A CALL TO ACTION:

The Cyber Aware Perception Gap

HM Government

Britainthinks
Insight & Strategy

CYBER AWARE

A CALL TO ACTION:

The Cyber Aware Perception Gap

HM Government

Britainthinks Insight & Strategy

CYBER AWARE

Introduced by Minister of State for Security and Economic Crime
The Rt Hon Ben Wallace MP

WHY SHOULD YOU CARE?

The internet has transformed modern life, bringing people closer together, and making the pace of business move faster than ever. What's more, the UK is a world leader in digital technology: we have one of the world's most successful gaming industries, are a leading light in the global FinTech industry, and we shop online more than anyone else in the world. The UK's digital economy is the largest of any G20 nation and, in 2016, 58% of UK businesses described online services as being a core part of the goods and services that their organisation provides.[1.2.]

But there is a sophisticated and growing threat to the UK's success. **Cyber crime has been identified as one of the biggest criminal threats to British business and the British economy,** with available estimates suggesting the cost could be billions of pounds each year. For many businesses affected by cyber crime, the impact goes far beyond the immediate financial cost, weakening business reputation and damaging trust in both individual businesses and business as a whole.[3.]

The UK Government is determined to make the UK a safer place - for businesses, small and large, and individuals - to interact and do business online. But the challenge of countering an issue that affects us all is huge.

This report summarises key research and identifies a large and growing gap between the nature of the threat, and public perceptions. A large proportion **of the public and Small and Medium-sized Enterprises (SMEs) vastly underestimate the risk of cyber crime and feel powerless to protect themselves against it.** There is a widespread belief that cyber criminals focus only on big businesses and celebrities rather than 'ordinary' people; a misconception that there are few consequences of being a victim of cyber crime; and an array of inconsistent advice that leads to dangerous inertia.

As a result of the perception gap, millions of people are leaving themselves, UK businesses and UK infrastructure vulnerable by failing to follow even the most basic secure online behaviours. Whether targeting global corporations or micro-SMEs, criminals frequently exploit the **weak cyber security of individuals** to facilitate their attacks. The recent experiences of Camelot and Deliveroo show that a company can be publicly blamed for breaches resulting from the poor cyber security (and subsequent data theft) of other organisations or the poor cyber security of their customers.[4.5.]

[1.] Boston Consulting Group, The Internet Economy in the G-20, 2012
[2.] Department for Culture, Media and Sport, Cyber Security Breaches Survey 2017, 2017
[3.] Home Office, Understanding the Costs of Cyber Crime, 2018
[4.] City AM, Thousands of online accounts feared hacked at National Lottery Operator Camelot, 2016, http://www.cityam.com/254689/thousands-online-accounts-feared-hacked-national-lottery
[5.] BBC News, Deliveroo customers billed for unordered food, 2016 http://www.bbc.co.uk/news/technology-38070985

Increasing our cyber resilience has clear and immediate business benefits, ranging from reducing or eliminating financial loss from cyber crime, to minimising reputational costs, to reducing time costs associated with recovering from an attack. But **the benefits extend far beyond these immediate impacts,** including reducing risk and strengthening business resilience, and enabling business to continue embracing technology-driven innovations and solutions. It also has the potential to develop a business's reputation: customers expect trustworthy organisations to help them to help themselves.

We will have most impact if we **work together to bridge this dangerous perception gap,** encouraging individuals to take simple actions to protect themselves, Britain, British people and British businesses. By speaking with 'one voice' to provide more consistent advice on the basic actions people should take to improve their online security, we can achieve real change.

The Government is already playing its part, investing £1.9 billion over the lifetime of the current National Cyber Security Strategy, including investment in the Cyber Aware campaign which is working closely with the National Cyber Security Centre to provide the latest technical advice for the public and SMEs on how they can easily secure themselves online.[6.]

Raising cyber awareness is important if we are to take advantage of investment in capability currently taking place by both the public and private sector.

The public and SMEs don't just look to Government, but as the internet continues to proliferate within our lives, they also look to an increasingly wide range of businesses for information and advice about being secure online. By working together, harnessing the power of your trusted brands, with customers, colleagues and partners, using every available communications channel, we can help make the UK much more cyber resilient.

By making these small changes together, we can make a big difference and step-change our cyber security culture for the better to protect Britain from cyber criminals.

Minister of State for Security and Economic Crime
The Rt Hon Ben Wallace MP

[6.] HM Government, National Cyber Security Strategy 2016-2021, 2016

WHAT IS THE ISSUE?

As the internet continues to transform modern life, the public and businesses of all sizes need to adapt, integrating online security as standard in order to continue to enjoy the benefits that it offers.

A key barrier to the adoption of new online mindsets and behaviours is the significant **perception gap** between how the public think about cyber crime and the reality of the threat. The result of this perception gap is that many members of the public put themselves and the organisations they buy from or work for at serious risk of falling victim to cyber crime by delaying or deprioritising online security.

THE PERCEPTION GAP IS BASED ON THREE KEY MYTHS:

01. "Cyber crime isn't something that I need to be concerned about"

"You'd have to be full on paranoid to worry about it [cyber crime]" [7]

02. "Cyber crime isn't 'real' crime"

"Before you even realise it the bank will just give you your money back. You don't really have to even worry about it" [7]

03. "There is nothing more I can do to protect myself"

"If the experts can't even agree what I need to do, then how am I supposed to know?" [7]

In the course of day to day personal and business lives, there are numerous opportunities to drive behavioural change that will bridge these gaps between perception and reality. The public and SMEs increasingly expect a range of organisations to provide consistent and easily actionable advice on how to stay secure online.

[7] Illustrative verbatim quotes taken from BritainThinks, Cyber Behaviours and Financial Fraud Messaging Research, 2017

01

MYTH: "CYBER CRIME ISN'T SOMETHING I NEED TO BE CONCERNED ABOUT"

The public and SMEs need to feel responsible and empowered if they are to prioritise taking protective security actions. Latest research and insight indicates that we collectively need to make cyber security feel more relevant and actionable to overcome these barriers to action.[8]

KEY POINTS:

- Rather than accepting cyber security as a personal responsibility, many feel that it is "someone else's problem" and absolve themselves of responsibility through an overly passive interpretation of common expectations:
  - Consumers expect companies and service providers to protect their users.
  - Employees expect their employers to provide them with the tools to be secure online, and to employ others to ensure they are secure.
- Many assume that "someone like me" is unlikely to fall victim to cyber crime, with the typical victim assumed to be older and somehow "vulnerable":
  - Most associate cyber crime purely with cyber-related fraud, to which they feel that only less tech-savvy individuals would be likely to fall victim.
  - As a result many individuals are not taking sufficient responsibility for their cyber security, leaving themselves and the organisations they associate with at risk.

