

# Cyber Essentials Scheme – process evaluation and communications testing

## Appendices

DCMS  
2016



**TNS BMRB**  
DCMS Cyber Essentials Scheme

© TNS 2016

JN260136173

# Appendices

## Contents


6.1	Summary of message testing responses	2
6.2	Case studies	4
6.3	Key quotes from Strand A respondents	10
6.4	Achieved sample	12
6.4.1	Strand A	12
6.4.2	Strand Bi – Message testing	14
6.4.3	Strand Bii - Remote User Testing	15
6.5	Topic Guides	15
6.5.1	Strand A	15
6.5.2	Strand Bi	19
6.5.3	Strand Bii	25
6.6	Stimulus materials (Strand Bi)	29


## 6.1 Summary of message testing responses


	G1 1 to 49	G3 1 to 49	G2 50 to 249	G4 50 to 249
<i>1 in 4 businesses experienced a cyber breach / attack in the past 12 months</i>				
<i>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. / Revised phase 2: 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.</i>				
<i>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.</i>	n/a			

You can protect against the common threats likely to harm your business by using free Government advice and training				
<b>Phase 2 only:</b> Small manufacturing case study	n/a		n/a	
50% of the worst breaches in the year were caused by inadvertent human error.				
<b>Phase 2 only:</b> "New Government research shows 51% of medium-sized businesses detected one or more cyber security breaches in the last 12 months	n/a		n/a	
The Federation of Small Businesses estimates the average cost of a cyber crime on a small business to be around £3,000. Government research says the average cost of a cyber attack to a small business is £3,100 / <b>Revised phase 2:</b> Government research says the average cost of a cyber attack to a small business is over £3,000				
Displaying the Cyber Essentials badge will show customers that you take cyber security seriously				
<b>Phase 2 only:</b> The Cyber Essentials scheme checks whether your business meets 5 basic cyber security requirements. You become certified when you meet these requirements.	n/a		n/a	
28% of the worst security breaches were caused partly by senior management giving insufficient priority on security - up from 7% a year ago.				
16% of small businesses were hit by DDoS attacks in the last year. <b>Revised phase 2:</b> 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.				
59% of businesses expect there will be more security incidents in the next year than last.				
Cyber crime is a growing threat to UK businesses – criminals target customer data, company finances, and the safety and integrity of IT systems.		n/a		n/a
4 is the average number of breaches suffered by small businesses in the last year		n/a		n/a
By taking action on cyber security you can protect customer data, company finances and the safety and integrity of IT systems.		n/a		n/a

## 6.2 Case studies

<b>Case study #1</b> <b>(1-49, Environmental Consultancy)</b>	
<b>Background</b> <ul style="list-style-type: none"><li>The business provides consulting, training, and auditing services to businesses to achieve ISO Environmental Standards and currently employs five people</li></ul>	
<b>Motivation</b> <ul style="list-style-type: none"><li>Her company website had been hacked and was completely destroyed, leaving her unable to communicate with her customers</li></ul>	
<b>Journey</b> <ul style="list-style-type: none"><li>Because she was already working in the auditing world, she heard about Cyber Essentials and enlisted her IT Services Provider to help her with the certification process</li><li>After getting a few quotes, she chose her Certifying Body because they were local and offered a competitive price</li><li>She worked closely with her Certifying Body and resubmitted the questionnaire after they provided initial feedback. She wasn't penalized for getting things wrong or charged additional fees. As a result, she felt she learned a lot during the certification process about embedding cyber security into company practices</li></ul>	
<b>Barriers</b> <ul style="list-style-type: none"><li>She had difficulty understanding the technical language in the questionnaire and being able to supply the answers to the questions</li></ul>	
<b>Value to Business</b> <ul style="list-style-type: none"><li>She was aware of the price (£300) early on, and there were no unexpected costs, which she said can be challenging for a microbusiness</li><li>She felt it was a good investment as she hasn't had an incident since becoming CE certified, and she plans to renew her certificate</li><li>She uses the Cyber Essentials logo in all her proposals and tenders, and uses Cyber Essentials as a unique selling point for her business</li></ul>	
<b>Improvements</b> <ul style="list-style-type: none"><li>It would have been helpful to have examples of 'what good looks like' to assist in filling out the self-certification questionnaire</li><li>A case study of a business that has been Cyber Essentials certified or video testimonials from one business owner to another business owner would be helpful</li></ul>	
<i>"We discovered lots of things when we engaged on Cyber Essentials, lots of interesting things lots of holes lots of gaps which we've now filled, you know, close down those loopholes."</i>	

<b>Case Study #2</b> <b>(1-49, Charity)</b>	
<b>Background</b> <ul style="list-style-type: none"> <li>• She works as the team coordinator for a public engagement charity and handles systems and processes, including IT which is outsourced to a consultant</li> </ul>	
<b>Motivation</b> <ul style="list-style-type: none"> <li>• They were required to become CE certified in order to compete for government tenders</li> </ul>	
<b>Journey</b> <ul style="list-style-type: none"> <li>• Prior to becoming Cyber Essentials certified, there was low awareness about Cyber Security; it was left up to individuals rather than having an organisational policy</li> <li>• She reached out to five Certifying Bodies for quotes, and she went with the only one who got back to her</li> <li>• Her organisation paid £1000 the first time and failed the test; they then had to pay £1200 to be re-evaluated even though she believed the reasons for failure were relatively minor</li> <li>• She did not feel equipped to handle the certification and received little help or support from the Certifying Body; her IT and website consultants dealt directly with the CB</li> </ul> <b>Barriers</b> <ul style="list-style-type: none"> <li>• The unexpected costs were challenging, they paid £2200 to CB and a further £400 to their IT consultant</li> </ul>	
<b>Value to Business</b> <ul style="list-style-type: none"> <li>• It allows them to bid for Government tenders</li> </ul>	
<b>Improvements</b> <ul style="list-style-type: none"> <li>• There was little support from CB and so there weren't opportunities for learning during the process</li> <li>• She would have liked more support from CB, possibly a helpline, in order to prepare for the questionnaire</li> </ul>	
<i>"I thought it was a nuisance...I think it first of all it's quite difficult to understand what is required and what we actually as an organisation have to go through to become cyber certified, so I think it was very very technical language as well, especially for small charities which we do not have an IT person in house."</i>	

<b>Case Study #3</b> <b>(1-49, Ergonomics)</b>	
<b>Background</b> <ul style="list-style-type: none"> <li>A small consultancy run by a husband and wife that works on tech systems design to make them more ergonomically friendly</li> </ul>	
<b>Motivation</b> <ul style="list-style-type: none"> <li>They were encouraged by a client with whom they were subcontracting to become certified, and they expected that eventually it would become mandatory so they should take the time to become certified</li> <li>Because nearly 90% of their business comes from one government department and they work with classified data, cyber security is very important</li> </ul>	
<b>Journey</b> <ul style="list-style-type: none"> <li>They chose a provider that was in their local area, with a mind to eventually having someone conduct an audit visit as part of Cyber Essential Plus</li> <li>They chose CE Basic because they were focused on getting certified as soon as possible, and they completed the questionnaire together and sent it off to the certifying body</li> <li>The certifying body came back with a few questions to check their understanding, but they passed the first time through and received their certificate a few days later</li> </ul> <b>Barriers</b> <ul style="list-style-type: none"> <li>They operate on a Mac system, and the questionnaire was written for Windows users</li> </ul>	
<b>Value to Business</b> <ul style="list-style-type: none"> <li>They sent a copy of the certificate to the client that had requested it, and if they were not certified they would not have been able to work with the Ministry of Defence</li> </ul>	
<b>Improvements</b> <ul style="list-style-type: none"> <li>Having a version of the questionnaire that is tailored to businesses that use Macs</li> </ul>	
<i>"It's something that we have to have in order to work for MOD and at the moment eighty, ninety percent of our work is from the MOD. We just went okay, well we are just going to have to pay for it and take the time to do it."</i>	

