Department for Science, Innovation & Technology

Cyber Essentials Scheme Impact Evaluation

Final Report

July 2024

Pye Tait Consulting
info@pyetait.com
www.pyetait.com

Certificate Number 10745

Contents

List of Figures

List of Tables

Acknowledgements

The Department for Science, Innovation and Technology (DSIT), along with Pye Tait Consulting, gratefully acknowledge the contributions of all organisations and individuals who helped to make this impact evaluation possible. This includes representatives from IASME, NCSC, other government and industry stakeholders, as well as current, lapsed and non-users of Cyber Essentials that took part in the research.

Executive Summary

Background

Cyber Essentials was developed to help protect organisations of any size against the most common internet-originating cyber attacks. This includes attacks carried out by individuals who may or may not have limited technical expertise, using tools and techniques readily available on the internet.

There are two levels of Cyber Essentials certification:

- **Cyber Essentials:** the basic, verified self-assessment option. The scheme is centred around five technical control areas designed to significantly reduce the impact of common cyber attacks.

- **Cyber Essentials Plus:** This takes the same approach and is based on the same five technical control areas, with the addition of independent testing and sampling of the organisation's infrastructure to verify compliance. If successful, this results in the award of a certificate valid for one year, i.e. certification is renewed annually.

Prior to commissioning this impact evaluation, DSIT commissioned Pye Tait Consulting to conduct a Cyber Essentials scheme process evaluation. The study examined the scheme's implementation effectiveness, including organisations' motivations to becoming certified, views on the scheme's information and guidance, experience of the journey to becoming certified, and ease of adopting the technical controls.

The process evaluation provided a glimpse of the scheme's ability to make a positive difference to the cyber security behaviours of Cyber Essentials users in different ways. For instance, it was largely perceived as affordable, easily attainable, cost-effective, accessible, and offering a good baseline for security. As part of the process evaluation, a feasibility study was carried out to inform a more detailed evaluation of the scheme's impact on users (process evaluation, Appendix 1).

Evaluation aims

In July 2023, DSIT commissioned Pye Tait Consulting to undertake the Cyber Essentials scheme impact evaluation, comprising the following objectives:

1. Assess whether the Cyber Essentials scheme has had a positive impact on increasing the cyber resilience of the UK economy.

2. Evaluate whether there are common positive impacts or negative consequences for organisations which do or do not gain certification.

3. Identify the extent to which Cyber Essentials is providing value for money and is an effective use of resources.

4. Provide evidence-based recommendations for maximising the effectiveness of Cyber Essentials.

Methodology

A combination of data collection methodologies were used, as follows:

- Development of an evaluation logic model and framework
- Review of existing evidence sources pertaining to Cyber Essentials' impact
- Primary research among current and lapsed Cyber Essentials users*, involving a survey (606 responses), 33 follow-up in-depth qualitative interviews, and three case studies of certified organisations
- A comparison survey of organisations that had never obtained Cyber Essentials (516 responses)

*Note that the terms 'Cyber Essentials users' or 'scheme users' throughout this report refer to organisations with current or lapsed Cyber Essentials certification – used for brevity.

The evaluation encompassed all types and sizes of organisations, including those classified into government, academia, private sector, Non-Governmental Organisations (NGOs), registered charities and a minority of 'other' groups (see Appendix 2, Table A2.3 for further details).

Key findings

Effectiveness of the technical controls

- An evaluation by Such et al (2015) provides evidence as to the efficacy of Cyber Essentials, with 99% of internet-originating vulnerabilities mitigated using the technical controls and none mitigated without them.
- Most Cyber Essentials users surveyed for this impact evaluation (82%) are confident that the technical controls provide protection against common cyber threats, while a similar proportion (80%) believe they are helping to mitigate cyber security risks within their organisation.
- Whilst scheme users think it highly likely that they would have implemented the technical controls even if they had not become certified, these organisations may be more predisposed to being cyber secure, while possible overconfidence bias could be at play.
- For more than half (53%) of Cyber Essentials users, the scheme appears to be providing the only form of external assurance for their cyber security. Furthermore, among organisations that had never obtained Cyber Essentials, almost three quarters (72%) are not using any other security schemes, standards and principles. This provides an indication that these organisations may be less cyber security risk aware or lacking external validation of their protocols and controls.

Relationship between Cyber Essentials and cyber risk awareness

- Almost two thirds (64%) of Cyber Essentials users agree that being certified through the scheme better enables their organisation to identify where they experience a common, unsophisticated cyber attack.

- Surveyed Cyber Essentials users rate their level of concern about potentially falling victim to a cyber attack at 5.8 out of 10 – significantly higher than organisations that had never obtained certification (3.7 out of 10). This points to greater risk awareness among users, fuelling a heightened sense of concern about the potential threats around them.

- With respect to the consequences of a possible cyber attack, Cyber Essentials users rate the perceived significance of impact on their organisation more highly than organisations that had never obtained Cyber Essentials in terms of the reputational, financial and legal effects. This suggests that the combination of being better informed and more concerned means that users are more appreciative of the potential impact of an attack for their organisation.

Influence of Cyber Essentials on understanding of cyber risks and confidence on cyber security posture

- Most Cyber Essentials users (85%) believe that the scheme has directly improved their understanding of cyber security risks, while an even greater proportion (88%) believe that the scheme has directly improved their understanding of the steps they can take to reducing those risks.

- Cyber Essentials users were asked whether the scheme has directly strengthened their senior management's understanding of the risks posed by cyber attacks, with most (86%) saying that it has. This builds on analysis undertaken as part of the Cyber Security Breaches Survey 2023 which found that Boards of Cyber Essentials certified organisations are more likely to say that they prioritised cyber security (93%).

- Most Cyber Essentials users (91%) say that the scheme has directly improved their confidence at being able to consistently implement steps to reduce cyber security risks. They generally say they are keeping on top of Cyber Essentials scheme requirements regularly through established internal processes, which is helping to boost their confidence further. Most scheme users (91%) also believe that Cyber Essentials has directly improved their confidence in being protected in the event of such an attack.

- Corroborating these findings, strategic stakeholders (comprising government representatives and key industry organisations) are broadly of the view that Cyber Essentials can help to support organisations starting their cyber security journey, build confidence in their cyber security posture and offer peace of mind. This is considered especially the case among smaller organisations that are less likely to have dedicated IT expertise.

- An important overarching observation is that the comparison survey of organisations that had never obtained Cyber Essentials reveals similarly high levels of perceived understanding and confidence in cyber security matters to that of scheme users. This points to a likely overconfidence bias. This is further justified from qualitative insights among scheme users that becoming Cyber Essentials certified opened their eyes to prior cyber security weaknesses and gaps which the technical controls have helped to plug.

- As a result of having a better understanding of cyber security risks and the extent to which this could be a pervasive problem, organisations may be more cautious and feel compelled to do more to boost their organisations' cyber resilience (explored further in chapter 6).

Stimulating wider cyber security practices

- Approximately three quarters of Cyber Essentials users (76%) report having taken additional preventative actions beyond the Cyber Essentials technical controls, with qualitative insights pointing to the scheme having a role in catalysing wider operational and behavioural change. This aligns with findings from Britain Thinks that Cyber Essentials users are more likely than organisations that had never obtained Cyber Essentials to take further steps to improve their cyber security.

- Examples of actions taken by surveyed Cyber Essentials users include attaining ISO 27001; putting in place additional software, standards, training, internal controls and review processes; undertaking penetration testing and investing in infrastructure change.

- Almost three quarters (71%) of surveyed Cyber Essentials users agree that the scheme has directly strengthened how seriously their organisation takes cyber security. In particular, they say it has prompted a more serious attitude and approach to cyber security internally, for example stimulating more regular and open conversations on cyber security protocols and why they are important.

- Cyber Essentials users also report adopting new cyber security policies and procedures, carrying out additional risk assessments to ensure their defences stay up to date, and thinking regularly about how to improve their cyber security posture.

- Additionally, Cyber Essentials is useful in guiding some organisations that had never obtained certification, with a small minority (13%) having drawn upon its published guidance to strengthen their own security.

- Among 53 surveyed organisations certified to ISO 27001 but not Cyber Essentials more than four in ten (42%) say that their organisation currently only meets some of the Cyber Essentials technical controls. This suggests that the technical controls could provide valuable protection to organisations that use other schemes, standards and accreditations.

Strengthening assurance mechanisms

- The single main reason (mentioned by 35% of surveyed Cyber Essentials users) for first becoming certified is that the scheme was mandated in government contracts. The commercial imperative for obtaining certification is also strong, with users reporting that a third (33%) of all contracts they entered into over the preceding 12 months required them to be Cyber Essentials certified.

- Some 15% of Cyber Essentials users have made it mandatory for their suppliers to become Cyber Essentials certified and plan to continue doing so, while a further third (33%) are actively considering mandating Cyber Essentials in the future. This points to the scheme's potential value in strengthening organisational resilience through supply chains.