Recent qualitative research has highlighted an increase in awareness of cyber crime amongst both consumers and SMEs, often driven by high profile cyber security breaches.[9] However, growing awareness of cyber crime has not been accompanied by a similar increase in the belief that cyber security is a personal responsibility, or an increased uptake in protective behaviours.[10] The latest research suggests that this is driven by two key beliefs on the part of individuals:

31%

Only 31% of businesses say that cyber security is a very high priority for senior management

BELIEF: "My cyber security is someone else's problem"

Levels of strong concern about cyber crime are not high amongst consumers, and only 31% of businesses say that cyber security is a very high priority for senior management.[11,12] Qualitative research suggests that engagement with cyber security as a topic is limited, with many seeing it as "too complicated for someone like me".[13]

[8] BritainThinks, Cyber Behaviours and Financial Fraud Messaging Research, 2017
[9] BritainThinks, Qualitative Tracking Research, 2017
[10] Ipsos Mori, Cyber Security Tracker, 2017
[11] Ibid
[12] Department for Culture, Media and Sport, Cyber Security Breaches Survey 2017, 2017
[13] BritainThinks, Cyber Streetwise Strategy Planning, 2016

72% of consumers believe it is the responsibility of companies to provide them with the tools they need to protect their privacy, security and reputation online

Compounding this lack of concern is the belief that "it is someone else's responsibility to protect my online security".[14] 72% of consumers believe it is the responsibility of companies to provide them with the tools they need to protect their privacy, security and reputation online.[15] Research based on focus groups with SME employees and decision-makers suggests that employees (even in microbusinesses and smaller SMEs with no IT department) strongly believe that someone else in their organisation, rather than themselves, is responsible for cyber security.[16]

Recent qualitative research suggests that both consumers and SMEs tend to believe that the most important security behaviours are 'forced' on them (for example, being prompted to use a strong password when creating an account) and that other behaviours which aren't enforced are 'nice to have', meaning that many disregard cyber security advice.[17]

REALITY: If you fail to follow basic cyber security measures there is little that others can do to protect you

If an individual's password to their email account is as basic as Pa$$word and is accessed by a criminal there is little that an organisation can do to protect them

Whilst companies and organisations can provide tools and services to help individuals protect themselves from cyber crime, there is little they can do to help individuals who put themselves at risk. For example, if an individual's password to their email account is as basic as 'Pa$$word' and is accessed by a criminal there is little that an organisation can do to protect them, in much the same way that a burglar alarm will be unable to protect your home if you have told a criminal the deactivation code.

This means that it is crucial that individuals take personal responsibility for their security, ensuring that they do the basics to protect themselves from cyber crime. Businesses can help by driving customers to integrate additional security measures – qualitative research suggests that individuals are willing to accept interruptions to their 'customer journeys' to do this. Promoting such security measures can also help to strengthen a perception that an organisation is responsible.[18]

"Just as people protect their homes from burglary they also need to take responsibility to protect their digital presence. Simple steps such as downloading the latest software and applications updates, and securing your email with a strong separate password can defend against many online threats. These crimes destroy lives and livelihoods, together we can make the UK a hostile environment for cyber criminals."

T/Commander Dave Clark, City of London Police and National Co-ordinator for Economic Crime

[14] BritainThinks, Qualitative Tracking Research, 2017
[15] Deloitte, The Deloitte Consumer Review: Consumer data under attack: The growing threat of cyber crime, 2015
[16] John M. Blythe, Unpacking security policy compliance: The motivators and barriers of employees' security behaviours, 2015
[17] BritainThinks, Cyber Behaviours and Financial Fraud Messaging Research, 2017
[18] Ibid

BELIEF: "Someone like me won't fall victim to cyber crime"

Recent qualitative research suggests that the public's understanding of how cyber crime happens is limited to cyber-related fraud, as opposed to cyber-dependent crime (i.e. crimes that can only be committed through the use of Information and Communications Technology, where devices are both the tool for committing the crime and the target of the crime. Examples include hacking or using malware for financial gain).[19. 20.] Spontaneous associations with the term 'cyber crime' focus, primarily, on terms relating to fraud, such as 'identity theft', or methods through which cyber-related fraud might be perpetrated, such as 'phishing'.[21.]

Qualitative evidence suggests consumers and SMEs tend to believe they are "too savvy" to fall victim to online fraud

This also drives the belief that "someone like me" won't fall victim to cyber crime.[22.] Both consumers and SMEs tend to believe they are "too savvy" to fall victim to online fraud, believing that their accounts could only be hacked, or their identity stolen, if they 'willingly' give up their details by clicking on a link in a phishing email. They think that only people who are older, more vulnerable and less tech-savvy are likely to fall victim to cyber crime.[23.]

CASE STUDY: Michelle*

Michelle is in her mid-20s and lives in London. Michelle's bank account was recently attacked, but her money was immediately reimbursed.

"I've never been the victim of cyber crime... I mean my bank account was hacked but the bank gave me money back immediately, before I even noticed to be honest."

Michelle's computer has a number of viruses on it, but she doesn't feel these represent a 'cyber crime'.

"When my computer says I have this many viruses I don't care. As long as my computer runs it doesn't matter, they just make it slow." [24.]

*Michelle's name has been changed

68%

A 2016 KPMG survey of small businesses found that 68% of those surveyed that had never been a victim of a cyber breach thought there was little to no risk of them becoming one

Similarly, many SME owners believe that a business like theirs is unlikely to fall victim to cyber crime. A 2016 KPMG survey of small businesses found that **68% of those surveyed that had never been a victim of a cyber breach thought there was little to no risk of them becoming one.**[25.] Furthermore, recent qualitative research has suggested that SME owners tend to believe that their businesses are 'too small' for cyber criminals to bother targeting them, associating cyber breaches with larger, more high profile businesses.[26.]

[19.] Ibid
[20.] HM Government, National Cyber Security Strategy 2016-2021, 2016
[21.] BritainThinks, Qualitative Tracking Research, 2017
[22.] BritainThinks, Cyber Behaviours and Financial Fraud Messaging Research, 2017
[23.] Ibid
[24.] BritainThinks, Cyber Streetwise Strategy Planning, 2016
[25.] Cyber Streetwise and KPMG, Small Business Reputation and the Cyber Risk, 2016
[26.] BritainThinks, Cyber Behaviours and Financial Fraud Messaging Research, 2017

REALITY: Cyber criminals are successfully targeting everyone

Each year there are millions of incidents of cyber crime impacting people from all walks of life causing both financial cost and emotional distress. Between October 2016 and September 2017, the Crime Survey for England and Wales recorded 3.2 million fraud offences (over half of which were online) and 1.5 million computer misuse offences including malware attacks and hacking. There were 1.2 million victims of computer misuse offences, meaning **the average person is roughly 11 times more likely to fall victim to computer misuse than a robbery.**[27.]

There are no significant differences in likelihood of falling victim to computer misuse, aside from those aged 75+ who are less likely

Everyone (not just the older and less tech-savvy) is at risk. Typical victims of computer misuse are less likely to be very old (75+) compared to all other age groups.[28.] Furthermore, it is not just large organisations that are at risk. While 46% of businesses experienced at least one cyber security breach in 2016, the figures for micro (38%), small (52%) and medium (66%) firms show that businesses of all sizes are falling victim.[29.]