## Case Study #4

### (1-49, Education)



#### Background

- A husband and wife team that work in the education sector, helping schools prepare for OFSTED inspections
- Their IT is handled by an IT Consultant

#### Motivation

- It was a requirement in order to bid for a government department contract

#### Journey

- First heard of CE in a government tender, and began to read more about the scheme; the more she read the more confused she felt about what it was and doubted that they would meet the criteria
- She chose the Certifying Body because its website was the simplest and easiest for her to understand, and they sent her a bullet point list of the steps of the process
- She first attempted the questionnaire and felt overwhelmed, so she enlisted her IT consultant and they completed the questionnaire together; she was surprised to learn they were well-protected already
- They sent off the questionnaire and answered one follow-up question, and were then informed they had passed and would be CE certified

#### Barriers

- The CB and her IT Consultant were helpful, but she felt the whole process was over her head
- She also struggled with understanding the differences between CBs and making that choice

#### Value to Business

- She thinks that there should be a greater effort to spread awareness of the CE scheme in order for it to add value to her business
- She's not sure if it's won any contracts, but they do have the CE badge on their website

#### Improvements

- She wanted more clarification on the certification process and what the steps were
- She found it difficult choosing a CB and felt it should be made clear that they are all offering the same CE Certificate

*"...the 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."*

**Case Study #5**  
**(1-49, IT Consultant)**



**Background**

- He is the technical director of a company that provides IT solutions; his organisation is Cyber Essentials certified and now he helps other businesses become CE certified

**Motivation**

- He believes that it is good basic hygiene for small companies to have, and that most SMEs will go for the Basic because the Plus is a huge jump in price and time involved

**Journey**

- He chose the only Certifying Body in his region, which he was already familiar with due to his work in IT in the area
- When he helps other businesses get CE certified, they pay both the CE certification fee and his consulting fee
- He visits his clients onsite to fill out the questionnaire, gather evidence and make any same day fixes; he then follows up on any remaining issues before submitting the questionnaire

**Barriers**

- Cost is a big barrier for SMEs, as well as not having in-house IT staff to help with certification and implementing the necessary procedures
- As a result, many are vulnerable to upselling from CE providers who try to add on additional products and services

**Value to Business**

- The SMEs he works for see CE certification as a unique selling point over other suppliers
- It's also been a business opportunity for him, as he now helps others achieve CE certification

**Improvements**

- He believes if there was more transparency about what is involved and covered by the CE scheme, SMEs would be less susceptible to upselling and taking on additional costs beyond what is required by CE
- His company tries to estimate all costs of implementing CE for his clients, and his goal is to get his clients certified, not squeeze money out of them

*"Everybody can do this. It's not onerous. It's not expensive...this is really essential to any business now. Because with all the security issues that are out there if these very simple steps - and they're not particular expensive and they're not difficult to implement - if you do these steps, you are protecting your business going forward."*



## Case Study #6

### (1-49, Auditing)



#### Background

- He is the principal consultant/owner of a micro specialist consulting firm that performs audits on payment schemes offered by large companies

#### Motivation

- He had gone through Cyber Essentials Plus at his previous company, and it was a priority for him at his new company because of the type of data they work with and the potential reputational risk for the companies he works with.

#### Journey

- He had previously achieved ISO 27001 certification, and he first heard about CE during a module while pursuing his postgraduate degree in Cyber Defence and Information Insurance
- He was confident that they had a high level of security and would meet the standards, and although they already tested their own systems, he went with CE Plus because he felt it would be beneficial to have someone else review their systems.
- Even though most businesses in his region went with a particular Accrediting Body, he decided to go with a different AB to gain exposure to how another AB operated because he wanted to eventually become a Certifying Body himself
- He chose his AB because they were a well-known company, their website on CE was clear and straightforward, and they were not trying to sell him extra services
- Although he passed, he was unhappy with the certification process because he felt he did not get what he paid for (£1500); they did not check the documentation adequately and they were unable to do some of the testing because he used Mac computers
- To make things worse, they had to send back their CE Certificate twice because the company name was not spelled correctly

#### Barriers

- There were some incompatibilities with the questionnaire and the penetration testing because his business operated on Macs

#### Value to Business

- He believed it would be good branding to be able to advertise being part of a government-backed scheme
- He wanted to get certified himself but also saw it as a business opportunity to potentially become a CE implementer himself

#### Improvements

- There should be more standardization across Accrediting Bodies in the questionnaire and what is being tested, so that his certification means the same thing as someone else's

*"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?"*

### 6.3 Key quotes from Strand A respondents

(#1) "I found the process painless but also informative, it gave me a good yardstick with which to manage our security." (Strand A, 1-49, IT Consultant)

(#2) "It was fairly straightforward, fairly simple.....Because we had all the procedures in place already, we just had to document it." (Strand A, 1-49, Ergonomics)

(#3) "Well as I say we had a conversation on the telephone where he didn't bamboozle me with science and it was a very good conversation. He then followed it up with a very easy to understand sort of email with exactly what I needed to do and actually any of the accredited bodies could do the accreditation kind of thing, and it was just a step by-, and once I had actually sort of hooked on to Indelible I thought right, I'm going to stay with them now, I have found somebody who I can pick up the phone, he understands the fact that I am finding it all quite.." (Strand A, 1-49, Education)

(#4) "From a simple password policy through to logging in through VPN, it's fundamentally changed how we operate, there's major benefits from that and we're up to date with the latest thinking" (Strand A, 1-49, Information and Security Consulting)

(#5) "Once you're made aware of it and its existence, the actual process is simple and easy." (Strand A, 1-49, Cyber Security Consultant)

(#6) "I was pleased with the service, it was really good." (Strand A, 50-249, Insurance)

(#7) "We won a very big contract with the government, on the basis of, several million pounds worth. And we wouldn't have been in that position if we hadn't got it. So, it was necessary for that particular contract. And I don't know but I believe it's been used in other bids since as well." (Strand A, 250+, Education)

(#8) "You won't have heard of it ... but this remains a very robust scheme." (Strand A, 1-49, Cyber Security Consultant)

(#10) "In the long run it helps us as a company, it helps us protect our data and it also helps customers stay safe. So it benefits us in the long run, so we were quite happy." (Strand A, 1-49, Pharmaceuticals)

(#11) "Having a government backed scheme which would offer insights into your own security levels and support you in that way was a good thing to do." (Strand A, 1-49, Trade Organisation)

(#12) "I found it a useful, rewarding and company reputational enhancing experience." (Strand A, 1-49, Risk Management Consultancy)