- Just under half of Cyber Essentials users (45%) take Cyber Essentials into account when assessing the cyber risk that a supplier poses to them, signalling that the technical controls appear to be acting as a benchmark as part of supply chain assurance.

- There is evidence that Cyber Essentials is overcoming the information asymmetry around cyber security; furthermore, that the scheme is now making organisations able to consider cyber security as part of their purchasing decisions. For example, the majority of Cyber Essentials users (61%) say they are more likely to choose suppliers that are Cyber Essentials certified than those without certification, while three quarters (75%) say they have greater confidence working with certified suppliers.

- Among organisations that had never held Cyber Essentials, almost a quarter (23%) say they are also more likely to choose suppliers that hold Cyber Essentials, and 25% have greater confidence working with such suppliers. These findings point to the scheme being valuable for supply chain cyber security protection, even among organisations that do not directly use the scheme themselves for whatever reason.

- Most Cyber Essentials users (79%) believe that the scheme has a positive impact on the confidence of their own clients and customers. A fifth (20%) of organisations that had never obtained Cyber Essentials are of the same view, which suggests that some of their clients would ideally like to see evidence of certification.

- Just under half of Cyber Essentials users (48%) report saving time on cyber security due diligence where a potential supplier is CE certified, rising to 59% where a potential supplier is CE Plus certified. This time can then be used by organisations in other ways. (It is important to note here that there are currently fewer CE Plus certifications compared to standard CE certifications).

- Thinking about surveyed organisations as suppliers of goods and services, more than three quarters (76%) report that being Cyber Essentials certified helps to reduce the due diligence burden placed upon them, potentially therefore resulting in time or resource savings. They note that it gives their clients peace of mind and acts as a stamp of approval that they are taking cyber security seriously.

- A small minority of Cyber Essentials users (8%) say they have noticed a reduction in cyber incidents since using Cyber Essentials to manage supply chain cyber risk, but most (57%) feel that is too difficult to gauge.

Creating wider value

- The Cyber Essentials scheme is encouraging strong growth in the cyber security sector, with increasing numbers of Certification Bodies and assessors. This means a stronger external support network for cyber security should organisations need it for information or advice.

- Ten of the 33 Cyber Essentials users interviewed following the survey mentioned that their Certification Body provides useful guidance and advice on a regular basis, going beyond their role as an intermediary. Some said they are good at answering any pressing questions, are always contactable, and produce helpful reports.

- The NCSC's 2023 Annual Review suggests that 80% fewer cyber insurance claims are made when Cyber Essentials is in place when compared with organisations that have the same insurance policy and do not have Cyber Essentials certification (based on 2022 claims data).

- Cyber Essentials users rate the value of the packaged cyber liability insurance with a score of 6.6 out of 10 (mode = 10), indicating that the insurance is considered moderately valuable. It is important to note that ratings could be inversely affected here where organisations have not experienced a cyber attack and thus not had to make use of the insurance. Reported benefits of the bundled insurance include having dedicated cyber security protection, the fact this comes at no extra cost, and that the insurance covers most types of cyber threats.

- Finally, more than two thirds of Cyber Essentials users (69%) believe that Cyber Essentials has increased their market competitiveness. This includes certification being perceived as "achievable" which makes the cost-benefits clearer to see, gaining additional credibility since their organisation is taken more seriously, and experiencing increased commercial activity since becoming certified.

Value for money

The points below summarise the evidence already identified in terms of how Cyber Essentials demonstrates value for money for organisations that use it, as well as for government.

- Whilst arguably a subjective measure, Cyber Essentials offers peace of mind against the potential reputational, financial and legal consequence of a cyber attack. In particular, most scheme users (80%) identify a commercial benefit that being certified can reduce the financial cost to their organisation of a common, unsophisticated cyber attack.

- Cyber Essentials evidently yields further commercial benefits considering that a third (33%) of contracts that Cyber Essentials users entered into over the preceding 12 months required them to be certified through the scheme and more than two thirds (69%) believe the scheme has increased their market competitiveness.

- Most surveyed Cyber Essentials users (82%) expressed confidence that the technical controls are positively impacting their level of protection against common cyber threats, while 80% are confident that the technical controls help to mitigate cyber security risks within their organisation.

- Cyber Essentials is evidently leading to more embedded and sustainable approaches to cyber security risk management, along with streamlined cyber security due diligence. Growth of the scheme itself is being helped by a rising trend in certifications, use of the technical controls by organisations that have never obtained Cyber Essentials, and supply chain assurance mechanisms.

- As evidenced by the Cyber Essentials scheme process evaluation, the scheme as intended is open and accessible to organisations of all types and sizes and its technical controls are providing baseline protection to organisations ranging from the smallest taking their first steps in their cyber security journey, to large organisations seeking to plug gaps in their existing cyber security risk management protocols.

- The scheme has directly contributed to the growth of the cyber security sector, with a network of over 340 Certification Bodies and over 900 assessors.

- In terms of value for government, the running of the Cyber Essentials scheme incurs minimal costs for the government for the impact it achieves. From the statistics above, it works to address the information asymmetry present in this market, in two ways:

    1. **Understanding what cyber security controls to put in place:** By the government including achievable controls that stop up to 99% of internet-originating vulnerabilities (Such et al (2015)) organisations can focus their time on implementation and other productive activities rather than deciding on what to implement.

    2. **Understanding cyber security when making investment and consumption decisions:** It has now allowed cyber security to be considered in purchasing decisions with 61% saying they are more likely to pick a supplier that uses Cyber Essentials

Conclusions

The evaluation’s conclusions are summarised below. Further details can be found in section 11.1.

1. Cyber Essentials is providing cyber security protection to organisations of all sizes, including larger organisations that use other schemes, standards and accreditations.

2. Cyber Essentials helps to improve organisations’ awareness and understanding of the cyber security risk environment – thus enabling them to become more informed – and helps to boost scheme users’ confidence at mitigating the risks of a possible cyber attack.

3. Cyber Essentials has stimulated wider actions, good practice and behaviours among organisations that use it, potentially born out of a heightened appreciation of the cyber security risk environment.

4. Cyber Essentials is being actively used as part of supply chain assurance to inform the supplier selection process, instil confidence and demonstrate basic cyber hygiene to the market.

5. Cyber Essentials is streamlining due diligence for some organisations and their supply chains, but this is not always the case.

6. Cyber Essentials is contributing to wider value, through growth in the cyber security sector, peace of mind through the bundled cyber liability insurance, and stronger market competitiveness.

Recommendations

The evaluation's recommendations are summarised below. Further details can be found in section 11.2.

1. Continue to promote Cyber Essentials as an affordable and responsive cyber security solution aimed at organisations that may otherwise lack basic protection.

2. Continue to invest in the scheme's supportive approach to helping organisations gain and sustain certification, by growing the supportive network of Certification Bodies and assessors.

3. Stimulate wider and more effective use of Cyber Essentials as a supply chain assurance tool.

4. Help clients to identify how they could improve the efficiency of cyber security due diligence processes where their suppliers are Cyber Essentials certified.

5. Encourage more organisations to prioritise cyber security by conveying more tailored information about the benefits of being Cyber Essentials certified to different sizes and types of organisation.

6. Consider providing more basic information to organisations that have never been certified to help them better understand the Cyber Essentials scheme and why it would be a good investment.

7. Continue to work with insurance providers to convey the latest evidence on the effectiveness of the Cyber Essentials technical controls and how the scheme contributes to organisational cyber resilience.

8. Consider rolling out more targeted and high-profile marketing and communications stressing the potential hard-hitting consequences of a cyber attack.

1. Introduction

This chapter sets the scene for the evaluation by summarising the importance of building cyber resilience in the UK economy, contextual information about the Cyber Essentials scheme, and the objectives for this impact evaluation.

1.1 Strengthening UK cyber resilience

The world is now more connected than ever before, with technology driving extraordinary opportunity, innovation and progress. However, the pace of change and a growing market for cyber capabilities, also gives rise to additional complexity and risk.

As noted in the National Cyber Security Centre's (NCSC) 2023 White Paper Ransomware, extortion and the cyber crime ecosystem, UK businesses and institutions are a high value target for cyber criminals seeking money, information and the potential to cause widespread disruption. As the threat landscape continues to evolve, coupled with an increase in ransomware, criminals no longer need an advanced knowledge of computing to access software that will do much of the hard work for them.

The White Paper describes how cyber attacks can affect every aspect of an organisation's operation, hitting finances, compromising customer data, disrupting operational delivery, eroding trust and damaging reputations. The government's National Cyber Strategy (NCS) 2022 made similar observations, for example that cyber attacks can lead to intellectual property theft, psychological distress, disruption to services and assets and damage to￼.

