because it responded to businesses needs and priorities specifically[17].

> *"[Message 19] makes me feel that the product can be viewed as a vital asset and not a liability." (Strand Bi, 1-49, London)*

4.2.3. Outline the cost and requirements of the scheme

Messaging then needs to build on this foundation communicating the nature of the scheme, and outline clearly the cost and requirements. This information is important to businesses' decisions about whether to proceed and sign up.

As outlined in chapter 3, businesses were frustrated that the cost of the scheme was not provided clearly up front. The message testing suggests that businesses on the whole think around £300 is a reasonable price for the scheme, and thought this should be advertised on the website. More informed businesses (tending to be medium businesses) recognised that the cost makes Cyber Essentials a cheaper alternative to other cyber protection schemes and products on the market. After discussing the other messages, businesses could also recognise that this was cheaper than the potential cost of an attack, although they did not make this comparison spontaneously (as discussed in chapters 2 and 3). The message testing showed that it is possible to drive businesses to make this comparison when they are provided with both pieces of information to make this assessment (the cost of the scheme and an attack). Without it, businesses lacked awareness as to what they could expect the cost of an attack to be.

> *"If I thought … I was going to get fined thousands, £300 is tiny." (Strand Bi, 1-49, Birmingham)*

In fact, not providing cost information clearly upfront can raise suspicion among business as to why this has not been done, given it is considered vital information. In the absence of cost information, small businesses in particular assumed that the scheme was more expensive. Similarly, any confusion around cost information could spark cynicism about the scheme. For example, businesses were confused that the scheme was described as 'cost-effective', yet other messages about aspects of the scheme described it as 'free'. This was perceived as misleading and led some businesses to distrust the scheme.

> *"I think once you see the word free it just brings up this association that you think everything is going to be free." (Strand Bi, 50-250, London)*

> *"I did expect to pay for something – nothing's for free … I want to see the cost now." (Strand Bi, 50-250, London)*

[17] We are supporting business productivity and growth through improved cyber behaviours.

To avoid frustrating and putting them off, businesses also need to know what the process and requirements are, in order to assess whether they can implement the requirements and what the costs of doing this for this business might be for them.

4.3. Tailoring messages according to business type

Beyond the foundation laid out above in section 4.2, businesses have different messaging needs depending on their knowledge about cyber crime, and their perception of the risk it poses to them. This section outlines which messages engage different types of business, set out in the typology below.

4.3.1. Business typology

Businesses can be mapped on to a rough typology based on their size, their knowledge about cyber crime and their perception of the risk this poses to their business. Three groups emerged from this typology, which are illustrated in figure 4.1 below. The characteristics of these groups and their particular messaging needs are explored in turn below.

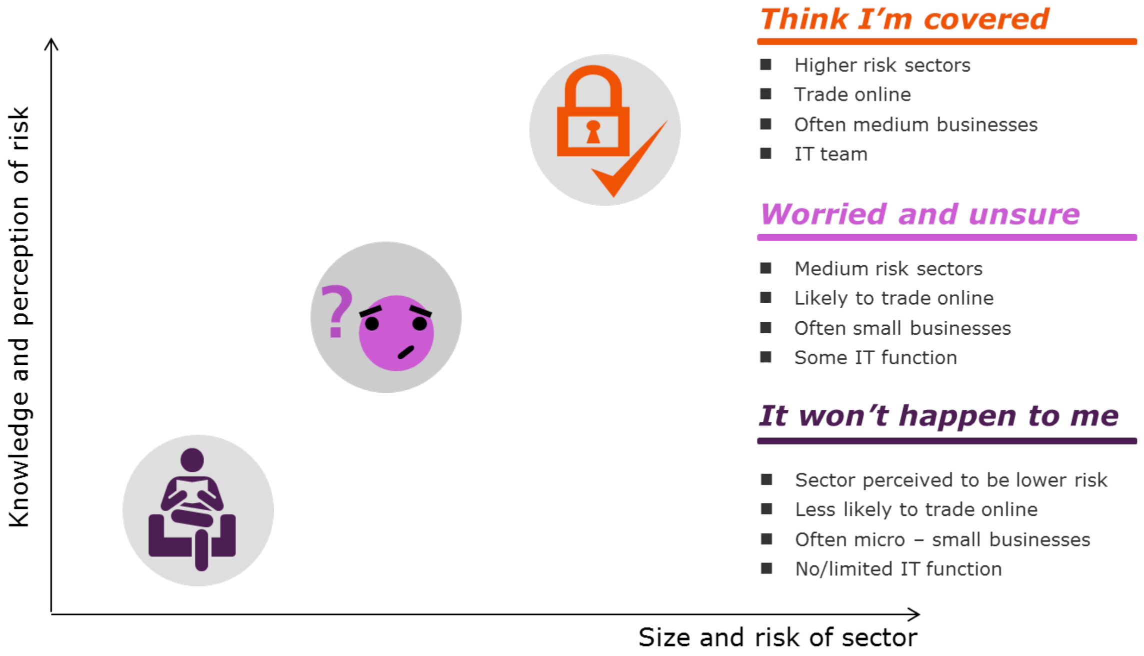


Figure 4.1: Business typology

"It won't happen to me"