(#13) "I found it a worthwhile, methodical way of checking our own IT infrastructure to make sure that it is up to standard in this modern era of cyber technology." (Strand A, 250+, Automotive industry)

(#14) "Everybody can do this. It's not onerous. It's not expensive...this is really essential to any business now. Because with all the security issues that are out there if these very simple steps - and they're not particular expensive and they're not difficult to implement - if you do these steps, you are protecting your business going forward. I think that's important, that's a message that is very very important to get across." (Strand A, 1-49, IT Consultant)

(#15) "It was an enjoyable experience. I got to understand more about what those key best practices are or other things, that kind of primary checklist of things that you should be doing in order to meet the government guidelines. So I feel more informed now. I would definitely

*recommend it to my colleagues from the point of view that it was a very easy process to follow, doesn't require a lot of time and doesn't require a lot of involvement from staff. And you get the benefit at the end of it being able to put a logo on your website to say that you've done it." (Strand A, 50-249, Recruitment)*

*(#16) "My experience was pretty simple, quick and easy which is how it should be, you know for this sort of scale." (Strand A, 1-49, Cyber Security/IT Consultant)*

*(#17) "It was made much more positive and straightforward by our certifier." (Strand A, 1-49, Local Authority)*

*(#18) "...the actual Cyber Essentials on the whole, we felt that was probably quite similarly aligned to our elements that we had for our ISO-27001. But actually having an active test to practice what you preach kind of approach, we thought that that was worth it." (Strand A, 1-49, IT Consultant)*

*(#19) "Once we started doing it, it was quite simple. It was literally here's a hundred questions or so, go and answer them" (Strand A, 50-249, energy industry)*

*(#20) "I can't say that we have, say won business directly because of Cyber Essentials. I think it has increased our own staff awareness of security as well" (Strand A, 1-49, Risk Management Consultancy)*

*(#23) "...the Cyber Essentials, I think, helped us define what we needed....it actually pushed us to then start putting policies in place and documentation." (Strand A, 50-249, Waste Management)*

*(#24) "I think generally it's a good idea. I think it could be done more about raising awareness of why it's important. Because we wouldn't have heard of it...we only heard of it because it's a requirement." (Strand A, 1-49, Charity)*

*(#25) "I found the whole process very useful exercise for our organisation in particular and for our IT department" (Strand A, 250+, Charity)*

*"Oh well to have the badge is great, it is good to say yes we've met this certain requirement and it is good for our agencies and other people that we work with in the, maybe work with in the future." (Strand A, 250+, Charity)*

*(#26) "In terms of the value to my other clients, I think that...so the primary focus of cyber essentials is about the extent to which you are secure from external attacks, cyber essentials plus is a slightly different focus...so I think for most of my clients and the clients I've talked to about it is about a level of peace of mind, where they've raised that as a question we're able to point towards this, but I've also said to them but you can also use it to an extent as a badge in terms of we take this seriously and therefore in terms of their communication of their approach to information security cyber security, that's a good thing. So I think therefore I perceive that there is a value for them...for my clients." (Strand A, 1-49, IT Consultant)*

*(#27) "For me it was more about making sure that I do what I say because I'm always telling people what to do to become more secure and I feel like I should do that myself." (Strand A, 1-49, Information Security Consultant)*

*(#28) "I thought it was good, as an entry level, because I also know...so for example ISO 27001 is quite an expensive scheme, so it's something that can add some credibility to a business in terms of from a marketing perspective, giving confidence to customers as well as having confidence within the business itself, assuming it's approached with the right mentality." (Strand A, 1-49, Information Security Consultant)*

(#28) "I approach it from a point of view this is going to improve your business...it's a useful tool to protect what you're doing. It's not just the government who are gonna to be looking at this, there's gonna be other people within your supply chain that this is gonna benefit you." (Strand A, 1-49, Information Security Consultant)

(#29) "[Getting hacked has] been a good thing because it's made me realise Cyber Essentials is out there the scheme, which is great. If I want to progress to the Plus bit I can do, if I want to do ISO 27001 I can do. It's made us as a business and as team, we became so much more aware of all the different loopholes all the different entry points for these criminals to get into the business, and so in a way, it was a bad thing but it highlighted the weaknesses and then we've turned those into strengths now. So yes, it was devastating, however, it shone a light on something I believe is not going away. Unfortunately this is here to stay, cause we live on the internet, don't we?" (Strand A, 1-49, Environmental Consultancy)

(#29) "It was quite interesting sitting down thinking about you know what do we do about backups, what do we do about passwords, what do we do about this thing called malware protection...it definitely forces you to address your gaps and it forces you to address the issues. And now when we do induction, we go through Cyber...we linked it to our induction pack, and we've got a whole section now on Cyber and Cyber policy and the bring your own device to work. So that as the business grows and we take on more staff, we're not ignoring it. We're facing it head on from day 1." (Strand A, 1-49, Environmental Consultancy)

(#29) "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, which means we look after our boundaries, our malware, our patch management. We've got antivirus. We've achieved it and we've been independently audited and we can prove that we look after the hardware and the software and we're not just gonna let someone steal our data and walk off with our customer information. We use it as a unique selling point." (Strand A, 1-49, Environmental Consultancy)

(#30) "It was just a good tick in the box...as far as I know we are the only clinical trials unit that are Cyber Essentials certified. So it was just a way of having a unique selling point...and just a way of saying we are doing all of these things to make sure we're treating data securely and responsibly." (Strand A, 50-249, Medical Research)

## 6.4 Achieved sample

### 6.4.1 Strand A

	TARGET	TOTAL
Phone	22	22
F2F	8	8
Paired	Max 5	1
<b>TOTAL</b>	<b>30</b>	<b>30</b>

Size	TARGET	TOTAL
1-49	12	22
50-249	12	5

250+	6	3
<b>TOTAL</b>	<b>30</b>	<b>30</b>

Sector (Max 8 each)	TARGET	TOTAL
Hi-tech industries (Pharmaceutical, Electronics, etc.)		x1 Pharmaceutical x1 Hi-tech industries
Insurance provider		x1 insurance provider
Cyber industry	Max 6	x5 Cyber Security Consultancy
IT Consultants/QG consultants	Max 4	x1 IT Security Consultancy x2 IT consultancy x1 IT local authority
Other		x3 Education Other - Charity & Think tank x1 Vehicle Sales x1 Recycling & waste management x1 Auctioneer x1 Charity x1 Audit Consultancy x1 Engineering x1 Ergonomics x1 Trade organisation x1 Recycling waste & IT Solutions x1 Specialist Recruitment x1 Risk Analysis x1 Environmental Consultant x1 Scientific research
<b>TOTAL</b>	<b>30</b>	<b>30</b>

Experience/Complexity	TOTAL
Very Positive/Very Easy	12
Somewhat positive/somewhat easy	12
Neither positive or negative / easy nor difficult	5
Somewhat negative / difficult	1
Very negative / difficult	0
<b>TOTAL</b>	<b>30</b>

#### 6.4.2 Strand Bi – Message testing

	<b>Group 1: Small (1-49)</b>	<b>Group 2: Medium (50-249)</b>
<b>Phase 1- London</b>	<b>5</b>	<b>6</b>
<b>Phase 2 – Birmingham</b>	<b>6</b>	<b>5</b>
<b>TOTAL</b>	<b>11</b>	<b>11</b>