"Small and medium sized businesses should not be fooled into thinking that criminals do not target them, or that they are safe from online vulnerabilities. If you hold data, you are a viable target, and 45% of micro/small businesses were the victims of successful data breaches or attacks over the past 12 months." [30.]

John Unsworth, Chief Executive, London Digital Cyber Security Centre

Communicating that anyone can be a victim of cyber crime and that cyber security is a personal responsibility can help to overcome behavioural barriers.

WHAT OPPORTUNITIES ARE THERE TO:

- help your customers, employees, suppliers and clients understand their responsibilities when it comes to cyber security?

HOW CAN YOU CLEARLY COMMUNICATE:

- the reality of cyber crime and its potential impact for your customers, employees, suppliers and clients?
- that anyone can fall victim to cyber crime, not just older and more vulnerable people, big businesses or people in the public eye?

[27.] Office for National Statistics, Crime Survey for England and Wales, 2018
[28.] Office for National Statistics, Crime Survey for England and Wales, 2017
[29.] Department for Culture, Media and Sport, Cyber Security Breaches Survey 2017, 2017
[30.] Ibid

02

MYTH: "CYBER CRIME ISN'T REAL CRIME"

The public and SMEs will only take action if they feel and believe that the cyber crime threat is real.

KEY POINTS:

- The public are likely to feel that cyber crime is, essentially, "victimless" – despite the significant consequences of falling victim.
- The public are much less likely to report that they have been a victim of cyber crime than 'traditional' crimes.
- Individuals are failing to protect themselves and crimes are under reported to the relevant authorities.

Although awareness of cyber crime has increased in the past couple of years, recent research shows that the way the public think about cyber crime compared to 'traditional' offline crime differs significantly.[31] When thinking about cyber crime, the public are likely to feel it is "victimless" and, when they fall victim, are less likely to report it as a crime to the police and law enforcement than they are in the case of 'traditional' crime types.

BELIEF: "Cyber crime is a victimless crime"

Individuals and decision-makers in SMEs believe that the primary impact of falling victim to cyber crime is financial loss

Individuals tend to assume that the only potential consequence of falling victim to cyber crime will be financial loss, which is consistent with the perception that cyber crime is simply another form of financial fraud.[32] However, unlike with other forms of fraud, there is a widespread belief that banks will reimburse victims without any quibble.[33] As a result, victims often don't see themselves as such, and for many, cyber crime is considered to be victimless.

Decision-makers in SMEs also believe that the primary impact of falling victim to cyber crime is financial loss, with 'financial loss from theft of money' cited as their biggest concern related to cyber crime.[34]

[31] BritainThinks, Qualitative Tracking Research, 2017
[32] Ibid
[33] Ibid
[34] Ipsos MORI, Cyber Streetwise Pre-Campaign Tracker, 2015

REALITY: There are a number of significant consequences of falling victim to cyber crime

1 in 8

Individuals are not always reimbursed for their financial losses. Of the 1.6 million victims of bank and credit account fraud who experienced a financial loss, around 1 in 8 were not fully reimbursed

The belief that cyber crime is essentially victimless stands in stark contrast to the reality of the situation.

Individuals are not always reimbursed for their financial losses. Of the 232,000 victims of computer virus attacks (including malware) that the Crime Survey for England and Wales recorded as experiencing a financial loss between October 2016 and September 2017, only 4,000 were fully reimbursed. Of the 1.6 million victims of bank and credit account fraud who experienced a financial loss, around 1 in 8 were not fully reimbursed.[35.]

Current data shows that for businesses, the average cost of a cyber security breach is £1,570 (rising to £19,600 for larger businesses). According to a recent estimate based on data from 1,250 incidents between 2007 to 2015, web defacement, where the appearance of a webpage is maliciously changed, costs a business an average of £1,200 per incident. For those businesses that experience a malware infection, an average cost of £57,000 has been estimated using data surrounding 89 infections reported between 2009 and 2014.[36.]

£19.6K

For businesses, the average cost of a cyber security breach in 2016 was £1,570 (rising to £19,600 for larger businesses)

CASE STUDY: Justine Roberts, CEO of Mumsnet

In August 2015 Mumsnet was the target of a distributed denial of service (DDoS) attack:

“We were offline for a couple of quite lengthy periods. The site basically seized up and fell over. So that’s incredibly stressful. You are just trying to work out what’s going on and it goes incredibly quiet. It took a while for our ISP to work out that was what it was. A lot of resource was put into repelling that attack.”

At the same time users were targeted by a phishing attack:

“There was some curious activity that made us aware of it before we realised what it was. A couple of users reported posts had been made on their accounts but not by them. We looked on the database and saw that something unusual had gone on at the back-end.”

In response Mumsnet forced all users to change their passwords and engaged them in a dialogue about what they believed was happening.

“When users started noticing something odd was happening we immediately told them to change passwords. We actually forced them to, we logged people out and made them change their password.

[35.] Office for National Statistics, Crime Survey for England and Wales, 2018
[36.] Home Office, Understanding the Costs of Cyber Crime, 2018

There was a level of irritation but it was well worth doing. We took the view that potentially everything had been accessed and we had to warn users that might be the case and ask them to do a set of actions to mitigate against their data being used fraudulently."

There were significant time-costs for Mumsnet of resolving the technical issues behind the hack.

"A lot of people were working on nothing but this for two or three weeks. Several people were working literally round the clock, especially in our tech and production teams. It's basically crisis stations and all men to the pump and that kind of stuff."

THOSE WHO FALL VICTIM TO CYBER CRIME EXPERIENCE A NUMBER OF KNOCK-ON IMPACTS, BEYOND IMMEDIATE FINANCIAL LOSS. POTENTIAL IMPACTS INCLUDE:

BUSINESS IMPACTS

CONSUMER IMPACTS

Stopping normal operation until issue is resolved

Time spent fixing compromised or damaged devices and networks

Time spent with financial institutions (such as their bank or insurance) resolving transactions, claiming insurance , etc.

Time spent reporting crime to law enforcement

Effort spent resolving any disputed transactions that have occurred

Loss of intellectual property or commercially sensitive information

Damage to reputation or brand value – leading to potential loss of future earnings

Time spent resolving customer or client complaints (both publicly and privately)

Damage to customer, client and/or supplier relationships

BUSINESS IMPACTS

CONSUMER IMPACTS

Time spent fixing compromised or damaged devices and networks

Time spent contacting financial institutions (bank, insurers, credit reference agency, etc.) to resolve transactions and damage to credit scores

Time spent reporting crime to law enforcement

Loss of files with sentimental value (e.g. photos, videos, etc.)

Emotional harm and embarrassment

Time spent alerting others you have become a victim in order to protect them (e.g. if email hacked and phishing emails sent from your address)

Blackmail, extortion and coercion

BELIEF: "There is no point in reporting cyber crime"

Both consumers and businesses are much less likely to report that they have fallen victim to cyber crime, compared to 'traditional' offline crimes.