Businesses in this group tended to have low knowledge about cyber crime. Whilst they were aware of the growth of cyber threats, they tended not to see themselves as a legitimate target, primarily based on their sector and bulk of their business being conducted offline. Businesses in this group tend to be smaller, and can be sole traders and micro businesses. Given their size (in terms of employees and turnover), they had either limited or non-existing IT functions in their business, and lacked regular access to IT consultants.

> *"Our business is chicken. I don't think anybody's going to care two hoots if it's Cyber Essentials chicken or non Cyber Essential chicken."* (Strand Bi, 50-249, Birmingham)

> *"I'm not so sure if somebody comes to book a coach they're going to be worried about their data." (Strand Bi, 50-249, Birmingham)*

Key messages need to first convince this group that they are at risk and that cyber crime is a relevant threat to businesses like them: businesses of their size, from their sector and with their structure and organisation. Whilst messaging needs to do this for all groups, it is crucial that messaging counteracts this group's belief they are not relevant to cyber risks. Case studies with sole traders and micro businesses from sectors which perceive themselves to be low risk could engage these types of businesses. They could demonstrates the ways in which these businesses are at risk and what the types of consequences and impacts for their business could be (particularly regarding damage to reputation). Messages then need to show businesses that Cyber Essentials is suitable for them, outlining the solutions it offers to businesses like them. In particular, messages need to convince this group that the scheme is not just for large businesses from high risk sectors.

> *"I think disruption and reputation are very important in a small business. If you're just, if you have your reputation goes, as you were saying, that's, you know you, a lot of businesses rely on people."[18] (Strand Bi, 1-49, London)*

Beyond this, there are other supporting messages which could help to engage this audience. These businesses tend to be engaged by messaging about cost which directs them to free elements of the scheme (although it should be clear that other parts incur a specific cost). Messages which emphasise government backing also appeal to this audience as this gives the scheme credibility. Given their lack of resource, messages which provide clarity about the amount of time and resource required are helpful. Given their lack of knowledge and confidence, messages should be jargon free and signpost businesses to help and assistance.

> *"It's a free download, so you think that's always a plus, if it's free." (Strand Bi, 1-49, Birmingham)*

"Worried and unsure"

Businesses in this group had slightly more knowledge than the previous one about cyber crime and had a slightly greater perception of the risk cyber crime poses to their business. However their knowledge and confidence is still relatively low. Their increased perception of the risk, combined with low knowledge, means that they can be worried and anxious about cyber crime – but this has not yet driven them to take action. Businesses in this group tend to come from medium risk sectors (e.g. education and recruitment). They use IT more frequently and are more likely to trade online. They are often small businesses and small/medium businesses and have some IT function (e.g. one person) or access to a more regular IT consultant.

Key messages need to first affirm this group's concerns that they are at risk. Messages then need to demonstrate the urgency of the issue to drive businesses to move beyond worrying and take action. As this group has a slightly higher level of knowledge and some access to IT experts, messages need to convince them that the scheme will empower them by increasing their knowledge at the same time as improving their cyber security. Messaging should also present the scheme as a solution which works with them.

[18] *A cyber attack can cause disruption, loss of time, loss of company and client data, be a barrier to growth and causes damage to a business' capacity to trade and reputation as well as having financial costs.*

> *"I'd like to know what caused that, I would look at that, I would like to know what I could do to not create that and not be part of the 50%."*[19] *(Strand Bi, 1-49, London)*

Supporting messages could emphasise the independent testing of their systems and how this helps to protect their business. Messages regarding human error and the role of senior management worked well with this group.[20] This may be because they drove recognition amongst smaller businesses that cyber crime and the consequences of an attack were their responsibility. Given that businesses in this group are often small business with limited resources, messaging should demonstrate the benefits and value of the scheme to the business itself and how the certification can prove an asset to the company. As with the previous group, it remains important that messaging is jargon-free as this group also has low knowledge and confidence. Messaging should also emphasise free aspects and government backing of the scheme.