	<b>Phase 1 - London</b>	<b>Phase 2 - Birmingham</b>
<b>SECTOR (max 8)</b>		
Retail	1	2
Manufacturing	1	4
Financial services	2	
Telecommunications		
Online media (e.g. information provider, entertainment provider, etc.)	2	
Hi-tech industries (Pharmaceutical, Electronics, etc.)		
Insurance provider		
Other, namely (record)	5	5
	RECRUITMENT EDUCATION PROPERTY/CONSTRUCTION TRANSPORT HOSPITALITY	Business consultancy Recruitment Construction Service cleaning Service security Transport
<b>ENGAGEMENT</b>		
Not taken or considered taking any action to increase our cyber security protection	2	2
Has considered looking into taking action to increase our cyber security protection	3	2
Has looked for information about taking action to increase our cyber security protection	2	2
Has sought advice on taking action to increase our cyber security protection	3	2
Has taken measures to increase our cyber security protection		2
Has updated our cyber security protection	1	1

### 6.4.3 Strand Bii - Remote User Testing

ACHIEVED	
SIZE	
1-49	5
50-249	6
SECTOR (max 4)	
Retail	3
Manufacturing	
Financial services	
Telecommunications	
Online media (e.g. information provider, entertainment provider, etc.)	1
Hi-tech industries (Pharmaceutical, Electronics, etc.)	
Insurance provider	
Other, namely (record)	7
	(heating/energy) (Healthcare/mobility) (construction) (leisure) (leisure) (leisure) (healthcare)
AREA	
North England	3
South England	3
The Midlands	2
Scotland	3
ENGAGEMENT	
Not taken or considered taking any action to increase our cyber security protection	1
Has considered looking into taking action to increase our cyber security protection	1
Has looked for information about taking action to increase our cyber security protection	3
Has sought advice on taking action to increase our cyber security protection	3
Has taken measures to increase our cyber security protection	3
Has updated our cyber security protection	0

## 6.5 Topic Guides

### 6.5.1 Strand A

#### DCMS Cyber Essentials - Strand A – Process Evaluation

#### Depth interviews: Topic Guide (45-60 mins)

##### 1. Introduction – 3 mins

- Thanks for agreeing to take part in the research. We are conducting this research on behalf of DCMS (the Department for Culture, Media and Sport).
- Introduce yourself and TNS-BMRB – an independent social research agency
- This research is exploring businesses' experiences of the Cyber Essentials Scheme, to understand how to improve it.

- This research is voluntary - participation will not affect your current or future relationship with DCMS or the Cyber Essentials scheme accrediting bodies
- The research is confidential and anonymous – though anonymised transcripts of the session will be provided to DCMS
- The information provided will be used for research purposes only
- Interested in their honest views and opinions
- Length: 45-60 minutes
- Gain permission for audio recording

## **2. Background – 3-5 mins**

- Introduce themselves
  - Brief background to their business – size, sector, and business activities
  - Current role and how long they have been in it
- How Cyber Security fits into their role
  - in terms of how it fits with their skills/expertise (e.g. specialise in IT)
  - in terms of core/peripheral responsibility
- Whether anyone else is involved (*explore roles fully in paired depth*)
  - Who, in what capacity
- How would they describe their attitude to the threat of cybercrime to their business
  - Attitude of wider business/business owners (if applicable)

## **3. Decision to become certified with Cyber Essentials – 10 mins**

*This section aims to explore the process of discovering the scheme, seeking information, and reaching a decision to become certified.*

- Approximately when they became certified with Cyber Essentials
- Prior to Cyber Essentials, can they briefly describe their business' cyber protection level (i.e. low, medium, high)
- Can they recall where they first heard of Cyber Essentials
  - First impressions of the scheme
- Who was involved in finding out more information
  - What they wanted to know
  - Where they sought information (website? Elsewhere? Anyone they spoke to/sought advice from)
  - How easy/difficult it was to find out information
    - Perceptions of the website – how easy/difficult to navigate
    - Clarity of information
    - Anything missing



■ How the decision was made to become certified through the scheme

- Who was involved
- What factors/considerations influenced the decision
  - Any barriers to implementation

SPONTANEOUS, then probe: requirements from businesses they supplied, providing services to government, investor/customer pressure

- When were documents downloaded, how were these used
  - Views on the content in terms of clarity/ease of use
- Why they decided to adopt the scheme
- How they decided the level to opt for (Basic or Plus)

■ Whether their security systems, and policies already met the standard (prior to certification)

- Was this known at the point of deciding to become registered (i.e. they knew they already had the controls in place, and decided to certify)
- Whether their business meets any other information security standards such as ISO27000; whether they require certification
- Whether they are part of Cyber Security Information Sharing Partnership (CISP) or other cyber security schemes
- Whether they already have any have security measures that go beyond Cyber Essentials

#### **4. Becoming certified – 15-25 mins**

*Moderator to plot the points on a journey map, establishing the order of stages in the process. Probe for **detail** at each stage, in terms of the time taken, who was involved, level of difficulty, noting positive and negative experiences.*

■ Once the decision was taken to become certified, what were the next steps  
SPONTANEOUS, then probe:

- Deciding which provider to use for assessment and certification
  - Understanding/areas of confusion around having ABs and CBs
  - How they chose (AB and) CB, SPONTANEOUS, then:
  - Whether they compared different providers
  - Whether/how the fee influenced the decision
  - Most important factor
- Appointing an assessor
  - Assistance provided by the certifying body, if any
  - At what point
- Order of self-assessment, implementation, and certification (including how CB was involved and at what point)
  - Reasons for taking these steps
- Whether passed first time, or failed and reapplied
  - Support from CB at each stage;
  - Fees for reapplication

- Any actions taken to implement the Cyber Essentials measures  
*NB. Do not need detail about how they implemented each one, rather probe for order of the steps in the process, clarity/ease of understanding, and overall time/burden of implementing*
  - Which they were responsible for and any they needed to seek additional help
  - Which were easier, which were more challenging
  - Time taken
  - Any costs incurred
  - Any external resources required, e.g. security system testers, training providers etc.
- End of the process – receiving certification
- If not already covered: Explore understanding of the cost of accreditation
  - At what point they became aware of the cost

Reflecting on their certifying body:

- How they would rate the service received from the certifying body
- Whether their CB provides any other services to them, beyond cyber essentials

## **5. Cost/Benefits of certification – 10 mins**

- Their overall estimation of cost of becoming certified
  - Whether they have calculated this before
  - Direct costs and staff time
  - Whether they see this as high
- Overall estimation of value to their business

SPONTANEOUS, then probe:

- Whether it is advertised / used to differentiate their business
- Where it is displayed (on website, other marketing materials?)
- Impact on suppliers/supply chain; how
- Impact on insurance costs (if they have (cyber) insurance)
- Views of owners/senior management
- Any other benefits
- If no value – why not
- Impact of failing the first time (if applicable)
  - Any additional costs incurred
  - Impact on perception of value
- Overall – whether they consider it to represent value for money
  - Why/why not
- Whether getting Cyber Essentials has had any longer term effect on theirs / the businesses awareness / knowledge / preparedness to deal with cyber threats