In its Annual Review 2023, the NCSC warned that the UK needs to accelerate work to keep pace with the changing threat, particularly in relation to enhancing cyber resilience. The government's Department for Science, Innovation and Technology (DSIT) defines cyber resilience as the ability for organisations to prepare for, respond to and recover from cyber attacks.

The government's National Cyber Strategy 2022 already sets out ambitious policies to protect the UK in cyberspace. Under Pillar 2 of the Strategy – building a resilient and prosperous digital UK – the government has set the following objectives to 2025:

1. Improve the understanding of cyber risk to drive more effective action on cyber security and resilience

2. Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations and providing greater protection to citizens

3. Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks

As part of this effort, the government aims to continue promoting take-up of accreditations and standards such as the Cyber Essentials certification scheme. Through such schemes, it aims to make the UK the safest place in the world to be online and the best place in the world to start and grow a digital business.

1.2 About Cyber Essentials

Scheme characteristics

Cyber Essentials was developed to help protect organisations of any size against the most common internet-originating cyber attacks. This includes attacks carried out by individuals who may or may not have limited technical expertise, using tools and techniques readily available on the internet. The NCSC describes these types of attacks as “the digital equivalent of a thief trying your front door to see if it’s unlocked.”

It is important to note that Cyber Essentials does not offer a one-stop solution to protecting organisations against all cyber security risks. For example, it does not address more advanced, targeted attacks, hence organisations facing these threats should consider additional measures as part of a cyber security strategy. The NCSC has produced guidance on risk management to help organisations better understand and manage the cyber security risks affecting their organisation.

The Cyber Essentials scheme has three main functions:

1. To help organisations put in place fundamental technical controls that increase their resilience and build their confidence in their security posture

2. To enable organisations to manage third-party cyber security risks, receiving assurance from suppliers and partners that they have implemented core technical controls effectively

3. To provide a tool for organisations to give assurance of basic cyber hygiene to the market (consumers, customers, suppliers and other business partners)

The government’s Procurement Policy Note 09/14 introduced a mandatory requirement for Cyber Essentials certification for organisations working on UK central government contracts that meet certain criteria, notably where this involves handling personal information and providing certain ICT products and services. As discussed in section 7.1 of this evaluation report, this approach has been a key driver of organisations becoming Cyber Essentials certified.

There are two levels of Cyber Essentials certification:

1. **Cyber Essentials:** The basic, verified self-assessment option. The scheme is centred around five technical control areas designed to significantly reduce the impact of common cyber attacks.

   Steps to certification typically involve working with either the IASME Consortium Ltd. (responsible for delivering the scheme) or one of more than 340 Certification Bodies to apply for an online assessment account, pay the relevant certification fee, complete the online assessment (signed off at board level) and supply supporting documents for review. If successful, this results in the award of a certificate valid for one year, i.e. certification is renewed annually.

2. **Cyber Essentials Plus:** This takes the same approach and is based on the same five technical control areas, with the addition of independent testing and sampling of the organisation's infrastructure to verify compliance.

The five technical control areas are:

1. **Firewall configuration:** To make sure that only secure and necessary network services can be accessed from the internet

2. **Secure configuration**: To ensure that computers and network devices are properly configured to i) reduce vulnerabilities; and ii) provide only the services required to fulfil their role

3. **User access control:** To ensure that user accounts i) are assigned to authorised individuals only; and ii) provide access to only those applications, computers and networks the user needs to carry out their role

4. **Malware protection:** To restrict execution of known malware and untrusted software from causing damage or accessing data

5. **Security update management:** To ensure that devices and software are not vulnerable to known security issues for which fixes are available.

The technical controls are reviewed on a 12-month rolling basis and ensure that the Cyber Essentials scheme continues to help UK organisations guard against the most common cyber threats.

Throughout this report, the term Cyber Essentials is used to refer to the overall scheme (including both levels mentioned above) and the separate terms CE and CE Plus are used when referring to a particular level.

Governance and delivery

Cyber Essentials is operated in partnership between DSIT and the NCSC. It is delivered through IASME. The scheme launched on 5th June 2014 and, from April 2020, IASME became the NCSC's sole Cyber Essentials partner responsible for the management and delivery of the scheme. Prior to that, it was delivered by five separate Accreditation Bodies, which included IASME.

IASME has accredited over 340 Certification Bodies, which are companies responsible for delivering the Cyber Essentials scheme through being trained and licensed to certify organisations. These companies comprise over 900 individual assessors who also have a role to provide information and guidance to the organisations they work with in the interests of encouraging better cyber security and reaching the scheme's baseline standard.

Scheme growth

The government wishes to increase the number of organisations holding Cyber Essentials.

Certification has been growing steadily over the years, principally driven through being mandated in UK government contracts as evidenced by the Cyber Essentials scheme process evaluation. IASME internal trend data show growth increasing from 500 certifications per month in January 2017 to more than 3,500 in February 2024.

Based on the same internal data (correct as of February 2024), a total of 31,294 unique organisations were Cyber Essentials certified in the preceding 12 months. This includes all types of organisations, for example government, academia, the private sector, Non-Governmental Organisations (NGOs), registered charities etc. The figure includes new certifications and annual re-certifications of existing certified organisations. Of these, 9,905 organisations had also attained CE Plus, making 41,199 total certifications awarded over the same period (CE Plus certifications are counted additionally to CE).

IASME data for the financial year 2022-23 show that micro and small organisations make up more than two thirds (69%) of CE certifications (Table 1). This can be reasonably explained by the fact micro and small organisations make up the vast majority of UK enterprises, including those within government contract supply chains. The scheme has certified just under a third (31%) of the UK's large organisations.

Table 1 Cyber Essentials certification – share and penetration by size-band

Employment size-band	% mix of CE certifications	% mix of CE Plus certifications	% of UK private sector businesses certified
Micro (fewer than 10 staff)	35%	33%	0.2%
Small (10-49 staff)	34%	28%	3.8%
Medium (50-249 staff)	20%	22%	12.6%
Large (250+ staff)	11%	17%	30.8%

Source: IASME (April 2023) Cyber Essentials Scheme Annual Review

Based on data from IASME's Cyber Essentials Scheme Annual Review (April 2023), the types of organisations and sectors seeing strongest uptake include the public sector, followed by charities, critical national infrastructure (CNI) organisations, construction, consultancies, education, healthcare, insurance and legal. The top three industry sectors accounting for the largest proportion of Cyber Essentials certifications are IT (12%), finance (10%) and consultancy (7%).

1.3 Evaluation background and objectives

Preceding process evaluation

Prior to commissioning this impact evaluation, DSIT commissioned Pye Tait Consulting to conduct a Cyber Essentials scheme process evaluation. The study examined the scheme's implementation effectiveness, notably:

- Organisations' motivations to becoming certified
- Views on the scheme's information and guidance

- An understanding of organisations' journeys to becoming certified
- Ease of adopting the technical controls

The process evaluation provided a glimpse of the scheme's ability to make a positive difference to the cyber security behaviours of Cyber Essentials users in different ways. For instance, the scheme was largely perceived as affordable, easily attainable, cost-effective, accessible, and offering a good baseline for security. However, the most reported reasons for organisations becoming Cyber Essentials certified were largely reactive (e.g. to meet contractual or customer requirements) rather than proactive (e.g. to improve their own cyber resilience). As part of the process evaluation, a feasibility study was carried out to inform a more detailed evaluation of the scheme's impact on users (process evaluation, Appendix 1).

Impact evaluation objectives

In July 2023, DSIT commissioned Pye Tait Consulting to undertake the Cyber Essentials scheme impact evaluation, comprising the following objectives:

1. Assess whether the Cyber Essentials scheme has had a positive impact on building the cyber resilience of the UK economy.

   This divides into the following areas:

   (i) Helping organisations to increase their security levels and build their confidence in their security posture.

   (ii) Providing organisations with a tool to manage third-party cyber security risks, receive assurance from suppliers and partners that they have implemented core technical controls effectively, and streamline due diligence processes

   (iii) Giving assurance of basic cyber hygiene to the market (customers and other business partners)

2. Evaluate whether there are common positive impacts or negative consequences for organisations which do or do not gain certification

3. Identify the extent to which Cyber Essentials is providing value for money and is an effective use of resources

4. Provide evidence-based recommendations for maximising the effectiveness of Cyber Essentials

2. Methodology

This chapter explains how the evaluation was designed, including the rationale for the approach taken. It explains the data collection tools, sampling approaches, margins of error and use of weighting, followed by important notes relating to how the findings are presented throughout this report and notes of caution.

2.1 Evaluation design

An impact evaluation of the Cyber Essentials was deemed eminently feasible in principle given the length of time the scheme has been running. Furthermore, three years have elapsed since the last major structural change to delivery, positioning IASME as the sole Accreditation Body in April 2020. This time factor is important since it allows outcomes and more lasting impact to have been felt.