> *"So it means spending a few hundred quid for some extra security is probably…well worth it, isn't it?" (Strand Bi, 1-49, Birmingham)*

"Think I'm covered"

Amongst the sample, this group had the highest level of knowledge about cyber crime and greater awareness of the risk this poses to their business and businesses more widely. Therefore these businesses tended to have already searched for information and taken action to install cyber security risk management measures of varying levels. Some of these businesses already held accreditations such as the ISO accreditations and had reliable software in place. These businesses tended to be from higher risk sectors such as banking, finance and IT, and were more likely to hold larger amounts of personal information and trade online. They were medium size businesses, with access to an IT team or consultants who maintain their systems for them. Directors of these companies may divest responsibility for cyber security to these IT experts and assume that their business is already adequately protected.

Key messages needs to challenge this group's assumptions and complacency. Messaging needs to first convince these businesses that they may still be at risk and encourage them to check the measures they know, or assume, they have in place. Given these businesses are more likely to have already searched for information and have taken some action, messaging then needs to convince these businesses of the specific benefits of Cyber Essentials and added value this scheme offers compared to other solutions and accreditations which are on the market. Given businesses in this group are likely to be larger, have greater resources and access to IT experts, as well as more advanced IT systems and capabilities, Plus may be more appropriate and accessible for them.

Supporting messages for this group should focus on providing incentives for these businesses to use this scheme rather than other alternatives which they have the resources to access. Case studies worked particularly well with this group, particularly those showcasing relatable examples and demonstrating the serious impact an attack can have on businesses like theirs. Businesses responded well to messaging which illustrated tangible consequences for businesses like theirs, particularly financial, legal and reputational costs as well as loss of time and resources (e.g. messages 7, 9, 11 and 12 in phase 2). Businesses also reported that they

[19] 50% of the worst breaches in the year were caused by inadvertent human error.

[20] (6) 50% of the worst breaches in the year were caused by inadvertent human error. (8) 28% of the worst security breaches were caused partly by senior management giving insufficient priority on security - up from 7% a year ago.

understand there is an emotional cost to cyber attacks, which was also reflected in Strand A among those who had experienced cyber attacks. This suggests messages with an emotional content could drive engagement and action.

> *"That's a hell of a message…that says do something or you will go out of business. " (Strand Bi, 50-250, London – Talk Talk message)*
>
> *"Case study. And then you can relate...You can say, well, our business is about that size and or our business is this big and what actually happened?" (Strand Bi, 50-249, Birmingham)*
>
> *"It is definitely lots of time and it is stressful. It's emotional. It's not just the financial but it's the emotional value as well – it's draining." (Strand Bi, 50-250, London)*

Messages for this group should avoid references to small businesses because these businesses can then perceive the scheme as too simple for their needs and not appropriate for their scale of operations. The new message referring specifically to medium size businesses worked well with them[21]. Messages including statistics received a markedly more negative response from this group as respondents challenged the use of statistics and questioned base sizes, where the data had come from and who had taken part in the surveys[22]. There was a more mixed response in the other groups. Messages concerning the role and responsibilities of senior management in this area worked less well with this audience who tended to reject this and claim that any employee can be responsible for a breach[23]. This may be due to more dispersed responsibility in larger medium size businesses.

> *"Have an emotional content and stop throwing numbers out." (Strand Bi, 50-250, London)*

4.4. Language, tone and imagery

Businesses in the communications testing provided consistent feedback about their responses to the language, tone and imagery used in the messaging which also chimed with responses given in the other strands.

Regarding needs around language, messaging should be in jargon-free plain English with as little technical language as possible. As stated throughout this report, given that cyber security is widely perceived as a confusing area, accessible language is crucial for engaging a wider range of businesses with this topic. For example, the message tested concerning DDoS (Distributed Denial of Service) attacks received a negative response and was found to be disengaging, even when a definition of the term was provided, across sizes and locations and regardless of levels of knowledge[24].

Businesses wanted to see content, particularly on the website, which is better tailored to businesses and their needs. They disliked being directed to what they perceived to be government policy documents for support, and did not respond well to messaging that referred to government action in relation to cyber crime – perceiving this as irrelevant to them.[25]

[21] *"New Government research shows 51% of medium-sized businesses detected one or more cyber security breaches in the last 12 months"*

[22] *4 is the average number of breaches suffered by small businesses in the last year*

[23] *28% of the worst security breaches were caused partly by senior management giving insufficient priority on security - up from 7% a year ago.*

[24] *16% of small businesses were hit by 'Distributed Denial of Service' attacks in the last year – which cause your website to go offline, preventing customers from accessing your website and making purchases. The attack could also prevent staff from accessing the internet, sending/receiving emails and accessing company data held online.*

[25] *On 22 September 2015 Minister for the Digital Economy, Ed Vaizey, urged businesses across the country to protect themselves by taking up the Government's Cyber Essentials scheme.*

Businesses reported that they would like clarity on whether the scheme is government-backed or government-run. Businesses regard 'backing' and 'running' to be different and wanted the government's role to be clear and clarified. Government backing of the scheme was well received. This was seen to give the scheme credibility in a marketplace where businesses are unsure who to trust. For smaller businesses, this also gave the topic a sense of security when they found this was something the government was taking action on. Businesses responded positively to the use of the HM Government logo where this appeared in materials, finding it reassuring, and questioned why it was absent when it was not used. This was again because the logo is seen to give the scheme weight and seriousness.