While there were an estimated 1.5 million incidents of computer misuse crime during the year ending September 2017, Action Fraud referred only 21,745 offences to the National Fraud Intelligence Bureau in the same period. Comparing this data to figures relating to a 'real world' equivalent of 'theft from the person' (386,000 estimated incidents and 95,684 crimes recorded by the police) indicates that many victims of cyber crime are not reporting in the same way they would if they were a victim of an offline crime.[37]

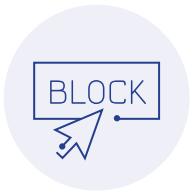
[37] Office for National Statistics, Crime Survey for England and Wales, 2018

Reporting cyber crime to Action Fraud is actually very easy. Visit: **www.actionfraud.police.uk** and submit a report using their easy to use form

There is a similar picture for businesses, with over half (57%) of businesses that experienced a cyber breach in 2016 failing to report the most disruptive breach to anyone outside of their organisation.[38] And amongst the 26% that did report their most disruptive breach to at least one external body other than their security provider, only 19% reported to the police and just 7% to Action Fraud.[39]

Recent qualitative research suggests this under-reporting of cyber crime happens because it isn't seen as a 'real crime', with the public feeling that there is little point reporting incidents to law enforcement.[40] Furthermore, qualitative research also shows that both consumers and SMEs struggle to understand the benefits of reporting cyber crime to law enforcement or other relevant parties (including insurers and customers). In particular, business owners have concerns that reporting will negatively impact their reputation and relationships with customers and clients.[41]

REALITY: Reporting cyber crime can help prevent future incidents and strengthen trust in your business



Reporting phishing emails to email providers helps to improve their ability to identify and block similar emails, thereby preventing others falling victim in future incidences

Reporting cyber breaches and implementing subsequently provided security advice from insurance firms has led to some businesses benefiting from a reduction in cyber insurance premiums. Other businesses (such as Mumsnet) have strengthened trust in their brands by proactively informing their customers about cyber security breaches and taking ownership of the issue.[42]

"Along with improving their protection, the public and businesses need to report these damaging crimes to Action Fraud. This allows the NCA, together with other law enforcement colleagues, to build a more informed picture of the threat so that we can work with the public and business to ensure that the UK remains the safest place to live and do business online."

Paul Hoare, National Prevent and Protect Coordinator, NCA

Reporting cyber breaches can result in lower insurance premiums and strengthened trust in brands for SMEs

When the General Data Protection Regulation comes into effect in May 2018, it will become increasingly important for businesses to report cyber breaches. This new regulation will institute harsher fines (up to 5% of global annual turnover or up to €20 million) for data security failings, with reporting of breaches being of core importance.

[38] Department for Culture, Media and Sport, Cyber Security Breaches Survey 2017, 2017
[39] Ibid
[40] BritainThinks, Cyber Streetwise Strategy Planning, 2016
[41] BritainThinks, Cyber Behaviours and Financial Fraud Messaging Research, 2017
[42] Justine Roberts, BritainThinks interview, 2017

Communicating that cyber crime is a 'real' crime with consequences for us all will help to mobilise action and greater personal ownership and responsibility when it comes to cyber security.

WHAT OPPORTUNITIES DO YOU HAVE TO:

- help ensure that your customers, employees, suppliers and clients feel and treat cyber crime as a 'real' crime?
- challenge the misconception that all financial loss from cyber crime will automatically be reimbursed?
  - Would greater clarity about when losses are and are not reimbursed encourage greater personal responsibility?
- increase understanding of the other knock-on effects of cyber crime amongst your customers, employees, suppliers and clients?
- encourage better reporting of cyber crimes?

03

MYTH: "THERE IS NOTHING MORE I CAN DO TO PROTECT MYSELF"

A plethora of cyber security advice and information can often leave the public and SMEs confused about where to start when it comes to protecting themselves and perpetuates the belief that action is only for technical experts. Collectively communicating consistent, simple, actionable protective cyber security actions is key to mobilising behavioural change.

KEY POINTS:

- There is a lack of clarity about what individuals need to do to be secure online.
- The public believe it is difficult to adopt even the most basic secure behaviours, and that anything beyond the basics is considered "impossible".
- Consumers and SMEs are leaving themselves and the organisations they buy from and work for vulnerable to attack.

BELIEF: "I don't know what I need to do to be secure online"

Recent qualitative research suggests that consumers and SMEs see conflicting advice about how to protect themselves online. This can result in them taking no action as they are unsure which advice is credible, or to assume protective behaviours that they have devised themselves, which often do nothing to improve their online security.[43] Furthermore they are of the view that if the experts can't agree then it's pointless them doing anything.

"There is just too much advice from different sources - and much of it is incorrect, too complex or too effortful. This is because much of it is made up in response to incidents, and untested. People are looking for concise, authoritative advice on key risks, and what protection is effective and worthwhile."

Professor Angela Sasse, Director of the UK Research Institute in Science of Cyber Security, University College London

[43] BritainThinks, Cyber Behaviours and Financial Fraud Messaging Research, 2017

Currently, advice on how to be secure online is inconsistent, with different pieces of guidance often contradicting one another

REALITY: Current advice is inconsistent

In this area the public perception matches the reality. Currently, advice on how to be secure online is inconsistent, with different pieces of guidance often contradicting one another. Alongside this, advice can often be difficult to put into practice due to differing requirements for different services.

CASE STUDY: Passwords

Advice on how to create a strong password is emblematic of this issue. Looking at just the first page of results on Google for the query 'How to create a strong password' brings up some of the following advice:

SOURCE	ADVICE
HOW-TO GEEK	• Use a password manager • Use a minimum of 12 characters • Use numbers, symbols, capitals and lower-case letters • Do not use dictionary words or a combination of dictionary words • Don't rely on obvious substitutions (e.g. 0 instead of O) • Create a mnemonic • Use four random words
GOOGLE SUPPORT	• Use a mix of letters, numbers, and symbols in your password • Don't use personal information or common words as your password
LIFEHACKER	• Take a sentence and turn it into a password • Use twelve random words • Use a 'person action object' password, e.g. Daniel eating gravel • Phonetic muscle memory method
THE GUARDIAN	• Create a mnemonic • Pick a number that means something to you but isn't so blatantly obvious, e.g. the latest unemployment figures • Use a nonsense word made up of several words
MICROSOFT SUPPORT	• Make the password at least 8 characters long • Don't contain your username, real name or company name • Don't contain a complete word • Contain uppercase letters, lowercase letters, numbers and symbols

This is compounded by inconsistent requirements for passwords when creating accounts on websites. Looking at just some of the largest websites these requirements can range from simply creating a password that 'Uses at least 6 characters' (Twitter and Amazon) to 'has at least 8 characters and contains at least two of the following: uppercase letters, lowercase letters, numbers and symbols' (Microsoft).