The evaluation was designed in accordance with the HM Treasury Green Book and Magenta Book, tailored to the specific context and nature of the scheme. The aim was to enable the government to reflect, in a structured and logical way, on the difference the scheme has made, and be capable of articulating a baseline along with desired outcomes and impact.

The starting point was the development of an evaluation feasibility study, set out in the preceding Cyber Essentials scheme process evaluation (Appendix 1).

At the outset of this impact evaluation, a theory of change was developed using a logic model approach. This defined:

- Scheme objectives
- Scheme inputs/processes
- Anticipated outputs (immediate/more tangible)
- Anticipated outcomes (short to medium term/less tangible)
- Anticipated impacts (longer term/less tangible)

Based on this, an evaluation framework was developed, setting out:

- A statement of the problem and what Cyber Essentials needs to achieve
- Scheme outcomes mapped to a suite of individual evaluation measures
- Data collection methods and target audiences appropriate to achieving each measure
- Timeframe for each stage of the data collection

It should be noted that a theory of change and logic framework had already been developed for Cyber Essentials, as part of a collaborative effort between (former) DCMS, IASME and NCSC. This was reviewed, refined and expanded upon as part of this impact evaluation.

The logic model and evaluation framework for the Cyber Essentials scheme impact evaluation are available as a separate MS Excel Annex to this report.

To assess the impact of the Cyber Essentials scheme, notably the difference it has made, it was important to form a counterfactual. This effectively meant comparing observed outcomes to those that would have been expected if the Cyber Essentials scheme had not been implemented. There were several possible approaches to achieving this:

1. **Establishing a comparison group** – to compare quantitative and qualitative data between Cyber Essentials users and organisations that had never obtained certification.

2. **Establishing a baseline counterfactual –** for example, gathering data from organisations prior to them becoming Cyber Essentials certified and revisiting these organisations after becoming Cyber Essentials-certified (this would ideally involve waiting at least 12 months, and ideally longer, for impact to be felt).

3. **Constructing a quasi-experimental approach, involving developing a logically constructed counterfactual –** for example, using baseline statistics and perspectives to develop a reasonable estimate of what would have happened without Cyber Essentials having been implemented.

Option 1 was selected as the most suitable in this case, given that i) it allowed an impact evaluation to be conducted in a relatively short timescale; and ii) the Cyber Essentials scheme has already been running for many years.

Establishing contribution and attribution

Determining complete causality is extremely difficult through evaluation logic models since other factors (confounding variables) can contribute to observable outcomes and be difficult to separate. One example might be determining the extent to which certain outcomes materialise as a direct result of Cyber Essentials certification, rather than as a result of other accreditations, schemes or standards.

An additional challenge associated with assessing the impact of Cyber Essentials relates to attempting to quantify the difference the technical controls have made to the number and frequency of successful cyber attacks. This is because cyber attacks may be infrequent or may never have previously been experienced by an organisation. Furthermore, organisations may be reluctant to disclose details of a cyber attack and there is a risk therefore that breach data could go under-reported. This evaluation therefore uses other measures to examine impact. In doing so, through carefully worded questioning as part of the primary research, it has attempted to attribute observable outcomes to Cyber Essentials as far as reasonably possible.

2.2 Data collection methods

A combination of data collection methodologies were used, as follows:

- Review of existing evidence sources as they relate to Cyber Essentials impact
- Primary research among current and lapsed Cyber Essentials users involving a survey, follow-up in-depth qualitative interviews and case studies
- A comparison survey of organisations that had never obtained Cyber Essentials

The evaluation encompassed all types and sizes of organisations, including those classified as government, academia, private sector, Non-Governmental Organisations (NGOs), registered charities and 'other' groups.

The evaluation components and timings are shown in Table 2. This is followed by further details about survey sampling, delivery, margins of error and weighting.

Table 2 Evaluation components

Component	Details	Dates
Development of the evaluation logic model and accompanying framework	To theorise how Cyber Essentials contributes to a chain of expected outputs, outcomes and wider impact; as well as the mechanisms used by the evaluation to gather and assess evidence	August 2023
Rapid desk research	To assess prior evidence of scheme outcomes and impact in line with the theory of change	August 2023
Stakeholder scoping interviews	Conducted with nine representatives from government and key industry organisations (UK, including devolved nations)	August – September 2023
Survey of current and lapsed users of Cyber Essentials	Online survey 606 total responses (including 532 current users and 74 lapsed users)	02 October – 06 December 2023
Comparison survey of organisations that had never obtained Cyber Essentials	Computer-Assisted Telephone Interviewing (CATI) and online surveying 516 responses (including 491 CATI and 25 online)	02 October – 06 December 2023
Follow-up in-depth interviews with a sample of Cyber Essentials users	33 completed interviews with a mix of organisation types and sizes to explore Cyber Essentials impact in more detail. Consent to	November – December 2023

	re-contact was obtained via the preceding survey	
Three impact case studies	Attributable case studies to showcase success and potentially transferable good practice from different types and sizes of organisation, developed through additional conversations with earlier interviewees	December 2023 – January 2024

2.3 Survey sampling, margins of error and weighting

Survey of current and lapsed users of Cyber Essentials

To maximise the potential response rate for this survey, Pye Tait Consulting shared the online survey link with IASME, which in turn shared it with all 340+ Certification Bodies for onward email distribution to Cyber Essentials users they had each assessed. It was also distributed by IASME to a further sample of Cyber Essentials users for which IASME held contact details and consent to take part in market research. Additionally, devolved nation government representatives were asked to promote the survey and it was further promoted through the Cyber Essentials newsletter, Cyber Exchange and via government social media channels.

Due to the protracted approach to distributing the online survey link to Cyber Essentials users, the total number of organisations invited to take part through Certification Bodies is not known. This prohibits a response rate being accurately calculated for these audiences.

This survey did not impose hard quotas due to the importance of maximising responses and not wanting to be restrictive.

Tables 3 and 4 show the proportional spread of survey responses by employment size-band and nation, respectively. As expected, the achieved spreads are closely aligned to IASME's population data for certified organisations.

Table 3 Achieved survey responses and IASME population data – Cyber Essentials users (by size band)

	Achieved survey responses (current and lapsed users)		**Cyber Essentials certified organisations (as of April 2023, IASME)**	
Micro (<10 staff)	191	32%	8,916	35%
Small (10-49 staff)	187	31%	8,662	34%
Medium (50-249 staff)	129	21%	5,095	20%
Large (250+ staff)	99	16%	2,802	11%
Totals	**606**	**100%**	**25,475**	**100%**

Source of IASME data: Cyber Essentials Scheme Annual Review (April 2023)

Table 4 Achieved survey responses and IASME population data – Cyber Essentials users (by nation)

	Achieved survey responses (current and lapsed users)		**Cyber Essentials certified organisations (as of April 2023, IASME)**	
England	522	86%	21,764	88%
Scotland	36	6%	1,470	6%
Wales	29	5%	997	4%
Northern Ireland	13	2%	270	1%
Crown Dependencies	6	1%	132	1%
Totals	**606**	**100%**	**25,475**	**100%**

*A further 842 certificates are recorded as 'rest of the world/unknown'
Source of IASME data: Cyber Essentials Scheme Annual Review (April 2023)

Based on a total count of 31,294 Cyber Essentials certified organisations (as of February 2024), the achieved total of 532 survey responses from current Cyber Essentials users (excluding lapsed users) yields an overall margin of error of ±4.2% at the 95% confidence level. This means that, had the survey been repeated, 95 times out of 100 the results would be true for the population of certified organisations give or take 4.2%.

It should be noted that margins of error are inevitably higher for questions not answered by all respondents and where cross-tabulations of the results are performed, for example by employment size-band.

Breakdowns of the margin of error are not provided by type of organisation since the achieved proportions for certain organisation types are very small and analysis by organisation type is not included within this report.

An overall margin of error has not been calculated for lapsed Cyber Essentials users since the corresponding population is not certain and the number of survey responses from this cohort is also small (74 responses).

Survey of organisations that had never obtained Cyber Essentials

The CATI component of this survey (target of 500 responses) involved stratified random sampling based on employment size-band and nation. Representative quotas were initially established and then manually adjusted to over-sample small, medium and large organisations, as well as the devolved nations. Over-sampling was important otherwise very low survey numbers would have been achieved from a purely representative sample.

Devolved nation government representatives were asked to promote an online variant of this survey and it was further promoted through the Cyber Essentials newsletter, Cyber Exchange and via government social media channels.

Tables 5 and 6 show the proportional mix of survey responses by employment size-band and nation, respectively. As a result of the adjusted sampling, the proportion of surveyed organisations turned out to be reasonably close to the proportion of Cyber Essentials users based on IASME data.