## **6. Improving the scheme – 5 mins**

- What, if anything, could have improved their experience
- Whether they consider the cyber security of their suppliers
- Whether they have ever suggested their suppliers become certified through the scheme
  - Would they in the future; why/why not
- Whether they have considered renewing their accreditation
  - Why/why not
- In one sentence, how they would describe their experience of becoming certified through Cyber Essentials
- Whether they would recommend it to other businesses like them, why/why not

## **7. Wrap up – 2 mins**

- Any other suggestions to improve any aspect of the scheme
- Any final comments/questions
- Thank and close
- Explain process and timescale for debit card incentives

## **6.5.2 Strand Bi**

### **1. Introduction**

- Introduce yourself and TNS-BMRB – an independent social research agency
- We are conducting this research on behalf of DCMS (the Department for Culture, Media and Sport)
- This research is exploring how businesses think about and protect themselves from cyber crime. DCMS wants to understand and learn more about **how to communicate with businesses about this issue**. In these sessions we will be looking at some messages and materials about cyber crime and the Cyber Essentials scheme and discussing your views and opinions about them. The results will help DCMS to develop the messaging for the scheme.
- In this session some language may be used inter-changeably – cyber crime, online fraud, internet threats and cyber security / protection
- No right or wrong answers – interested in your views
- Length – 90 minutes
- This research is voluntary - participation will not affect your current or future relationship with DCMS or the Cyber Essentials scheme accrediting bodies
- The research is confidential and anonymous – anonymised transcripts of the session will be provided to DCMS
- The information you provide will be used for research purposes only.
- Gain permission for audio recording.

### **2. Background – 5 mins**

- Introduce themselves

- Name, current role and how long they have been in it
- Background about their business – its sector and products / services
- Their role with regards to cyber security in their business

### **3. Existing understanding and views around cyber crime and cyber security – 10 mins**

- Moderator to lead a brief discussion on participant understanding of cyber crime

- What constitutes cyber crime / cyber security
- What level of risk they perceive this to pose to their business (*explore with those perceiving this to be a low risk first and then those reporting high risk*)
- What level of risk they perceive this to pose to businesses in the UK more generally
- Sources of knowledge
- How important cyber crime is relative to other priorities?

- Moderator to lead a brief discussion about participant understanding cyber security measures

- Ways businesses can protect themselves from cyber crime
- Sources of knowledge

- Moderator to lead a discussion about seeking information about cyber security

- Whether participants have looked for information about cyber / online security
  - Sources of information
  - If they have not sought information – where they would seek information (*Prompt - business organisation / trade association, government, police, local authority, anti-virus firm, retailer, online search engine, consumer organisation, citizens advice*)
  - Who they would trust to offer good advice
  - Explore barriers to seeking information
- What sort of cyber security information people have looked for / would be interested in looking for
  - *Prompt - how to protect customer data; how to sell goods and services online safely; how to fix a specific problem (e.g. spam email; a hacked account); how to send/share files with sensitive information; how to avoid viruses / malware; how to spot suspicious emails; choose security software etc)*
- Action and measures, if any, their business has taken to protect themselves from cyber crime
  - Explore any barriers and challenges to action experienced

- Explore which, if any, Government cyber security schemes they are aware of

- Briefly explore views on the effectiveness of these

- Check levels of awareness of the Cyber Essentials scheme

- Sources of awareness
- Whether they know anyone who is/has completed the scheme
- Knowledge and understanding of the scheme

- Engagement with the scheme (e.g. whether they have visited the website; considered seeking certification; sought further information about the scheme; contacted the accrediting bodies)

#### **4. Encouraging interest in cyber security – 20-25 mins**

*Moderator to explain - in this session we are going to look at some messages about cyber crime / cyber security. We would like to know what you think about these message and whether they would encourage and motivate you to seek more information about cyber security and to take action on cyber security. Explain that they would see these messages online, on the Cyber Essentials website and also in emails and online ads.*

*Researcher notes:*

- statistics are from DCMS' 2014/15 and 2015/16 Breaches Survey
- DDoS (Distributed Denial of Service) is a type of attack where a website is overloaded by connections from multiple computers, causing it to go offline

Moderator to introduce one message at a time and display these on the screen and also show an A4 hard copy to the group (Stimulus 1)

#### **REVERSE MESSAGES FOR YOUR SECOND GROUP**

*See Appendix 6: Stimulus materials (Strand Bi) Phase 1 Stimulus 1, Phase 2 Stimulus 1*

*Moderator to show each message in turn and ask the questions below, sorting the messages into two piles – those which are perceived to be more and less interesting / relevant to respondents*

- Moderator to probe on each message in turn:
  - How does this make you feel?
  - Relevance – is it aimed at them? If not, why not?
  - What would make it more relevant / interesting for them?
  - Is anything unclear?
  - Is the language appropriate?

*Moderator to return to the positive pile in turn and explore key themes:*

- Explore which message(s) would catch their attention
  - Are positive or negative messages about this topic more likely to draw their attention?
- Which **one** stands out the most for them
  - Does this message make you want to do anything? If so, what?
- Which messages are most relevant to them
- Which messages would be **most** likely to encourage them to seek information about cyber security – why?
- Which messages would be **most** likely to encourage them to take action on cyber security – why?

*Moderator to return to the more negative pile in turn and explore key themes:*

- Explore why these messages are perceived to be less interesting / relevant

- Explore how they could be made more relevant
- Which messages would be **least** likely to encourage them to seek information about and take action on cyber security – why?

## **5. Testing key messages – 20 mins**

*Moderator to explain that in this section we are going to look at some messages about the Government's Cyber Essentials Scheme. We would like to know what you think about these messages and whether they provide enough information about the scheme, and which of these messages would most encourage you to be interested in the scheme, seek more information about it and sign up.*

Moderator to hand out stimulus material to respondents – one copy per respondent (Stimulus 2)

*Moderator to ask participants to spend 5 minutes reading through the information. Then ask participants to use the blue, red and green pens to annotate the messages:*

- In green – circle words / phrases / messages which interest them and would encourage them to seek information and sign up for the scheme. [Encourage them to annotate the messages and explain why these messages would motivate them]
- In red – circle words / phrases / messages which are off putting or confusing [Encourage them to annotate to explain why]
- In blue – indicate where they would like more information

Moderator to lead a discussion on:

- Engagement and cut through
  - Relevance - How relevant are these messages to their business – are they interesting, in line with what they feel?
  - Which messages are most interesting / relevant to them?
  - *Which are most memorable?*

*Moderator to probe on:*

- Clarity and understanding
  - What are the key messages they take out; where do they get these from?
  - What do they think the designer of the messages wants them to take away?
  - How clear are the messages; do they understand what the scheme is, are they left with any questions – if so, what?
  - What would be the top 3 messages in terms of what they would want to know about the scheme?
  - *Are any of the messages surprising or confusing*
- Tone and language
  - How do the messages make them feel?
  - Is the tone appropriate?
  - Is anything unclear / confusing?
  - Which words / phrases particularly resonate with them
- Motivation, call to action
  - Does seeing any of these messages make them want to do anything?