The inconsistency of both password advice and password requirements leads to confusion among both consumers and SMEs about what best practice is, with many choosing to take no action at all as a consequence.[44]

BELIEF: "Protecting myself from cyber crime is optional"

Although both consumers and SMEs report that there is a lack of clarity about what they need to do to be secure online, their uptake of the protective behaviours they do understand is often mixed, with many viewing them as 'optional'.[45] Significant proportions of the public fail to consistently follow the official government advice on how to remain secure online. For example, only 40% of individuals say that they always install the latest software or app updates once they notice that they are available.[46]

40%

Less than half (40%) of individuals say that they always or often download the latest software

Recent qualitative research suggests that individuals weigh the perceived level of protection a behaviour will give them against the perceived inconvenience of adopting that behaviour and often 'abandon' protective behaviours which they deem to be inconvenient.[47] Consumers and SMEs across all life stages consistently report times they had abandoned protective behaviours in order to make it easier for them to achieve something they wanted to online.[48]

Many businesses (particularly SMEs) tend to treat cyber security as a secondary concern and do not have processes in place to protect themselves from cyber crime. For example, just 7% of micro-firms, 14% of small firms and 24% of medium firms have incident management processes in place to deal with cyber security breaches. Even for large firms, only 45% have formal cyber security incident management processes in place.[49]

CASE STUDY: Stephanie*

Stephanie is in her early 30s and lives in the Midlands. Stephanie considers herself to be savvy and tech-literate, with a good knowledge of how to protect herself online.

"You have to have a strong password and make it different for every account.

[44] BritainThinks, Cyber Behaviours and Financial Fraud Research, 2017
[45] Ibid
[46] Ipsos Mori, Cyber Security Tracker, 2017
[47] BritainThinks, Cyber Behaviours and Financial Fraud Research, 2017.
[48] Ibid
[49] Department for Culture, Media and Sport, Cyber Security Breaches Survey 2017, 2017

7%

Just 7% of micro-firms have incident management processes in place to deal with cyber security breaches

Don't click on links in dodgy emails. Don't buy stuff from scam websites. It's pretty basic."

However, Stephanie often admits to ignoring her own advice when it is inconvenient.

"It's just a real pain having a different password for everything isn't it? I just use like variations on one password, like change the number or something... I have bought stuff from some pretty dodgy looking websites! You look and think, "this looks a bit funny, but it's 50% off...". If the deal is good enough then I'll risk it, you know?"

*Stephanie's name has been changed

REALITY: Cyber criminals can exploit even momentary lapses in protective behaviour

Cyber criminals are opportunistic and aim to take advantage of even momentary lapses in protective behaviour to target their victims

Much like offline criminals, cyber criminals are opportunistic and aim to take advantage of even momentary lapses in protective behaviour to target their victims. It is vital that individuals keep their software up to date and consistently practice secure behaviours online, in much the same way that it is important to always lock your door and close your windows when you leave your home.

"Small vulnerabilities in operating systems or lack of staff awareness can lead to criminals taking advantage of outdated software; for example through use of ransomware delivered through opening an attachment on an unsolicited email. For a large proportion of threats, cyber security doesn't need to be overly complicated and advice from the Government's National Cyber Security Centre, Cyber Essentials scheme and Cyber Aware campaign can be used to educate employees, improve systems and promote a business's cyber hygiene credentials."

Paul Hoare, National Prevent and Protect Coordinator, NCA

CASE STUDY: Reverse brute-force attacks

'Reverse brute-force attacks' are a common form of cyber attack which aim to take advantage of individuals' poor cyber security to access their accounts and data. Reverse brute-force attacks take a single common password, e.g. 'password123' and test it against multiple usernames or email addresses. Computer programs enable cyber criminals to do this to large numbers of accounts simultaneously, allowing them to gain access to multiple accounts.[50.]

Collectively and consistently communicating what individuals need to do to be secure online is key to driving behavioural action.

WHAT OPPORTUNITIES ARE THERE TO:

- clearly communicate to your customers, employees, clients and suppliers what they need to do to be secure online?
- make sure that advice is consistent across government and industry?
- communicate how to be secure online to your employees, customers and clients?
  - E.g. when creating accounts (customers), during training or induction (employees), etc.

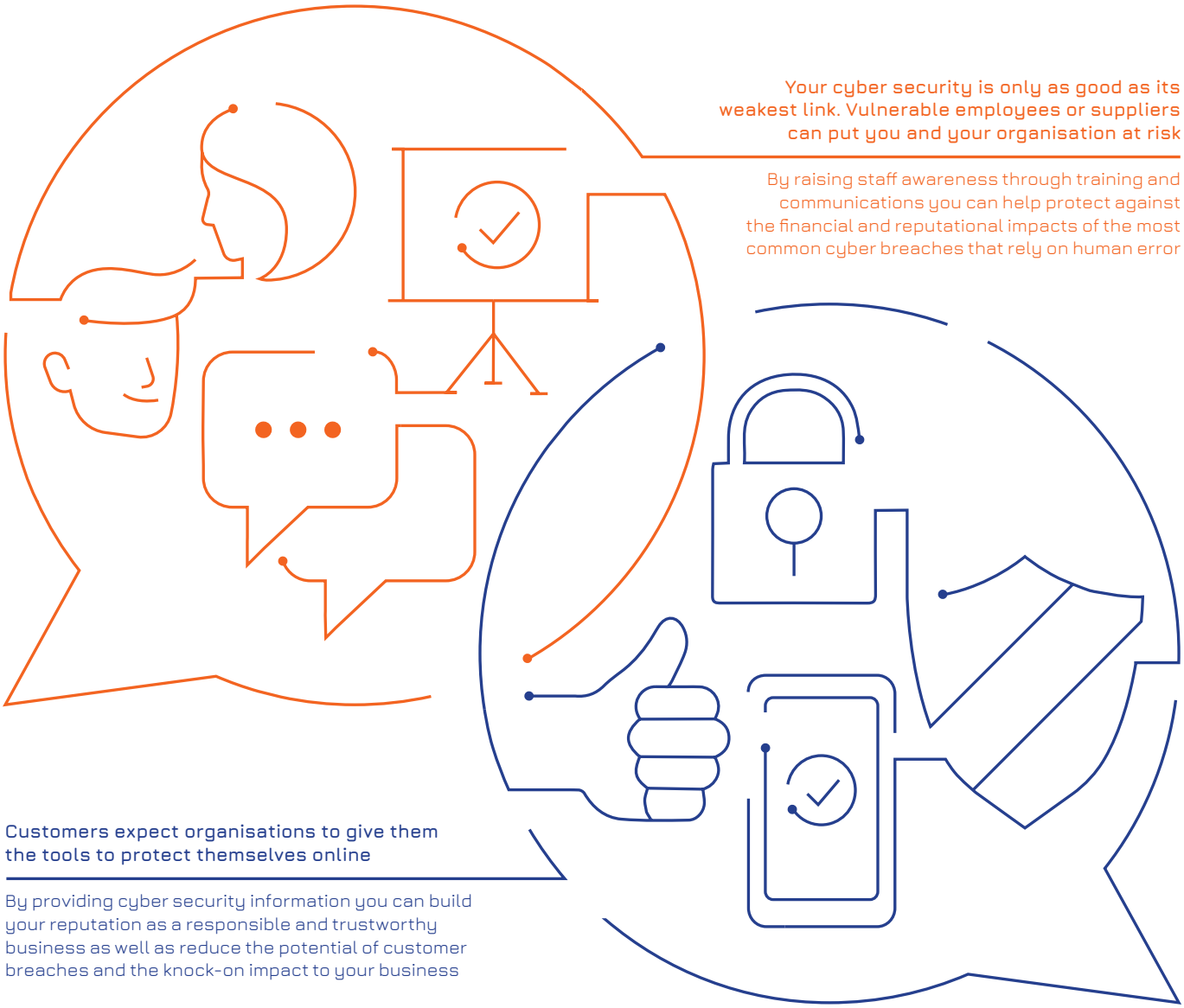
[50.] Computer Weekly, Techniques for preventing a brute force log-in attack, 2012, http://www.computerweekly.com/answer/Techniques-for-preventing-a-brute-force-login-attack

WHY DOES IT MATTER?