Table 5 Achieved survey responses and population data – organisations that had never obtained certification (by size band)

	Achieved survey responses		National population of organisations		IASME data
Micro (<10 staff)	201	39%	5,364,525	95%	35%
Small (10-49 staff)	158	31%	238,185	4%	34%
Medium (50-249 staff)	101	20%	42,405	1%	20%
Large (250+ staff)	56	11%	10,895	<1%	11%
Totals	**516**	**100%**	**5,656,010**	**100%**	**100%**

Source of population data: Department for Business and Trade, Business Population Estimates 2023

Table 6 Achieved survey responses and population data – organisations that had never obtained certification (by nation)

	Achieved survey responses		National population of organisations		IASME data
England	383	74%	4,915,780	87%	88%
Scotland	54	10%	298,255	5%	6%
Wales	50	10%	218,995	4%	4%
Northern Ireland	28	5%	122,095	2%	1%
Crown Dependencies	1	0%	76,000	1%	1%
Totals	**516**	**100%**	**5,631,125**	**100%**	**100%**

Source of population data: Department for Business and Trade, Business Population Estimates 2023

This survey sought a reasonable spread of responses by Standard Industrial Classification (SIC) code at four-digit level.

The sample was drawn from Moody's FAME database.

For the CATI component of this survey, a total of 8,845 organisations were contacted by phone to achieve 491 CATI responses – a response rate of 6%. The most common reasons for some organisations not taking part were as follows:

- Outsourcing IT arrangements and not feeling sufficiently confident talking about cyber security
- Reluctance to discuss any aspect of their cyber security with a third party
- Organisational policy to not take part in surveys
- Not returning messages or requests to find the most appropriate person to speak to
- Already being a current or lapsed Cyber Essentials user (therefore outside the scope of this survey)

Based on 5.6 million organisations in the UK economy, a total of 516 survey responses from organisations that had never obtained Cyber Essentials yields an overall margin of error of ±4.3% at the 95% confidence level.

Weighting

Weighting of survey results aims to adjust achieved proportions (for example by size band or nation) to be representative of the wider population from which the sample was drawn.

Weighting was not deemed necessary for the survey of current and lapsed Cyber Essentials users as the achieved proportions by size-band and nation very closely reflect the population of certified organisations based on IASME data (Tables 3 and 4, above). As such, weighting would make very little statistical difference. It is also important to note that the cost of weighting data is reduced accuracy, since the sampling variance, standard deviation and standard error increase. This makes it important to weight selectively.

For the survey of organisations that had never obtained Cyber Essentials, weighting was performed for the main reason of simulating the proportions achieved from the survey of current and lapsed users. This decision was taken given that the main purpose of the two surveys together is that of comparison.

Weighting was achieved using the Random Iterative Method (RIM). This involves adjusting multiple characteristics in a dataset simultaneously using an algorithm that distorts each variable as little as possible. In this case, RIM weights were created and applied with respect to employment size-band and nation.

Notes of caution

The two surveys of: i) current and lapsed Cyber Essentials users; and ii) organisations that had never obtained Cyber Essentials, both encompassed the same broad types and sectors of organisations, as well as organisations spanning the four UK nations and all employment size-bands (see Appendix 2 – Survey Respondent Profile). However, possible instances of bias may be at play for the reasons set out below.

The survey of current and lapsed Cyber Essentials users was non-random due to the approach described above of the online survey link being distributed via IASME and the 340+ Certification Bodies. The approach taken is justified on the grounds of practicality and maximising response rates given the lack of commercial contact lists specifically identifying Cyber Essentials certified organisations. Furthermore, the resulting respondent profile is broadly representative of the population of current and lapsed users by size-band and nation, as noted in the sub-section ‘Weighting’, above. However, there remains a risk of sampling bias that is important to note, given that not all Certification Bodies may have distributed the online survey link to organisations they had assessed. This means that not all current and lapsed Cyber Essentials users necessarily had an equal chance of being directly invited to take part.

Additionally, it was not possible within the constraints of the evaluation to undertake detailed data matching to identify the nature and extent of similarities or differences between the two survey groups, which might lead to further possible instances of bias.

With respect to the survey of organisations that had never obtained Cyber Essentials certification, and especially perceptual questions relating to aspects of understanding and confidence, there may be an element of overestimation bias or overconfidence bias at play. This is a tendency to estimate one’s judgment or performance as better than reality, especially where it has not been put to the test or where complacency may be a factor. This type of bias is difficult to quantify accurately since it can vary considerably based on a wide range of factors. As such, responses from organisations that had never obtained Cyber Essentials certification should be treated with a degree of caution.

2.4 Presentation of findings in this report

This report presents the impact evaluation findings by theme, interweaving the results of survey research with evidence from secondary resources, strategic stakeholder interviews (comprising representatives from government and key industry organisations), and follow-up depth interview insights with a sample of current and lapsed Cyber Essentials users.

Chapters 3 to 8 present the survey results using charts, followed by narrative descriptions and analysis. Certain charts are supplemented by tables showing breakdowns by size-band.

Some questions were asked of all respondents and some only of a subset of respondents. Base numbers responding to each question are shown as part of each chart. These appear either in the X axis (for all respondents) or adjacent to the Y axis labels for particular subsets (usually shown in brackets).

Most survey results show cross-tabulations by employment size-band. This was agreed given that size is a critical variable affecting attitudes and behaviours relating to Cyber Essentials certification, as determined by the preceding process evaluation. Size-bands are defined as follows:

- Micro (fewer than 10 staff)
- Small (10-49 staff)
- Medium (50-249 staff)
- Large (250+ staff)

This report does not present analysis by geography. This is because the survey response numbers for Cyber Essentials users based specifically in Wales, Northern Ireland and the Crown Dependencies are considered too small (i.e. below 30) to permit meaningful analysis.

With respect to organisations that had never obtained Cyber Essentials, the survey results in this report are based on the weighted dataset.

Statistical significance testing has been carried out on certain questions to assess whether there are meaningful differences in the distribution of results per size-band. This applies to both survey groups, i.e. Cyber Essentials users, as well as organisations that had never obtained Cyber Essentials certification.

Additionally, and only for directly comparable questions, statistical significance tests have been carried out to compare the results of Cyber Essentials users with the comparison group of organisations that had never obtained Cyber Essentials.

Statistical tests were performed based on the unweighted dataset of Cyber Essentials users and the unweighted dataset of organisations that had never obtained Cyber Essentials. The term ‘significant’ is only used within this report to denote statistically significant differences.

3. Effectiveness of the Cyber Essentials Technical Controls

This chapter begins by summarising the findings from an existing technical assessment of the performance of the Cyber Essentials technical controls. It then presents survey evidence from this evaluation regarding Cyber Essentials users' confidence in the impact of the controls and the likely extent to which they would have been implemented had organisations never become Cyber Essentials certified.

Key findings summary

Existing research points to the efficacy of the Cyber Essentials technical controls, with almost all internet-originating vulnerabilities mitigated using the controls and none mitigated without them. There is strong confidence among surveyed Cyber Essentials users that the technical controls provide protection against common cyber threats, and that they are helping to mitigate cyber security risks within their organisations.

For most Cyber Essentials users, the scheme appears to be providing the only form of external assurance for their cyber security. Among surveyed organisations that had never obtained Cyber Essentials, most are not using any other security schemes, standards and principles. This suggests that these organisations could be less cyber security risk aware or that they lack external validation of their existing protocols.

3.1 Efficacy of the technical controls

Existing research points to the Cyber Essentials technical controls being effective at mitigating internet-originating vulnerabilities. This points to organisations that adopt the technical controls being better protected.

Research by Such et al (2015) – Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials involved analysing 200 internet-originating vulnerabilities. Of these, it was observed that 99% were mitigated using Cyber Essentials technical controls, but none were mitigated without them.

Research by Such et al (2019) – Basic Cyber Hygiene: Does it work? observed that among 20 small and medium sized enterprises (SMEs) surveyed across four sectors, 137 vulnerabilities applied to at least one SME, 69% were mitigated using the Cyber Essentials technical controls, 29% were partially mitigated, and 1.5% were not mitigated.

These positive impacts clearly stand to benefit not only Cyber Essentials users, but those that have adopted the technical controls without actually attaining the certification (be it due to conscious choice or lacking awareness of the scheme).

As further evidence of this, the Cyber Security Breaches Survey 2023 found that a fifth (20%) of total surveyed businesses reported adhering to the Cyber Essentials technical controls in all five areas – considerably higher among medium businesses (42%) and large businesses (61%). These proportions clearly go far beyond current levels of certification, pointing to the scheme's potential reach.

It is important to point out that whether organisations are Cyber Essentials certified, or adhering to all of the technical controls without being certified, they could be demonstrating equal cyber resilience. However, where they are not certified and not subject to repeat annual assessment, this could reduce the propensity of consistently adhering to the technical controls. Furthermore, this could contribute to overconfidence bias among organisations that had never obtained Cyber Essentials in relation to their cyber security posture. This issue is explored further below and later throughout this report.