- Which messages / aspects / phrases?
- What action? Why? Where would they go / what would they do?
- Which 3 messages would most make them want to take action?
- Would they know where to go for more information?
- Who / what would they ask for advice?
- Explore challenges / barriers to action they might face
  - How would they overcome these
  - Which messages motivate them to overcome barriers
- Improvements
  - What would they change to make the messages more engaging for businesses – why (e.g. language, tone, content?)
  - Is there anything further they would like to inspire them about the scheme?
  - Is there anything missing? (Details about cost, the threat, the benefits?)
- Explore to what extent messages join up with:
  - Other knowledge about cyber security
  - Wider government messaging around cyber crime

## **6. Testing the leaflet – 10 mins**

*Moderator to explain that in this section we are going to look at a leaflet for the Cyber Essentials Scheme. We would like to know your views on this, whether you find it interesting and whether it provides enough information about the scheme, and whether it would encourage you to find out more about the scheme and sign up.*

Moderator to hand out the leaflet – one per respondent (Stimulus 3)

*Moderator explain that this leaflet would be handed out to businesses. Ask participants to spend 5 minutes reading through the leaflet. Then ask participants to use the blue, red and green pens to annotate the leaflet:*

- In green – circle words / phrases / messages which interest them and would encourage them to seek information and sign up for the scheme. [Encourage them to annotate the messages and explain why these messages would motivate them]
- In red – circle words / phrases / messages which are off putting or confusing [Encourage them to annotate to explain why]
- In blue – indicate where they would like more information

Moderator to probe on:

- Clarity and understanding
  - What are the key messages they take out; where do they get these from?
  - How clear are the messages; do they understand what the scheme is, are they left with any questions – if so, what?
  - *Is any information missing?* (Details about cost, the threat, the benefits etc?)
- Tone and language
  - How do the messages make them feel?
  - Is the tone appropriate?
  - Is anything unclear / confusing?
  - Which words / phrases particularly resonate with them

- Motivation, call to action

- Does seeing this leaflet encourage them to seek more information about the scheme; visit the website; sign up for the scheme
- Explore challenges / barriers to action they might face
  - How would they overcome these
  - Which messages motivate them to overcome barriers

- Improvements

- What would they change to make the messages more engaging for businesses – why (e.g. language, tone, content?)
- Is there anything further they would like to inspire them about the scheme?
- Is any information missing?
- Is there any further information they would require to find out more about the scheme?

## **7. Testing adverts – 5 mins**

*Moderator to explain that we are going to look at some online adverts for the Cyber Essentials Scheme. We would like to know your views on these adverts. Explain they would appear as an advert when looking at a website – possibly one connected to this subject (e.g. on a business advice page)*

Moderator to show adverts on the screen (Stimulus 4)

Moderator to probe on:

- Whether the adverts are a good reflection of the scheme
- Whether the adverts are relevant / interesting
- Whether it is clear
- Whether it is credible
- Whether it is clear who the scheme is owned by – whether it would make a difference to them if the HM Government logo was on the advert
- Whether they would click through to the website – why / why not?
- Improvements
  - What would they change to make the adverts more engaging for businesses – why (e.g. language, tone, content?)

## **8. Channels – 5-10 mins**

- Explore how participants would like / expect to be informed about the scheme, and the most appropriate:
  - Channels
  - Timing
  - Messengers
- Moderator to explore what else would make respondents take action and sign up for Cyber Essentials (beyond communications and a website). *Record spontaneous suggestions and then:*

Probe:



- Media coverage
- Phone call
- Information session
- Tailored report to their company
- Talking to other businesses who have become certified
- Case studies
- More details about the benefits
- More details about the risks / threats
- Financial incentives

■ How would you like to hear about these other measures?

- Which channels?

## **9. Summing up – 5 mins**

■ Moderator to explore summary views:

- Will you look for any further information about cyber security?
- Will you take any action regarding cyber security?
- Will you seek information about Cyber Essentials? (where will you go?)
- Will you sign up for Cyber Essentials? (why? Why not?)

■ Overall – what messages about the Cyber Essentials Scheme do you remember? (which stood out, which were most distinctive, which made you feel positive about the scheme?)

■ After seeing all of the messages, how do you feel about cyber crime?

- How big a risk do you think this is for your business?
- How big a risk do you think this is for UK businesses more generally?

## **10. Close**

■ Any final comments

- Thank and close
- Explain how incentive cards work

## **6.5.3 Strand Bii**

### **1. Introduction**

We are glad you've agreed to participate in this website testing. This research is being conducted by TNS BMRB – an independent research agency specialising in social research – on behalf of the Department for Culture, Media and Sport (DCMS).

This research will explore how businesses think about and protect themselves from cyber-crime. In this session we will be looking at the Cyber Essentials scheme website and discussing your views about it.

Please be reassured that this is not a test of your knowledge and there are no right or wrong answers – we are just interested in your honest opinions and feedback. Participation in the research is voluntary, confidential and anonymous – we will not share your name or details with DCMS or any other organisation, or identify you/your business in the report.

The test should take between 20-30 minutes to complete, so please make sure you've got enough time to complete it now in one sitting. Everyone who successfully finishes the tasks and the survey questions will be sent £60 as a thank you.

## **This is how this test will work:**

You will be shown the Cyber Essentials website. Here's an overview of your "job" for the next 15-20 minutes:

- Your image and your voice will be recorded throughout.
- We want you to **tell us what you're thinking and doing** as you navigate through the site.
- To begin, you will see a number of specific tasks – please complete them, talking aloud through your thought process as you go.
- Next, you'll be asked some questions about the navigation and your reactions to the layout.

You will be able to see the tasks and questions at any time by clicking the "Show Tasks" icon.

Please click on "Hide tasks" in the same place when you are ready to continue with your tasks so that the website is not hidden by these drop-down instructions.

Once you have finished all the tasks, please click the "*I am finished*" icon. You will then see a short survey to complete, which should take around 5 minutes. Once you've answered the questions, please click "*Submit*" before closing the recorder.

**Important:** please wait until the video is fully uploaded, before you exit!

Also – if you think anything has gone wrong or you want to start again, please get in touch with the research team by phone or e-mail. Now, let's proceed with the questions. Please press the green "Start" icon in the upper left of this box, to start recording (if you have not done so yet).

## **2. Tasks**

*These tasks will appear at the top of the screen, over the Cyber Essentials website. Respondents will complete the task, and click on 'next task' when they have completed it.*

**Task 1:** Starting on the homepage: have a brief look around and tell us what your **initial impressions** are of the website. Tell us anything you notice about the page. Then tell us, what do you think the website is offering?

*Please remember to talk us through what you are thinking/ feeling.*

**Task 2:** If you wanted to **find out more about the scheme**, what steps would you take? (Feel free to click through to any links on the page, in order to do this).

*Please talk us through what you're doing and why.*

**Task 3:** Now going back to the homepage, please take a closer look at the **description of the scheme** near the top of the page. It reads: *The Cyber Essentials scheme provides businesses small and large...*

After reading the information in this box, **how clear are you about what Cyber Essentials is and aims to do?** Is there anything unclear, or confusing?

*Don't forget to describe aloud – what do you think the scheme is?*

**Task 4:** The next section on the page shows the Cyber Essentials **badges**. Please take a moment to read the information and *tell us in your own words* what you think the differences are between the two badges. Is there anything unclear here, or confusing?

**Task 5:** Please take a look at the section '*What Industry has to say about Cyber Essentials*'. Please have a read through some of the **quotes**. *Talk us through your thoughts about these* – do they help clarify what the scheme is? Would the quotes encourage you to take up the scheme? Why/ why not?