As a result of the perception gap, both consumers and SMEs are not taking cyber security seriously enough, leaving both themselves and other organisations at serious risk of falling victim to cyber crime.

- Individuals don't feel that cyber crime is something that they personally have to be concerned about, meaning that they are failing to take responsibility for their cyber security.
- Individuals aren't treating cyber crime as a 'real' crime, meaning they are failing to see the serious consequences of falling victim and failing to report incidents to the police, law enforcement and (in the case of businesses) their customers.
- Finally, they feel are doing all that they can to protect themselves online, despite treating cyber security as 'optional' and failing to put protective behaviours into practice.

WHAT DOES THE PERCEPTION GAP MEAN FOR YOUR ORGANISATION?



Your cyber security is only as good as its weakest link. Vulnerable employees or suppliers can put you and your organisation at risk

By raising staff awareness through training and communications you can help protect against the financial and reputational impacts of the most common cyber breaches that rely on human error

Customers expect organisations to give them the tools to protect themselves online

By providing cyber security information you can build your reputation as a responsible and trustworthy business as well as reduce the potential of customer breaches and the knock-on impact to your business

Cyber criminals are using these vulnerabilities to target both consumers and organisations. Individuals failing to fully or properly implement cyber security behaviours are a major vulnerability for organisations of all sizes. This is evidenced by a number of high profile cyber breaches in recent years, including the phishing attack on Snapchat and the Mirai malware attack that infected vulnerable devices and impacted organisations including Twitter and PayPal and the customers of TalkTalk and the Post Office.[51] [52] Attacks like these can happen to businesses of all sizes with 46% of all firms in the UK saying they had been the victim of a cyber breach in 2016. Whilst there is no systematic recording of the cause of all breaches, current figures indicate that human error plays a crucial role in a significant number. The most common breaches that organisations experience (fraudulent emails, viruses, spyware and malware, impersonation of an organisation in emails or online and ransomware) can be linked to human factors, such as unwittingly clicking on a malicious link or succumbing to impersonation.[53]

As the digital economy grows and organisations become even more linked, the impact of breaches on individuals and organisations will have an impact far wider than their immediate target.

The prevalence of these kinds of breaches is only likely to increase with the rise of 'bring your own device' (BYOD) and the remote working culture. As increasing numbers of employees bring their own devices to work, the separation between 'work' and 'personal' cyber security is likely to become increasingly irrelevant, meaning that it is even more important to ensure employees are cyber secure both at work and at home. It is vital that good cyber security becomes a habit, in much the same way that locking your doors when you leave your home is.

"There's been a big move over the last maybe year and a half, two years, to 'BYOD' - Bring Your Own Device to work - where perhaps you go into a work environment and there's a bit of an archaic PC or laptop you're given and more than likely your own smart phone is better than what you're given, so you tend to want to be able to use your own devices at work. So there is a blurring of the work environment and personal devices because people want to be able to work as and when they're comfortable or time allows"

Shaab Al Baghdadi, Principal Privacy Practitioner, Online DPO

Alongside this, large-scale password re-use attacks (where hackers take log-in details gained from cyber breaches of one website and use them to try and hack into other accounts) against customers of large organisations (including Camelot and Deliveroo) has led to negative press coverage of those organisations.[54] This clearly demonstrates that the threat of cyber crime to organisations is wider than simply when their own systems are compromised. If your customers' security is compromised, this can have an impact on your businesses systems and reputation.

[51] Tech Crunch, Snapchat Employee Data Leaks Out Following Phishing Attack, 2016, https://techcrunch.com/2016/02/29/snapchat-employee-data-leaks-out-following-phishing-attack/
[52] National Cyber Security Centre, The cyber threat to UK business, 2017
[53] Department for Culture, Media and Sport, Cyber Security Breaches Survey 2017, 2017
[54] BBC, National Lottery accounts feared hacked, 2016 http://www.bbc.co.uk/news/technology-38155710

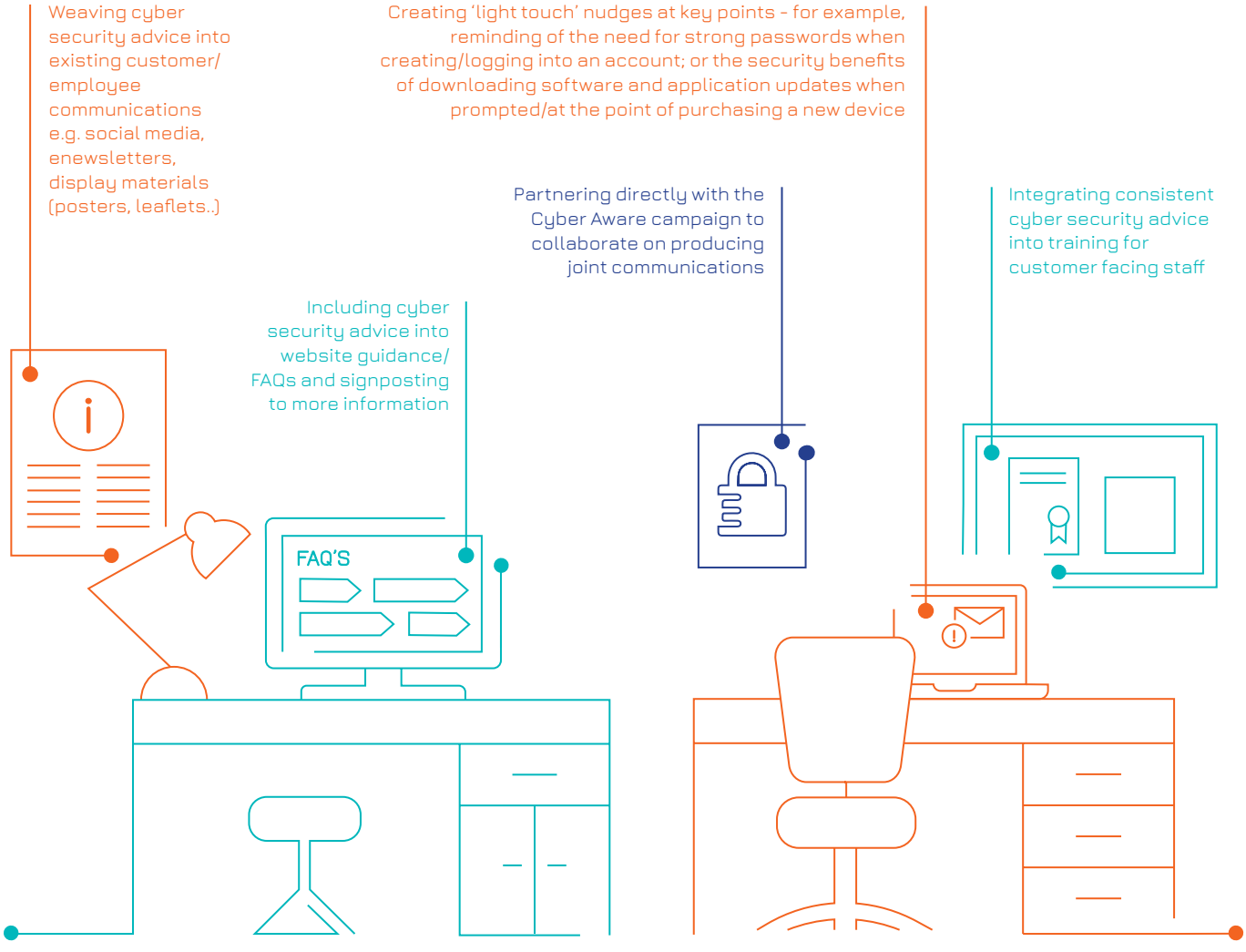
WHAT NEEDS TO BE DONE?