Further insights into use of the scheme (including its information and standards) by organisations that had never obtained Cyber Essentials can be found in section 6.2.

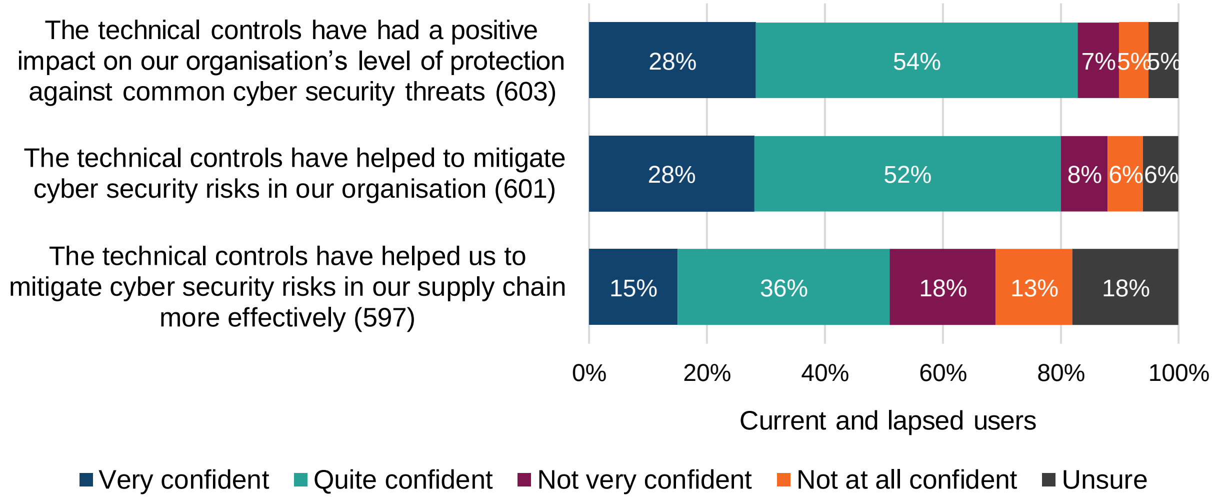
Confidence in the impact of the Cyber Essentials technical controls

Evidence points to strong perceived confidence among organisations that the technical controls are providing protection against common internet-based cyber threats.

Findings from research by Britain Thinks reveal that – among organisations that had never obtained Cyber Essentials certification but had duly implemented all of the technical controls, 85% felt well-protected, compared with 67% that had not implemented the controls. The same study also found that three in four surveyed Cyber Essentials users (75%) considered the scheme to have had a positive impact on their level of protection.

Cyber Essentials users surveyed for this evaluation were asked how confident they are that the technical controls are having an impact in three specific ways (Figure 1).

Figure 1 Confidence in the impact of the Cyber Essentials technical controls (current and lapsed users)



Most surveyed organisations (82%) are confident that the technical controls have had a positive impact on their level of protection again common cyber threats; 80% are confident that they help to mitigate cyber security risks within their organisation; and just over half (51%) are confident that they help to mitigate risks in the supply chain more effectively. Supply chain risk assurance is explored in more detail in chapter 7.

Breakdowns of the above chart by size-band are shown in Table 7. With respect to statements A and B, the proportion of small, medium and large organisations stating very or quite confident is significantly higher than micro organisations. This may be where larger organisations already have greater concerns about falling victim to a successful cyber attack (section 4.2) and for whom the perceived consequences are more significant (section 4.3).

Table 7 Confidence in the impact of the Cyber Essentials technical controls (current and lapsed users by size-band)

STATEMENT A: The technical controls have had a positive impact on our organisation's level of protection against common cyber security threats

	All (603)	Micro (< 10 staff) (190)	Small (10-49 staff) (186)	Medium (50-249 staff) (129)	Large (250+ staff) (98)
Very confident	28%	26%	31%	25%	33%
Quite confident	54%	48%	54%	64%	52%
Not very confident	7%	10%	5%	6%	9%
Not at all confident	5%	9%	5%	2%	3%
Unsure	5%	7%	5%	4%	3%

STATEMENT B: The technical controls have helped to mitigate cyber security risks in our organisation

	All (601)	Micro (< 10 staff) (190)	Small (10-49 staff) (186)	Medium (50-249 staff) (128)	Large (250+ staff) (97)
Very confident	28%	23%	34%	27%	27%
Quite confident	52%	48%	50%	57%	54%
Not very confident	8%	9%	6%	9%	10%
Not at all confident	6%	10%	4%	2%	7%
Unsure	6%	10%	6%	5%	2%

STATEMENT C: The technical controls have helped us to mitigate cyber security risks in our supply chain more effectively

	All (597)	Micro (< 10 staff) (187)	Small (10-49 staff) (183)	Medium (50-249 staff) (129)	Large (250+ staff) (98)
Very confident	15%	13%	19%	12%	13%
Quite confident	36%	33%	36%	36%	40%
Not very confident	18%	17%	14%	24%	22%
Not at all confident	13%	18%	13%	9%	12%
Unsure	18%	19%	19%	19%	12%

How the technical controls are mitigating cyber security risks

Most Cyber Essentials users interviewed following the survey believe that the technical controls are helping them to mitigate cyber security risks more effectively as follows:

- Fuelling continual, proactive monitoring and management of security procedures and policies

- Encouraging more regular cyber security checks, such as malware and firewall testing
- Enabling a more structured approach to looking at potential risks
- Streamlining decision-making processes
- Encouraging improved training in cyber security practices
- Saving time on cyber security tasks through greater automation of systems and processes, such as software updating

"When we get a patch reminder, we are given a seven-day turnaround or Windows will update it for us, but we've set our own standard to fix any patches within two days."

Non-governmental Organisation, micro employer

"Before, where we had to seek permission or have additional meetings before undertaking certain cyber security actions, it's now a case of saying 'this is what's happening because that is what the criteria says'."

Registered charity, medium employer

"We had 500-600 machines that were in their end-of-life stage, and we knew that because of Cyber Essentials drawing our attention to it. There wouldn't have been anyone keeping an eye on it unless we had Cyber Essentials. It would have been a case of they'll get updates when they get updates."

Private business, large employer

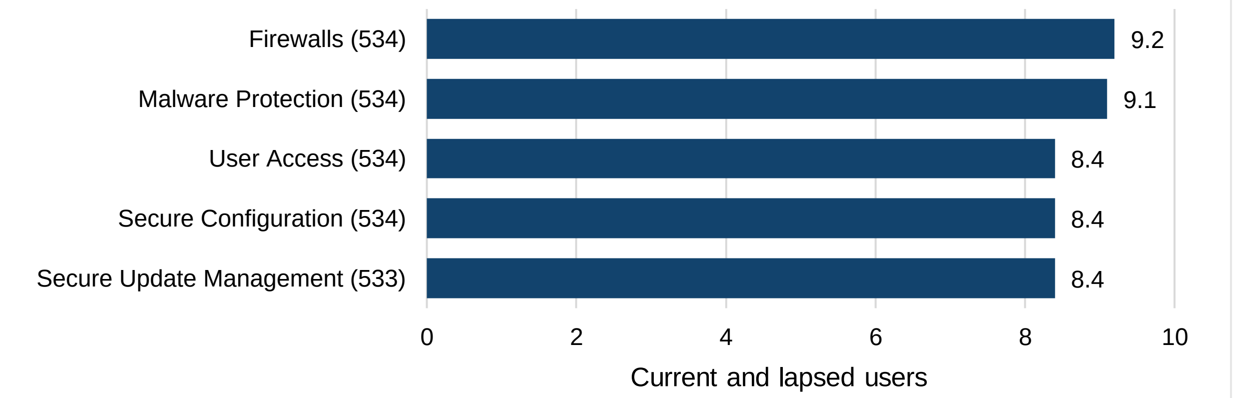
Those organisations **not confident** that the technical controls are helping to mitigate cyber security risks within their own organisations or supply chains were asked for their reasons. The main points are summarised below, which may point to a misunderstanding of the scope of Cyber Essentials:

- Perceived gaps in the technical controls, for example one organisation mentioned that the controls do not cover how to wipe a particular device in the event of a data breach (although this would be post-incident and beyond the scope of Cyber Essentials which focuses on preventative controls)
- ISO 27001 is seen as demonstrating a more "sophisticated security posture" (although this assumes it is scoped correctly for the organisation in question)

3.2 Likely implementation if never previously certified

Surveyed Cyber Essentials users were asked the extent to which their organisation would likely have implemented all of the procedures and protocols associated with each of the scheme's five technical control areas had they never become certified (Figure 2). Ratings are on a scale from 1 (not at all) to 10 (the full extent).

Figure 2 Extent to which technical controls would still have been implemented if never certified (current and lapsed users)



At first glance, the mean ratings are clearly high for each of the five technical control areas, ranging from 8.4 to 9.2 out of 10. For all five groups, the modal answer is 10 out of 10 and the median either 9 or 10 out of 10. The full range of ratings were received (between 1 and 10) for each of the five groups.