**Task 6:** Please have a look at the next section 'Cyber Essentials FREE downloads'. **Before clicking** – please describe what you think the downloads are for? Do you think you'd be likely to download these? Why/why not?

**Task 7:** Take a moment to **click through and scan** the free documents. Talk us through what you think of these: do you think you would use them? Why/why not?

**Task 8:** Now imagine you are **trying to sign up to the scheme:** what steps would you take? If you didn't already, click through to one of the accrediting bodies. *Don't forget to talk us through your thoughts/feelings, and what you think you would need to do next.*

**Task 9:** (whilst still on the Accrediting bodies page) Is there anything you think is **missing** here, or anything **different to what you were expecting?** *Tell us any thoughts that struck you whilst you were visiting those pages.*

**Task 10:** Please now go back to the Cyber Essentials home page and go to the **self-assessment questionnaire** at the bottom of the homepage and take the 'test', based on the business you work for. *Please talk us through your thoughts/ feelings on the process of the questionnaire as you answer it (including any positives or negatives).*

**Task 10:** After taking the self-assessment questionnaire, can you tell us: are you now clearer on what the Cyber Essentials scheme is? How helpful did you find the final score and assessment at the end? Did taking the questionnaire make you more/ less likely to want to pursue the Cyber Essentials scheme? *Make sure you've answered all three questions verbally!*

**Task 11:** Overall, what are your thoughts of this website? Just tell us your top of mind feedback about the site.

Now you have finished with the recorded part of this study, you can press the 'I am finished' button and you will be asked to complete a short survey.

### **3. Survey**

- 1) Overall, on a scale of 1-5, how easy did you find it to **navigate** the website and get relevant information on the Cyber Essentials scheme?

Where 1= Very easy and 5 = Very difficult

(1-5 scale response)

- 2) What did you think about the **amount of text** / information on the website?

- Not enough
- About right
- Too much

(Single choice response)

- 3) What did you think about the **layout** of the information on the home page? Would you prefer this to be all on one page as it currently is or split across separate webpages which you can click through, why?

(Open text response)

- 4) What **improvements**, if any, would you suggest to make it easier to get more information?

(Open text response)

5) Did you notice the **URL** of the site [www.cyberstreetwise.com/cyberessentials](http://www.cyberstreetwise.com/cyberessentials) - what did you think of it – was it confusing at all?  
(Open text response)

6) Which of the following do you think is the most appropriate **URL address** to host this website:

- [www.cyberstreetwise.com/cyberessentials](http://www.cyberstreetwise.com/cyberessentials)
- [www.cyberessentials.org.uk](http://www.cyberessentials.org.uk)
- [www.gov.uk/cyberessentials](http://www.gov.uk/cyberessentials)
- It doesn't make a difference

(Single choice response)

7) Is there any other information **missing** on the website which you would expect?

*Please select all that apply.*

(Multiple choice response)

- Pricing information
- How to implement the Cyber Essentials Scheme
- Steps required to get the certificate
- What the process is
- How long it takes
- Other

8) If you selected other on the previous question – please specify here what else you think is missing on the website.

9) Based on your experience so far, **how much** do you think the Cyber Essentials scheme costs? Is it free?

Explain the **reasons** for your response.

(Open text question)

10) If there was an information **pack** about the Cyber Essentials scheme, what **format** would you prefer:

- e-mailed to you
- instant download (no e-mail needed)
- posted in hard copy
- automated online tool
- Other

(Single choice response)

11) If you selected other on the previous question – please specify here what format you would prefer for an information pack to be sent to you.

12) What **key information** would you want to be included in an information pack?

(Open text question)

13) Would any of the following encourage you or your business to sign up for the Cyber Essentials scheme? Please select the top three most important.

- a phone call
- an information session
- a tailored report on your company

- an opportunity to talk to other businesses who have been through Cyber Essentials
- case studies
- more details on the benefits
- more detail on the potential threats/dangers of cyber Crime
- other
- none of the above

(Multiple choice response; multi-code)

14) If you selected other on the previous question – please specify here what would encourage you or your business to sign up for the Cyber Essentials scheme.

## 6.6 Stimulus materials (Strand Bi)

### Phase 1 - London

#### Phase 1 (London) Stimulus 1

- (1) *Cyber crime is a growing threat to UK businesses – criminals target customer data, company finances, and the safety and integrity of IT systems.*
- (2) *1 in 4 businesses experienced a cyber breach / attack in the past 12 months*
- (3) *4 is the average number of breaches suffered by small businesses in the last year*
- (4) *By taking action on cyber security you can protect customer data, company finances and the safety and integrity of IT systems.*
- (5) *16% of small businesses were hit by DDoS attacks in the last year.*
- (6) *50% of the worst breaches in the year were caused by inadvertent human error.*
- (7) *59% of businesses expect there will be more security incidents in the next year than last.*
- (8) *28% of the worst security breaches were caused partly by senior management giving insufficient priority on security - up from 7% a year ago.*
- (9) *You can protect against the common threats likely to harm your business by using free Government advice and training*
- (10) *The Federation of Small Businesses estimates the average cost of a cyber crime on a small business to be around £3,000. Government research says the average cost of a cyber attack to a small business is £3,100*
- (11) *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.*
- (12) *Displaying the Cyber Essentials badge will show customers that you take cyber security seriously*
- (13) *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.*



### **Cyber Essentials Scheme**

1. GCHQ analysis shows that over 80% of successful cyber attacks exploit basic vulnerabilities in IT systems. Cyber Essentials shows you how to address those vulnerabilities.
2. Cyber Essentials sets out the basic technical standards which will help protect organisations from the majority of threats on the internet.
3. Cyber Essentials protects your business against the common threats on the Internet.
4. Since its launch in summer 2014, around 2,000 businesses have adopted the scheme, including many in the FTSE100 and household names such as Barclays, Vodafone and National Grid.
5. 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.
6. The Cyber Essentials Scheme has been developed in order to meet the UK Cyber Security Strategy objective of making the UK one of the safest places in the world to do business in cyberspace.
7. The scheme is Government-backed and supported by industry. It delivers an action from the UK Cyber Security Strategy to provide organisations with clarity on the basic requirements to implement good cyber security practice.
8. Cyber Essentials comprises core actions necessary to mitigate the majority of cyber threats through five key controls, within the context of the '[10 Steps to Cyber Security](#)' (and reflecting those covered in well-established and more extensive cyber standards, such as the ISO/IEC 27000 series, the ISF's Standard of Good Practice for Information Security and the IASME Standard).
9. FREE to download from [www.cyberstreetwise/cyberessentials.com](http://www.cyberstreetwise/cyberessentials.com), organisations can use the requirements to implement essential security controls.
10. Those which want or need to gain independent assurance that they comply can apply for a Cyber Essentials badge - awarded to organisations successfully independently assessed and certified through the assurance framework.
11. The badge helps show customers, partners or clients that the organisation takes cyber security seriously, boosting reputations and providing a competitive selling point.
12. Cyber Essentials is accessible to all and applicable to all organisations, of all sizes, and in all sectors.
13. We encourage all organisations to adopt the requirements to some degree. This is not limited to companies in the private sector, but is applicable to universities, charities, and public sector organisations.
14. Funded by the National Cyber Security Programme, the scheme was developed and delivered with industry. It is cost-effective and suitable for smaller businesses with two levels of assurance available: Cyber Essentials and Cyber Essentials Plus. Costs are set by individual "licensed" companies, independently assessing applicants, so market forces set rates.
15. Government sought to identify its preferred standard but nothing fully met our requirements. Industry told us they had the appetite to work with Government to create something new that did meet our requirements.