Across all strands of research, businesses responded positively to any diagrams used (for example the diagram outlining scope in the website downloads). Good use of well made and clear diagrams, process diagrams and infographics can help make the scheme and its content more accessible to businesses – and this was something they repeatedly specifically asked for.

Businesses reported that they wanted to see more 'hard' security images used in the messaging. They perceived the current imagery to be too soft for the topic. Particularly smaller businesses wanted to see 'harder' images and edges, such as padlocks which they associate more readily with online security.

> *"…you put your trust in things that are government based and I think you go on their website, you know their website is secure and, again it's something that I would trust in." (Strand Bi, 1-49, Birmingham)*

> *"I have a comment about the actual logo. To me it doesn't look secure. Because a red tick looks flexible, not solid. Like because I do a bit of graphics, so stuff like that, it just doesn't scream technology, it doesn't stay solid, it doesn't ...It looks like a passport. Looks like a bit of a passport look, do you know what I mean?" (Strand Bi, 1-49, London)*

The Cyber Essentials leaflet and online advert were also tested in the groups (see appendix 6.6). Feedback was consistent with the findings and recommendations provided in this chapter, though detailed feedback specific to these communications is set out below.

4.5. Response to the leaflet

Though government branding is a strong benefit, medium size businesses were sensitive to the format of the leaflet which could risk undermining the credibility of the scheme.

There was a difference between the responses given by small and medium businesses to the leaflet. Smaller businesses tended to respond more positively to the leaflet and perceive it to be professional and helpful. They were particularly attracted to messages offering free information and guidance. However messaging in the leaflet drove some confusion about the nature of the scheme and what the next steps should be as this was not seen to be clearly set out.

> *"I just don't know where I would go, where would I look?" (Strand Bi, 1-49, London)*

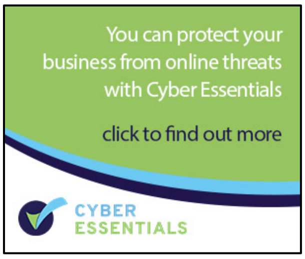
Medium businesses responded less positively overall. On the one hand they found the leaflet simple and clear and to provide adequate information about the process. They responded positively to the case study which suggests the benefits of the scheme. However on the other hand the design was perceived to be somewhat amateur and out of date. Medium businesses were also put off by what they perceived to be non committal language providing caveats to the limitations of the scheme at this stage.[26] They also questioned where they could expect to find and pick up this leaflet. Overall the leaflet was perceived to be out of date and businesses expected more modern solutions.

> *"To me this seems a bit- I'm going to be quite disparaging now, so apologies: This seems like a GCSE IT project to produce a leaflet." (Strand Bi, 50-24, London)*

> *"It's very interesting what you were saying about it was produced in 2014. To me this seems like this is their first stab at getting some information out there." (Strand Bi, 50-24, London)*

> *"And just the method of delivery – a leaflet. It's a bit 1998. I don't know. I just- Where would I pick this up? I just- Yes. It's very dry." (Strand Bi, 50-24, London)*

4.6. Response to the online advert


You can protect your business from online threats with Cyber Essentials
click to find out more
CYBER ESSENTIALS

The advert was perceived to be professional but was not associated with government or online security. This was due to the colour theme, imagery and lack of security related imagery.

Businesses reported that the colour scheme was too 'soft' and associated the green and blue with utility companies. They wanted to see harder and more solid images and lines, as well as the HM Government logo. Smaller businesses thought the advert should offer something 'free' as an incentive to click on it – although this should be done carefully with the findings about clarity around costs in mind.

> *"I think of British Gas or an electricity company in terms of just the way the colours and the squiggly lines and stuff." (Strand Bi, 50-249, London)*

Smaller businesses tended to report that they might click on the advert, whereas medium businesses tended to report they were less likely to click through. Medium businesses also raised the concern that the advert itself may be a threat.

> *"To be honest, I would more than likely think it could be actually dangerous to click on it. Because it could actually be something to entice you in and there's a hacker." (Strand Bi, 50-249, London)*

Lack of recognition of the scheme and badge, and non-association with government, risks the advert being ignored or itself distrusted as a cyber threat.

4.7. Suggested communication channels and messengers

Businesses suggested a range of government and non government channels and messengers from which they would like to hear about the scheme.