However, it is important to note that there could be several reasons for these high ratings. Firstly, Cyber Essentials users may have been more predisposed to being cyber secure prior to becoming certified, possibly with greater knowledge or confidence in matters of cyber security. Secondly, there may be some overestimation bias at play whereby organisations assume it is something they would have naturally done even though that might not always have been the case. Furthermore, it is also worth noting that not all organisations would have necessarily implemented all five of the technical control areas.

Qualitative questioning established that the certification process can add value to organisations that are already cyber security conscious by validating current practices, maintaining their cyber security mindset, and helping them over the line to certification by addressing pockets of weakness.

> "Cyber Essentials is a good base level cyber security standard that aims to do the right things and validate that we have a good baseline level of cyber security in place."
>
> **Private business, small employer**

> "We already had suitable high-level security in place prior to Cyber Essentials, but the certification process has made us more aware of upgrades and certain issues where we could have been weak."

Private business, small employer

These ideas are explored further in section 5.1 in terms of how Cyber Essentials has boosted organisations' understanding of cyber security risks and steps to reducing them.

Cross-tabulations of the above chart by size-band are shown in Table 8, although there are no significant differences.

Table 8 Extent to which technical controls would still have been implemented if never certified (current and lapsed users by size-band)

	All (534)	**Micro (< 10 staff) (165)**	**Small (10-49 staff) (169)**	**Medium (50-249 staff) (110)**	**Large (250+ staff) (90)**
Firewalls (534)	9.2	9.2	9.2	9.2	9.4
Secure configuration (534)	8.4	8.3	8.2	8.5	8.7
User access (534)	8.4	8.5	8.2	8.4	8.6
Malware protection (534)	9.1	8.9	9	9.2	9.4
Security update management (533)	8.4	8.7	8.3	8.5	8.2

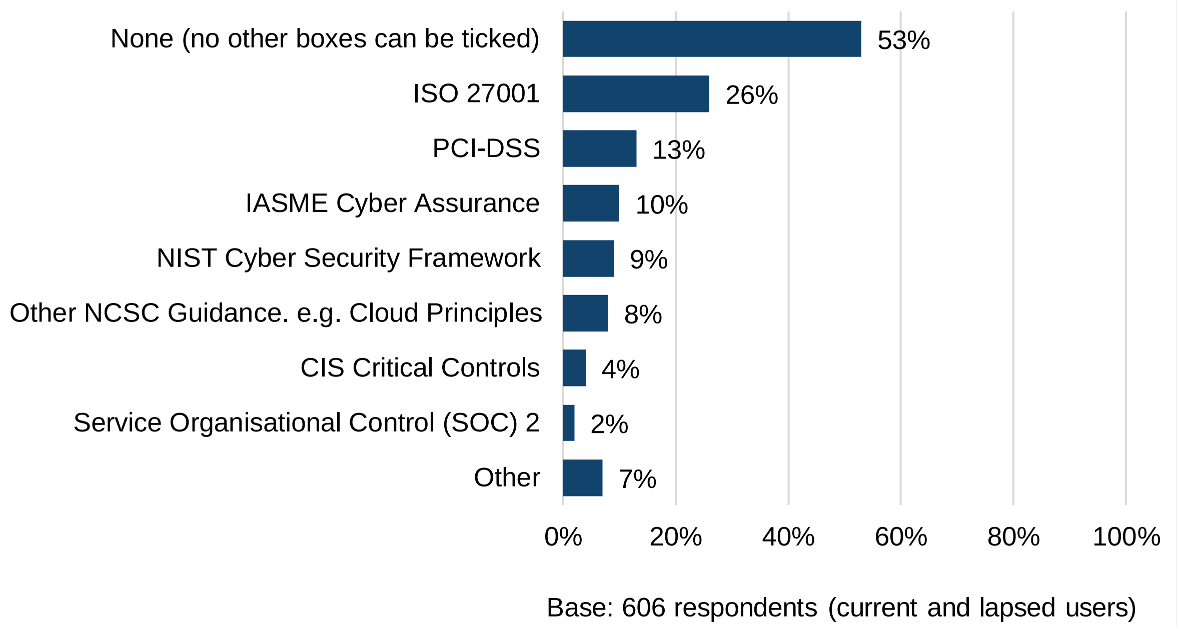
3.3 Use of any other cyber security schemes, standards and principles

All surveyed organisations were asked which, from a list of other specific cyber security schemes, standards and principles, they currently use (Figure 3). Breakdowns by size band are shown in Table 9.

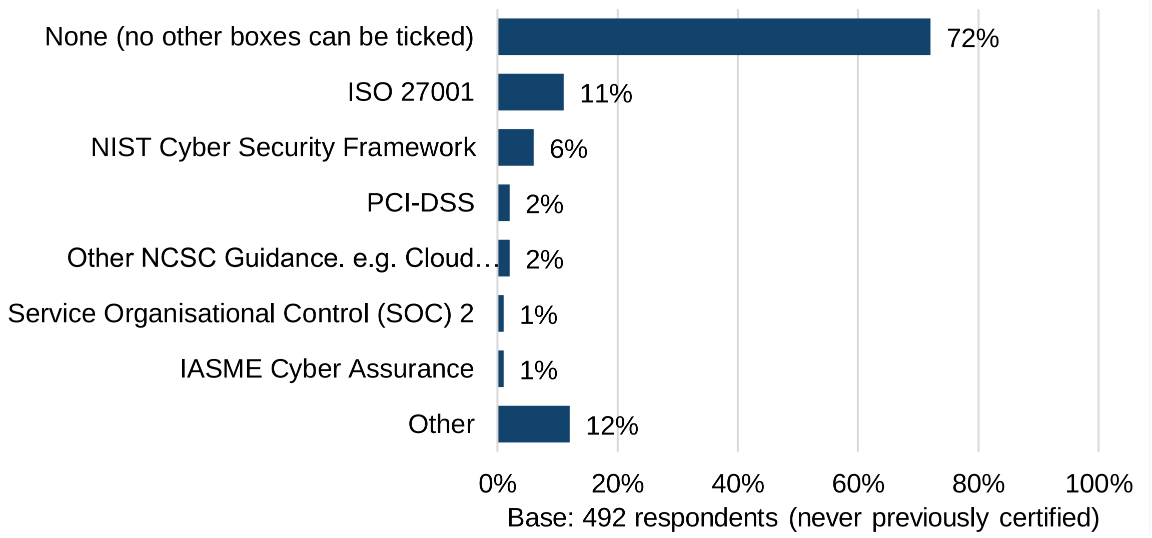
The results offer an early indication of the potential scale of cyber risk awareness among Cyber Essentials users, i.e. from working to the technical controls, compared with organisations that had never obtained Cyber Essentials.

Figure 3 Use of other cyber security schemes, standards and principles

Current and lapsed Cyber Essentials users



Organisations that had never obtained Cyber Essentials



For more than half (53%) of Cyber Essentials users, the scheme appears to be providing the only form of external assurance for their cyber security. Among micro organisations, the proportion is even higher, at two thirds (66%).

Without Cyber Essentials, these organisations could have been left exposed to the potential risks of a successful basic cyber attack. However, with the technical controls in place, they could be helping to boost users’ cyber risk awareness, understanding and confidence in assessing and reducing cyber security risks – explored further in chapters 4 and 5.

In cases where Cyber Essentials users hold more than one solution, e.g. Cyber Essentials in tandem with ISO 27001, this could mean that Cyber Essentials is complementary to other products. Conversely – and especially where Cyber Essentials is mandated in government contracts – it could also mean that some organisations feel no choice but to adopt both.

Among organisations that had never obtained Cyber Essentials, almost three quarters (72%) are not using any other security schemes, standards and principles, rising to 80% among micro organisations. This provides the first indication that these organisations could be lacking basic cyber security risk awareness. The exception might be where they are already working to the Cyber Essentials technical controls without being certified (explored further in section 6.2).