16. Organisations that are assessed and awarded the badge will be demonstrating that they have achieved a certain level of cyber security. This also gives customers and other stakeholders a clear indicator of whether a business is taking cyber risk seriously which gives a competitive advantage.
17. Since October 2014, central government departments were required to adopt Cyber Essentials into procurement processes for certain ICT, sensitive or personal information handling contracts, helping address cyber security risks in supply chains.
18. Government works with large primes and FTSE 100 companies which have achieved Cyber Essentials to encourage the smaller firms in their supply chains to adopt it.
19. We are supporting business productivity and growth through improved cyber behaviours.

## **Phase 2 - Birmingham**

### Phase 2 (Birmingham) Stimulus 1

- (1) *1 in 4 businesses experienced a cyber breach / attack in the past 12 months*
- (2) *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.*
- (3) *50% of the worst breaches in the year were caused by inadvertent human error.*
- (4) *59% of businesses expect there will be more security incidents in the next year than last.*
- (5) *28% of the worst security breaches were caused partly by senior management giving insufficient priority on security - up from 7% a year ago.*
- (6) *You can protect against the common threats likely to harm your business by using free Government advice and training*
- (7) *Government research says the average cost of a cyber attack to a small business is over £3,000*
- (8) *"New Government research shows 51% of medium-sized businesses detected one or more cyber security breaches in the last 12 months"*
- (9) *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.*
- (10) *Displaying the Cyber Essentials badge will show customers that you take cyber security seriously*
- (11) *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.*
- (12) *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) *The Cyber Essentials scheme checks whether your business meets 5 basic cyber security requirements. You become certified when you meet these requirements.*







### **Cyber Essentials Scheme**

1. GCHQ analysis shows that over 80% of successful cyber attacks exploit basic vulnerabilities in IT systems. Cyber Essentials shows you how to address those vulnerabilities.
2. Cyber Essentials protects your business against the common threats on the Internet.
3. Cyber Essentials sets out the basic technical standards which will help protect organisations from the majority of threats on the internet.
4. The Cyber Essentials scheme checks whether your business meets 5 basic cyber security requirements. You become certified when you meet these requirements.
5. Cyber Essentials requires your business to have five controls in place:
  - a. Malware protection [i.e. using anti-virus software]
  - b. Patch management [i.e. updating software]
  - c. Access control [restricting access to those who need it]
  - d. Secure configuration [setting up systems securely]
  - e. Boundary firewalls [to prevent unauthorised access]
6. To complete the scheme you need to:
  1. Read the Cyber Essentials documents
  2. Contact one of the Accrediting Bodies [contact details on website]
  3. Complete the Cyber Essentials questionnaire
  4. An assessor will verify your answers
  5. Your Cyber Essentials certificate is awarded.
7. Since its launch in summer 2014, around 2,000 businesses have adopted the scheme, including many in the FTSE100 and household names such as Barclays, Vodafone and National Grid.
8. The Cyber Essentials Scheme has been developed in order to meet the UK Cyber Security Strategy objective of making the UK one of the safest places in the world to do business in cyberspace.
9. The scheme is Government-backed and supported by industry. It delivers an action from the UK Cyber Security Strategy to provide organisations with clarity on the basic requirements to implement good cyber security practice.
10. Cyber Essentials comprises core actions necessary to mitigate the majority of cyber threats through five key controls, within the context of the '10 Steps to Cyber Security' (and reflecting those covered in well-established and more extensive cyber standards).
11. FREE to download from [www.cyberstreetwise/cyberessentials.com](http://www.cyberstreetwise/cyberessentials.com), organisations can use the requirements to implement essential security controls.
12. Those which want or need to gain independent assurance that they comply can apply for a Cyber Essentials badge - awarded to organisations successfully independently assessed and certified through the assurance framework.

13. The badge helps show customers, partners or clients that the organisation takes cyber security seriously, boosting reputations and providing a competitive selling point.
14. Cyber Essentials is accessible to all and applicable to all organisations, of all sizes, and in all sectors.
15. We encourage all organisations to adopt the requirements to some degree. This is not limited to companies in the private sector, but is applicable to universities, charities, and public sector organisations.
16. Funded by the National Cyber Security Programme, the scheme was developed and delivered with industry. It is cost-effective and suitable for smaller businesses with two levels of assurance available: Cyber Essentials and Cyber Essentials Plus. Costs are set by individual "licensed" companies, independently assessing applicants, so market forces set rates.
17. Organisations that are assessed and awarded the badge will be demonstrating that they have achieved a certain level of cyber security. This also gives customers and other stakeholders a clear indicator of whether a business is taking cyber risk seriously which gives a competitive advantage.
18. Since October 2014, central government departments were required to adopt Cyber Essentials into procurement processes for certain ICT, sensitive or personal information handling contracts, helping address cyber security risks in supply chains.
19. Government works with large primes and FTSE 100 companies which have achieved Cyber Essentials to encourage the smaller firms in their supply chains to adopt it.
20. Cyber Essentials supports business productivity and growth through improved cyber behaviours. Businesses with Cyber Essentials can display the Cyber Essentials badge and demonstrate to customers they take this issue seriously, thereby giving them a competitive advantage. Customers will have more confidence increasing demand and it will prevent cyber attacks and therefore loss of staff time.
21. The cost of the scheme is typically around £300 for a small business. Costs will be higher for larger & more complex organisations, e.g. those with more staff or more complex computer networks, and typically around £800 for a medium sized business.

#### Phase 1 & 2 Stimulus 3

## 5 Cyber Essentials key controls

**Boundary firewalls and internet gateways** – good set up of devices designed to prevent unauthorised access to or from private networks

**Secure configuration** – systems are configured in the most secure way

**Access control** – only those who should have access to systems have access, and at the appropriate level

**Malware protection** – virus and malware protection is installed and up-to-date

**Patch management** – the latest supported version of applications is used and all necessary patches have been applied

## Further information

The Cyber Essentials free download and list of Accreditation Bodies can be found on the Cyber Essentials web (located on Cyber Streetwise):

[www.cyberstreetwise.com/cyberessentials](http://www.cyberstreetwise.com/cyberessentials)

Guidance to help maintain cyber security defences

10 Steps to Cyber Security available from GOV.UK at [www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility](http://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility)

What you need to know about Cyber Security available from GOV.UK at [www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know](http://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know)



Protect your business against cyber threats



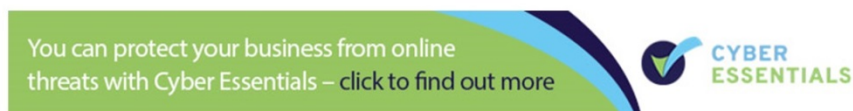
Information correct at time of publication  
September 2014  
© Crown Copyright



Cyber Essentials or Cyber

Getting assessed

Cyber Essentials Scheme online adverts



Phase 1  
& 2  
Stimulus