Small businesses wanted to hear about the scheme from organisations they regularly interact with, trust and associate with cyber security and security more broadly including: banks, (accountancy) software companies and trade associations. They also suggested IT and internet providers who they associate with this topic and regard as having expertise. Finally, small businesses reported they would also pay attention to communications sent from HMRC.

[26] *"Next steps – no measures, however well implemented, can provide 100% protection from internet based attack".*

In terms of timing, small businesses regarded the purchase of a new computer and during business set up as good touch points for engaging with this topic. They would also engage with leaflets sent in the post and pop ups which appeared on websites they trust and use frequently (e.g. Facebook, Google, and business and trade association advice pages).

Medium size businesses suggested that information should be cascaded through trusted advice organisations, such as trade associations and professional bodies whose advice is seen to be serious and credible. They also suggested a wider TV and radio campaign and posters in key sites (e.g. on the tube and at rail stations). They also suggested the use of appropriate ambassadors from business, rather than politicians promoting the scheme. In addition, they suggested the use of a sponsored YouTube advert to reach businesses which could outline the risks of the threat and benefits of the scheme.

4.8. Summary of recommendations

Section 3.3 provides a detailed account of the recommendations to improve the completion of the scheme revealed by the research. These recommendations are summarised here according to the strand they were primarily derived from. However findings from across the strands were broadly consistent and support and build upon each other. The strands are presented in this order as the first two produced recommendations around improving the sign up and completion processes and the third regarding recommendations to improve messaging to increase uptake to a wider audience. Increasing take up in a wider range of sectors, and then growing this within areas and sectors, can help to boost recognition of the badge and therefore credibility and value of the scheme.

4.8.1. Suggested improvements to the completion process (process evaluation)

- Clarify the value and benefits of the scheme to businesses upfront
- Improve upfront understanding of the scheme
  - Clarify costs upfront (the cost of the scheme, and indicate other like costs and resources which will be required)
  - Clarify the process upfront (via an infographic or process diagram, which indicates the length of time stages are likely to take)
  - Clarify the requirements upfront (provide a check list, use consistent terminology and outline the requirements in plain English)
- Help businesses to make informed choices
  - Provide greater clarity about the difference between Basics and Plus
  - Outline the added value and benefits of Plus
  - Outline clearly the difference between ABs and CBs (and explain their role in the process for businesses)
  - Provide a comparison table or tool which enables businesses to compare CBs and select the one which is most appropriate for their needs (this should include costs, additional products and services they provide, length of questionnaire, an indication of the level of support provided, and customer service reviews and scores)
- Improve the completion process for non-experts
  - Standardise the length of the core questionnaire
  - Standardise approach to answer codes
  - Provide guidance and model answers for how to fill in answer codes

  - Standardise evidence requirements and set out instructions clearly
  - Provide greater support for those who lack knowledge and confidence
  - Simplify the language used in materials, on the website, in documents and the questionnaire (this should be jargon free and in plain English as far as possible)
  - Reduce the amount of text used where possible and do not use policy style documents

4.8.2. Suggested improvements to the sign up process (remote testing)

- The website should provide clearer information about the purpose and nature of the scheme, such as the messages tested in the groups.
- It should also set out clearly the benefits and added value of the scheme to businesses themselves through case studies of a variety of businesses from different sectors and sizes.
- Businesses need a clearer outline of the process they need to go through to adopt the scheme. This can be done through an infographic or flow chart.
- Businesses would like clear, up front information about costs as this is crucial to their decision making as to whether to pursue the scheme
- Clearer information should be provided about the difference between the two badges – the difference in cost and what the benefits of each are, and in particular which makes clear what the added value of the Plus badge is.
- Businesses would like a clearer upfront summary of the requirements that they will need to meet initially (e.g. as a checklist), and then more detailed information about how to meet these.
- Provide a table which summarises information about the different ABs and CBs in order to help businesses decide which is the most suitable for them.
- Provide a tailored report after completing the questionnaire on the website with further explanation of what businesses have to do to increase their cyber security and pass the scheme.
- Further quotes are likely to be well received from a wider range of sectors and businesses of different sizes, particularly some smaller businesses to appeal to micro and small businesses. Video testimonies are also likely to be well received and engaging.
- Adding a chat function and/or email contact address for those with queries about the scheme and requirements would likely be well received.
- Split the website into different tabs or pages rather than users needing to scroll down the page. Further information could then be provided on the webpages rather than in downloads.
- Less text / more images - too much text is both time consuming and off putting.