Cyber crime is one of the biggest threats to us all. It is crucially important that we take action now to strengthen our cyber security by closing the perception gap.

To achieve this, it is vital that both the government and businesses work together to deliver consistent information to the public. Businesses like yours can ensure that there is clear advice about what individuals need to do by building consistent cyber security messaging and 'nudges' into your business as usual processes, as well as mutually reinforcing advice via industry networks and collaboration with media.

Crucially, **individuals expect to receive information from businesses like yours about how to be safe online and evidence shows that seeing this messaging contributes to perceptions of trust and reputation.**[55.56.] This expectation and responsibility is only likely to increase as we move into an increasingly digital world.

HOW YOU CAN HELP TO CLOSE THE PERCEPTION GAP:



[55.] BritainThinks, Qualitative Tracking Research, 2017
[56.] Ipsos Mori, Cyber Security Tracker, 2017

All organisations like yours are in a unique place to take action and to take the lead on this important issue as employers, trusted brands, suppliers and clients. Doing this at key points (e.g. when a customer is creating an account, activating a product, purchasing something online or accessing a service) is particularly valuable as these are the moments when individuals are most likely to be receptive to messaging on cyber security.[57]

Organisations like yours can take action ranging from light touch to full integration into customer journeys. Activity can also be woven in to existing communications to customers across both online and offline channels.

noddle

CASE STUDY: Noddle

Noddle, the free-for-life credit reporting service, is one of Cyber Aware's committed private sector partners. Since working together, the collaboration has focused on extending the core protective messages of the campaign to a wider consumer audience. Activity has included cyber security advice articles on the Noddle blog and in their newsletter reaching millions of people per send, content across social media platforms in support of campaign peaks such as #quickupdates, as well as being an integral member of the Cyber Aware Expert Forum. Noddle and Cyber Aware have also worked on a joint PR story, which saw coverage in The Mirror and on Press Association.

"We're a proud partner of Cyber Aware as there is a real synergy between the guidance and support we provide to our customers, and the aims of the campaign. It's important to us that consumers understand how to protect themselves online, and we've been able to amplify these messages through our Cyber Aware partnership work. We're pleased to be planning more exciting activity for the coming months."

– Jacqueline Dewey, Managing Director, Callcredit Consumer

[57] BritainThinks, Qualitative Tracking Research, 2017

CASE STUDY: Currys PC World Business

Currys PC World Business is one of Cyber Aware's dedicated retail partners. Over the last 12 months, our collaboration has focused on increasing the reach of Cyber Aware's core protective messages. Activity has comprised of spokesperson opportunities in the national media, a bespoke cyber security information page on the Currys PC World Business Advice Hub, native advertising, and e-newsletter editorial sent to over 500,000 small businesses. The Dixons Carphone team understands that their customers are seeking information and advice for cyber security messages. The behaviours promoted by working with Cyber Aware have helped Dixons Carphone live its brand values.

"We're delighted to be partnering with Cyber Aware, we speak to businesses everyday who highlight security as being a priority for their business. Working with Cyber Aware allows us to educate our customers with relevant information and empower them with the latest guidance."

– Frances Sue, Senior Marketing Manager
Currys PC World Business is a part of Dixons Carphone Group

CASE STUDY: Law Enforcement

The October #ThinkRandom campaign was the most successful peak of activity in the 2016/17 period and showed the power of coordinated Police support for Cyber Aware across all media channels. The majority of Police Forces (29/43) supported the October activity on social media, which trended in the UK on that day. The top tweets of the campaign peak came from the Metropolitan and Greater Manchester Police. Four out of the six top authors by followers were Police Forces, with a combined audience reach of 1.3 million. 16 regional media pieces were successfully secured and through coordination with cyber leads in ROCUs (Regional Organised Crime Units) 12 local force quotes were added into tailored regional press releases.

One of the highlights of the #ThinkRandom activity was the 47 regional radio slots fronted by the then NPCC cyber crime Protect Co-ordinator, Detective Inspector Danny Lawrence. He spoke confidently about Cyber Aware's 'three random word' message for passwords.

Police involvement in this campaign showed the real power that could be harnessed by forces across the country delivering consistent advice through their own channels. Their trusted spokespeople and channels delivered real cut through to key audiences.

As well as the work of the National Cyber Security Centre and business specific initiatives such as Cyber Essentials and 10 Steps to Cyber Security, the government is currently encouraging individuals and businesses to take some simple steps to improve their cyber security as part of its Cyber Aware campaign. These include:

Use a strong, separate password for your email account.

A good way to create a strong and memorable password is to use three random words or numbers, which are memorable to you, but not easy for other people to guess

Install the latest software and app updates.

They contain vital security updates which help protect your device from viruses and hackers

Secure your tablet or smartphone with a screen lock

Always back-up your most important data

Don't use public Wi-Fi to transfer sensitive information such as card details

Don't 'jailbreak' or 'root' your smartphone

Beware of fake websites

Never click on suspicious links or attachments

"The National Cyber Security Centre works closely with Cyber Aware to provide the ongoing technical expertise on which the campaign is based. As such, the advice delivered through the campaign takes into account the evolving cyber security risks to both individuals and SMEs and suggests appropriate measures to counter a range of threats. By following Cyber Aware guidance and adopting these simple and secure online behaviours individuals and businesses can proactively protect themselves from cyber criminals."