4.8.3. Suggested improvements to scheme’s messaging to engage a wider audience (message testing)

Messaging should follow three key principles

- Convince businesses that cyber crime is a real, relevant, and urgent threat

  - Explain the nature of the threat - through the use of tangible examples and case studies which demonstrate the potential impacts of a threat (particularly involving financial costs, damage to reputation and loss of time).
  - Convey the level of the threat – through the use of high figures (particularly using a “1 in X” format)
  - Demonstrate that this is a relevant threat to their type of business

  - Avoid messages which describe what cyber crime is without providing any new information about this threat (its nature, consequences, or urgency), and in technical language
  - Avoid the use of percentages and averages which businesses are less able to relate to

- Convey what the Cyber Essentials scheme is and what it offers

  - Communicate the nature of the scheme and what it offers
  - Use messaging about the scheme which serves as a call to action
  - Use consistent terminology to avoid confusion
  - Set out the benefits of the scheme and how it will be useful and valuable to businesses themselves

- Outline the costs and requirements

  - Outline the cost of around £300 clearly upfront to prevent upselling and because this is perceived to be a reasonable price
  - Set out clearly the process and requirements to set expectations

Beyond these three key principles, messaging should be tailored to three groups in a typology of businesses underpinned by knowledge about cyber crime and perception of risk this poses to them.

- "It won't happen to me"

  - Messages need to convince them they are at risk and see cyber crime as relevant to them
  - Convince them the scheme is for them
  - Show the scheme is affordable and not too time consuming

- "Worried and unsure"

  - Messages need to affirm concerns about risk and demonstrate urgency
  - Convince them the scheme will empower them by increasing their knowledge
  - Use clear language and demonstrate that the scheme works with them to help and benefit them

- "Think I'm covered"

  - Messages need to challenge complacency, show they are still at risk and encourage them to check their measures
  - Convince them of the added value of this scheme and what it offers
  - Plus may be more appropriate
  - Include messages around 'trail blazing'

- Tailor and target messages to businesses rather than using government policy documents
- Provide clarity on whether the scheme is government-backed or government-run
- Use jargon free plain English as far as possible
- Increase the use of diagrams and infographics and reduce the amount of text used
- Make greater use of the HM Government logo
- Make greater use of 'harder' security images (e.g. padlocks)
- Change the colour scheme which is currently perceived to be too 'soft'
- Provide different leaflets for different groups of businesses

- Emphasise the free aspects of the scheme.

5. Summary

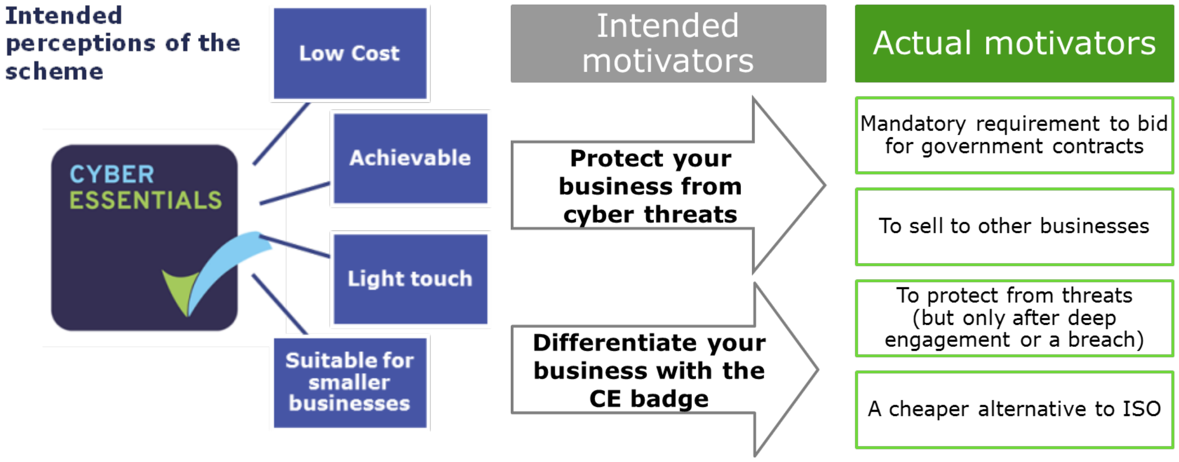
Some businesses in the research reported positive experiences of the Cyber Essentials scheme, finding it simple and efficient to complete, their CB helpful, and the experience and certification valuable to their businesses. However, feedback suggests that improvements could be made to the sign up and certification process to further improve business' experience of the scheme. Across the research strands, businesses reported low awareness of the scheme and low recognition of the badge. The messaging testing revealed three key principles for engaging a wider range of businesses more effectively.

This chapter first reports on the mismatch between intended and current motivators. It then summarises current barriers businesses face before outlining risks and opportunities for the scheme. The recommendations this report makes to improve the scheme, derived from the three research strands, are provided in chapter 4 and the executive summary.

5.1. Current and intended motivators

The research found that there is currently a mismatch between the intended and actual motivators for engaging with Cyber Essentials. It was intended that businesses would undertake the certification in order to protect themselves from cyber threats and to differentiate themselves in their marketplace. However, current motivations tend to be financially or business driven. Businesses tended to have undertaken the scheme because it was a mandatory requirement of a procurement process; as a cheaper alternative to the ISO accreditations; to increase protection after a breach or deep engagement; or to sell the scheme as a product to other businesses among consultants. The current limited range of motivators for uptake may be driven by low awareness of the scheme; businesses (outside of the cyber security sector) tended to report that they had not heard of the scheme before it appeared as a requirement.

Figure 5.1: Intended and actual motivators for the scheme



Intended perceptions of the scheme
Low Cost
Achievable
Light touch
Suitable for smaller businesses
CYBER ESSENTIALS
Intended motivators
Protect your business from cyber threats
Differentiate your business with the CE badge
Actual motivators
Mandatory requirement to bid for government contracts
To sell to other businesses
To protect from threats (but only after deep engagement or a breach)
A cheaper alternative to ISO

Whilst the current motivators may not be what was intended for the scheme, the findings suggest that including the scheme as a mandatory (procurement) requirement is an effective lever for driving uptake. There was some suggestion that businesses may then be more aware of who else in their supply chain holds the certificate. Regardless of their motivations, completion of the scheme will mean that levels of cyber protection are rising in the business community.

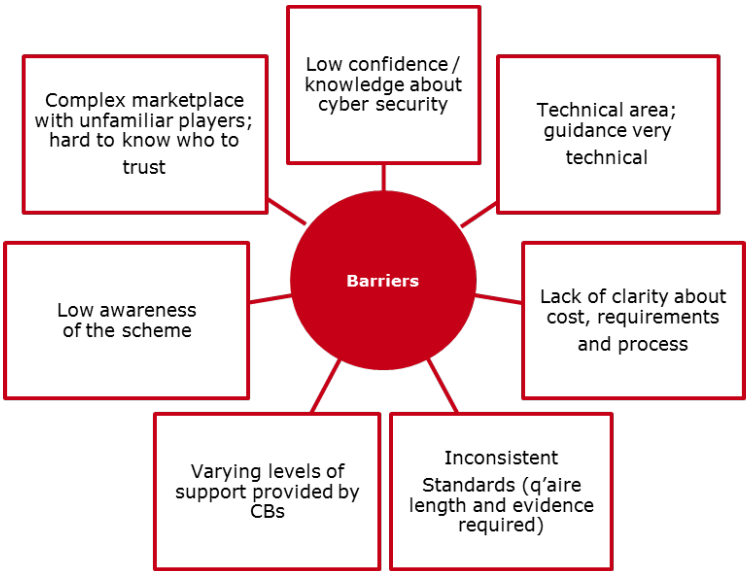
However, business' motivations may shape the way that they approach the certification process and value the scheme, which may not be in line with what was intended. For businesses completing the scheme in order to bid for contracts, the scheme can be perceived as a tick box exercise which is perceived as just another hurdle to be completed as quickly as possible, rather than engaged with more deeply. This has implications for upskilling in this area as businesses may not be taking the opportunity to learn about cyber security as deeply as they could be.

Businesses tended to report that they perceive the scheme to be good value for money. Their evaluation should be understood within the context of business' current motivations: businesses value the scheme on the basis of the contracts and business it enables them to bid for and retain. Consultants meanwhile value the certificate in terms of the new business it enables them to win, although the scheme seems to be sometimes sold as a loss leader for other products. However the message testing showed the scheme was also seen as good value when weighed against the potential cost of an attack so the price should be advertised more clearly.

5.2. Barriers to sign up and completion

It was intended that Cyber Essentials would be a low cost, achievable and light touch way for SMEs in particular to protect themselves against cyber threats. As discussed in section 3.2, some businesses reported finding the scheme simple and efficient and their CB helpful. However feedback suggests that businesses currently face a number of barriers at the sign up and completion stages which can cause confusion, frustration and be off-putting. These are summarised below in figure 5.2 and also in the executive summary.

Figure 5.2: Summary of barriers



Barriers

Low confidence / knowledge about cyber security

Technical area; guidance very technical

Lack of clarity about cost, requirements and process

Inconsistent Standards (q'aire length and evidence required)

Varying levels of support provided by CBs

Low awareness of the scheme

Complex marketplace with unfamiliar players; hard to know who to trust

5.3. Risks and opportunities

The current barriers and motivators for the scheme, and the way it has been designed and presented, present a number of risks and opportunities for the scheme. There are a number of key risks to the reputation and credibility of the scheme which should be addressed before a wider audience is sought.