The National Cyber Security Centre

By all working together, whether we're Government, business, or the third sector, we can drive a behaviour change in Britain, creating a culture where it's as normal to protect ourselves on line as it is in our homes. By doing this we can all help build our nation's cyber resilience. Join this movement today for direct updates and support from Government on how we can protect Britain from cyber crime by contacting cyberaware@homeoffice.x.gsi.gov.uk

The National Cyber Security Centre is the UK's authority on cyber security and is a part of GCHQ. It was set up to help protect the UK's critical services from cyber attacks, manage major incidents, and improve the underlying security of the UK internet through technological improvement and advice to citizens and organisations. Visit www.ncsc.gov.uk for more information and advice, and use the NCSC Small Business Guide (www.ncsc.gov.uk/smallbusiness) for more advice to small businesses.

METHODOLOGY

APPENDIX 1: ABOUT THIS REPORT

This report is designed to be the first step towards being more proactive in collating and sharing insights on cyber security and cyber crime from across Government and a range of other credible and authoritative sources. As well as aiding partnership working, this approach of bringing together a range of data sources to identify a coherent narrative on public and business attitudes towards cyber security and cyber crime is designed to address the need for clear and consistent communications across the private and public sector on these topics. This report was compiled through a process of desk research on public attitudes towards cyber crime and cyber security, and drafted between September 2016 and February 2018. The report was produced for RICU in the Home Office by BritainThinks in collaboration with Home Office Analysis and Insight.

APPENDIX 2: METHODOLOGICAL NOTE ON BRITAINTHINKS PRIMARY RESEARCH

Throughout the report, three pieces of primary research conducted by BritainThinks are referenced, the 'Cyber Streetwise Strategy Planning' research from 2016, the 'Cyber Behaviours and Financial Fraud Research' from 2017 and the 'Qualitative Tracking Research' from 2017. These projects were qualitative in nature and, as with qualitative work in general, findings cannot be generalised to a wider population. Across these projects BritainThinks used a combination of focus group discussions and online communities. Online communities are closed qualitative research forums, where respondents can participate in moderated group discussions and complete individual activities using text, photo and video responses.

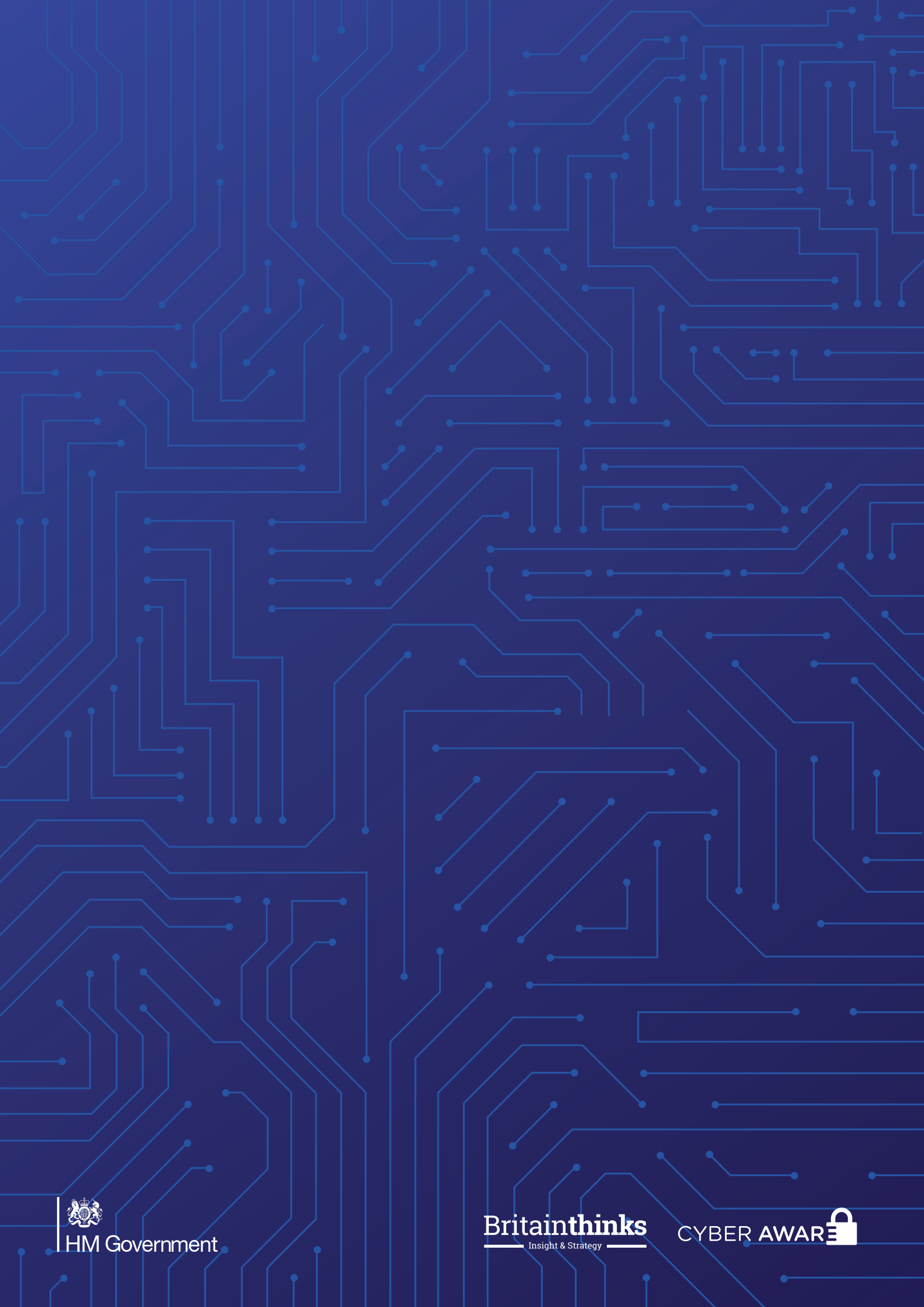
During the Cyber Streetwise Strategy Planning BritainThinks conducted 6 focus groups (with 6-8 participants in each) with consumers and SME owners, and follow-up online community with reconvened participants.

During the Cyber Behaviours and Financial Fraud Research BritainThinks conducted 18 focus groups (with 6-8 participants in each) with consumers and senior decision makers in SMEs and a follow-up online community with reconvened participants.

During the Cyber Aware Qualitative Tracking Research BritainThinks conducted 12 focus groups (with 6-8 participants in each) with consumers and SME owners, conducted across September and December 2017.

APPENDIX 3: METHODOLOGICAL NOTE ON IPSOS MORI PRIMARY RESEARCH

Throughout the report, two pieces of primary research conducted by Ipsos MORI are referenced, the 'Cyber Streetwise Pre-Campaign Tracker' from 2015 and the 'Cyber Security Tracker' from 2017. Both reference an ongoing regular non-random online panel survey (approximately 2,000 consumer and 1,000 SME responses during most recent fieldwork), designed to measure the adoption of safer cyber security behaviours. Findings relate to self-reported behaviours which may be influenced by a range of factors.


HM Government
Britainthinks
Insight & Strategy
CYBER AWAR