5.3.1. Role of cyber security and IT consultants

The role that cyber security and IT consultants, as well as some CBs, are currently playing in this marketplace presents a key risk to the reputation and credibility of the scheme. Cyber security and IT more widely is an area where businesses can lack knowledge and confidence and therefore find potentially scary. These businesses are therefore potentially vulnerable in a market place which is increasingly crowded and where businesses lack familiarity with the players and are unsure who they can trust.

The current audience for the scheme includes cyber security and IT consultants who have become certified in order to sell the scheme as a product to other businesses. Consultants reported that sometimes the scheme is being sold as a loss leader in addition to other more expensive products and services (e.g. scans and penetration tests). This situation, combined with the current lack of upfront clarity about the cost of the scheme, may mean that businesses are being unknowingly upsold unnecessary products. They may also be unable to disentangle to cost of the scheme from the other charges submitted by consultants. Some businesses may be happy to pay these additional costs and appreciate the value these products offer in helping to further protect their systems. However, a risk is presented if consultants refuse to provide assistance with the scheme without additional products, or if businesses realise there has been a lack of transparency and that they have unknowingly paid for non-mandatory products when completing the scheme. This could damage the reputation and credibility of the scheme and mean that businesses are put off the scheme and less likely to renew, move on to Plus and/or recommend it to others.

However, the presence of these consultants in the marketplace also presents an opportunity for the scheme. DCMS could work with them and they could provide a key channel and act as messengers to inform businesses about the scheme as well as assisting with implementing the requirements in the business community.

5.3.2. Low awareness and badge credibility

The current low awareness of the scheme and low recognition of the badge presents a risk to the scheme. This lowers the credibility of the badge as this can only meaningfully provide reassurance and value to businesses if it is recognised by suppliers and customers / clients. Increasing awareness of the badge and take up of the scheme should initiate a virtuous circle as increased prevalence motivates others to investigate and complete the certification.

Increasing visibility within sectors within particular geographic regions could begin to kick start this cycle. Members of local business communities communicate and work together and value recommendations from people they know and trust. Businesses suggested in the message testing that they would like to hear about the scheme through trade associations and professional bodies, and this could also include chambers of commerce and other advice organisations. Businesses who have completed the scheme could be encouraged, and incentivised, to act as ambassadors for the scheme to build credibility and boost the cycle. Case studies about these businesses, from a range of sectors, could also be used to engage businesses more widely across the country.

5.3.3. Lack of standardisation

CBs are able to tailor their questionnaires and this means that currently there are different length questionnaires available. Some businesses reported being aware of this and this factor influencing their choice of CB. Businesses reported being asked to submit different types and levels of evidence by their CB, with some perceiving CBs to require more and less rigorous evidencing. A cyber security consultant reported hearing that some CBs do not require any evidence to be submitted. Regardless of whether this is true, even the perception in the sector that this is the case can be damaging to the credibility of the scheme.

It could help to protect the reputation and credibility of the scheme if the questionnaire and evidence requirements are standardised. However, some of the questions CBs add may help to increase the cyber security protection measures businesses have in place, as well as raising awareness and educating businesses about additional measures. Businesses could be helped to make informed choices by transparency about this being increased. For example, it could help if the questionnaire were standardised and then CBs were able to add questions or sections but these were clearly labelled as voluntary sections. Given some businesses approach the scheme as a tick box exercise to be completed as quickly as possible, a lack of explanation of the value of additional questions could create a race to the bottom as businesses seek the shortest and easiest questionnaires available.

5.3.4. Variation in levels of customer service

As described in section 3.2.3, businesses reported receiving different levels of support from their CBs. This means that businesses report different levels of satisfaction with the customer service CBs provide. It should be noted that businesses required and expected different levels of support. Those who lacked knowledge and confidence could need a consultant to fill in the questionnaire and make changes for them. Other businesses were more able to do these tasks themselves with some guidance. Those with more knowledge and confidence, particularly cyber and IT consultants, needed little more than clarifications.

There is a risk to the scheme where businesses who need and expect higher levels of support from their CB do not receive this. This can lead to poor experiences of the scheme and may mean business do not renew, move to Plus or recommend the scheme to others. This risk could be addressed by providing a rating and feedback system through the Cyber Essentials website. This could allow businesses to give CBs a score and leave qualifying feedback about the service they received. This dual system would take account of businesses needs and expectations. Knowing feedback was being left publically could raise the level of customer service provided in the marketplace overall. This system, provided alongside a comparison table helping businesses to make a more informed choice in their provider, could help businesses to choose a CB which provides the appropriate level of support for their needs.

A summary of the recommendations derived from the three strands of this research are outlined at the end of chapter 4 and are summarised in the Executive Summary.