Table 9 Use of other cyber security schemes, standards and principles (by size-band)

Current and lapsed Cyber Essentials users	**All**	**Micro (< 10 staff)**	**Small (10-49 staff)**	**Medium (50-249 staff)**	**Large (250+ staff)**
Base	**606**	**191**	**187**	**129**	**99**
None (no other boxes can be ticked)	53%	66%	52%	48%	33%
ISO 27001	26%	14%	26%	36%	38%
PCI-DSS	13%	6%	9%	14%	32%
IASME Cyber Assurance	10%	14%	10%	8%	5%
NIST Cyber Security Framework	9%	6%	5%	8%	22%
Other NCSC Guidance. e.g. Cloud Principles	8%	5%	6%	5%	19%
CIS Critical Controls	4%	4%	3%	2%	12%
Service Organisational Control (SOC) 2	2%	1%	1%	4%	5%
Other	7%	5%	9%	8%	3%

Organisations that had never obtained Cyber Essentials	**All**	**Micro (< 10 staff)**	**Small (10-49 staff)**	**Medium (50-249 staff)**	**Large (250+ staff)**
Weighted Base	**492**	**156**	**154**	**103**	**79**
None (no other boxes can be ticked)	72%	80%	77%	74%	43%
ISO 27001	11%	4%	6%	17%	25%
NIST Cyber Security Framework	6%	4%	5%	6%	14%
PCI-DSS	2%	1%	-	-	13%
Other NCSC Guidance. e.g. Cloud Principles	2%	2%	-	1%	6%
IASME Cyber Assurance	1%	1%	-	1%	3%
Service Organisational Control (SOC) 2	1%	-	1%	-	4%
CIS Critical Controls	0%	1%	1%	-	-
Other	12%	12%	12%	5%	19%

Responses self-classified as ‘other’ among Cyber Essentials users include: CREST penetration testing, NHS Data Security and Protection Toolkit, NHS Digital Toolkit. Several also mentioned ISO 9001 – a quality standard rather than a cyber security standard – indicating possible confusion.

Responses self-classified as ‘other’ among organisations that had never obtained Cyber Essentials include: Antivirus software, C5 (Germany), Carbon Neutral and PRI, CMA, DNV Cyber Assurance, FedRAMP Moderate (US), FLS, FMA, IASME Maritime Baseline Scheme, ISO 9001, ISO 14001. Some of these are not related to cyber security and others relate to very specific aspects. This suggests that some organisations may be adopting these because they are asked to do so to gain contracts, as is the case to some extent with Cyber Essentials.

4. Relationship between Cyber Essentials and Cyber Risk Awareness

This chapter explores organisations' awareness of cyber security risks, their concern about falling victim to a successful cyber attack, and the perceived impact of a hypothetical cyber attack. In doing so, it compares the views and attitudes of Cyber Essentials users with those that had never obtained Cyber Essentials certification to understand the possible relationship between the scheme and aspects of risk awareness.

Key findings summary

The evidence suggests that – compared to organisations that had never obtained Cyber Essentials – scheme users are better able to identify where they experience a common, unsophisticated cyber attack. They also appear to be more concerned about potentially falling victim to a cyber attack and have a greater appreciation of the potential consequences of a successful attack in terms of reputational, financial and legal effects.

The findings point to initial greater risk awareness among Cyber Essentials users, fuelling a heightened sense of concern about the potential threats around them. As a result, scheme users are then able to better appreciate the potential impact of a cyber attack.

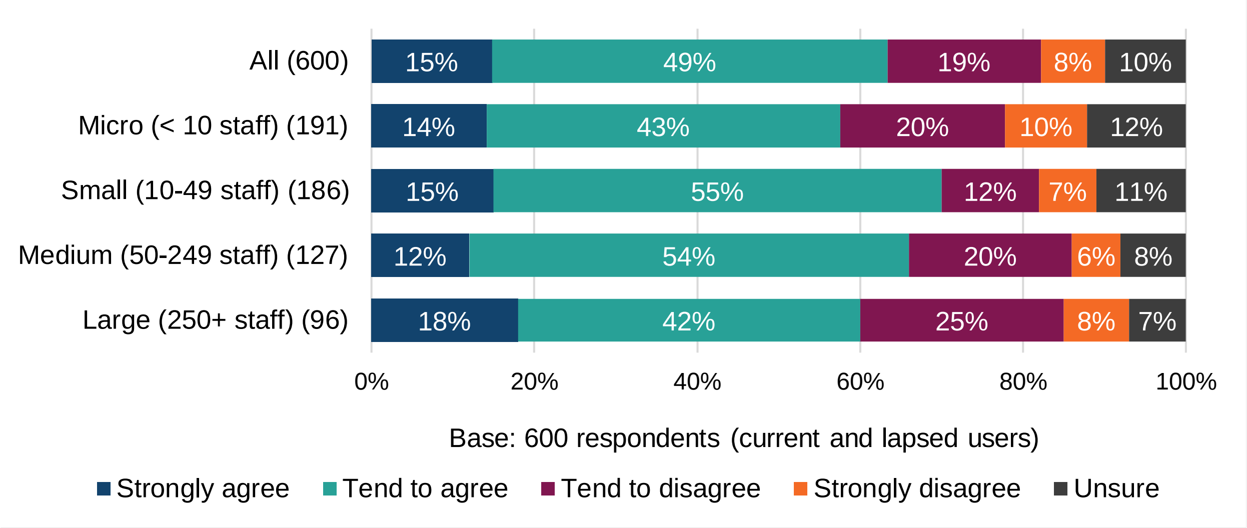
4.1 Cyber risk awareness and identification

Evidence gathered and assessed for this evaluation points to Cyber Essentials certification playing a key role in increasing organisations' awareness of cyber security risks and being better able to identify instances of an unsophisticated cyber attack. This is important since, otherwise, a breach could go unnoticed or cyber criminals could remain on systems for a long period of time, which might be more harmful.

Looking at the existing evidence for this, the Cyber Security Longitudinal Survey: Wave 2 noted that organisations adhering to one or more cyber security standards were more likely to report having experienced a cyber security incident. Additionally, Britain Thinks found that 50% of Cyber Essentials users reported one or more occasion in which they had been targeted in the past 12 months compared to 24% of organisations that had never obtained the certification.

Taking this a step further, almost two thirds (64%) of Cyber Essentials users surveyed for this evaluation agree that being certified better enables them to identify where they experience a common, unsophisticated cyber attack (Figure 4). The picture is similar across the size-bands.

Figure 4 Extent of agreement that Cyber Essentials improves an organisation's ability to identify a common, unsophisticated cyber attack (current and lapsed users by size-band)



Cyber Essentials users interviewed following the survey were asked if they had experienced a noticeable change in apparent cyber incidents since becoming certified. Most found this difficult to gauge or answer, although a small number did affirm that they had become more aware of having experienced attacks which they put down to having better awareness.

> "We are more aware and track incidents. We have seen an increase in incidents, but a decrease in those that are getting through."
>
> **Non-governmental Organisation, large employer**

> "We're still bombarded with spam emails, it isn't a reduction of attacks, but we have added protections so they're not successful. Our employees are now trained to a standard with spam filters and virus protection. The level of successful attacks has probably decreased just because of that heightened awareness."
>
> **Private business, medium employer**

4.2 Concern about falling victim to a successful cyber attack

As a result of scheme users being better able to identify cyber security risks, they are potentially more informed. As a result of being more informed, they can have a heightened sense of concern about potentially falling victim to a successful cyber attack.

This could have the effect of making it appear that they are in a worse situation (i.e. that the attack frequency is increasing) when in fact it may mean that previous attacks went undetected, organisations have since improved their awareness of them through being

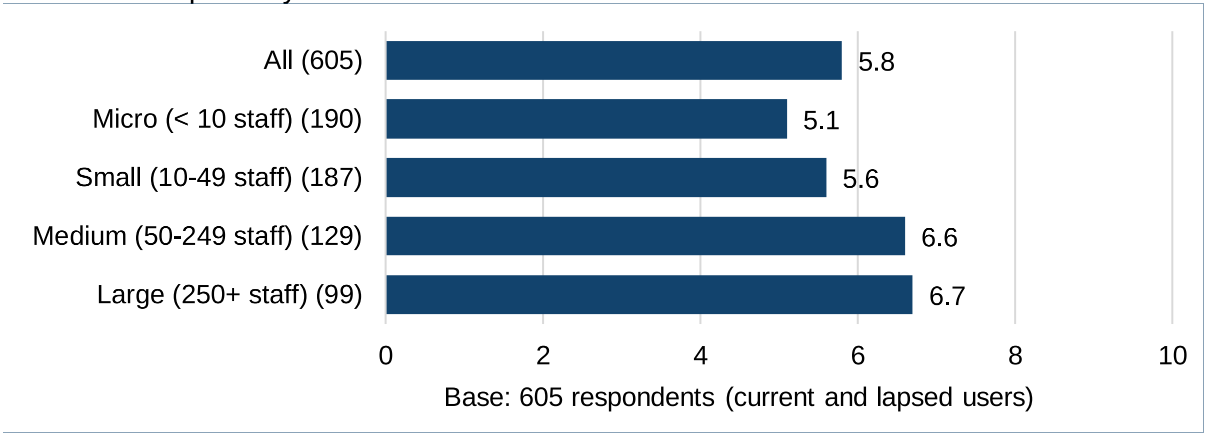
Cyber Essentials certified, and the technical controls could have played a role in preventing an attack.

Looking at the existing evidence base, Britain Thinks noted that Cyber Essentials users are more likely than those that had never obtained certification to believe their organisation is likely to suffer a cyber breach (24% and 13% respectively).

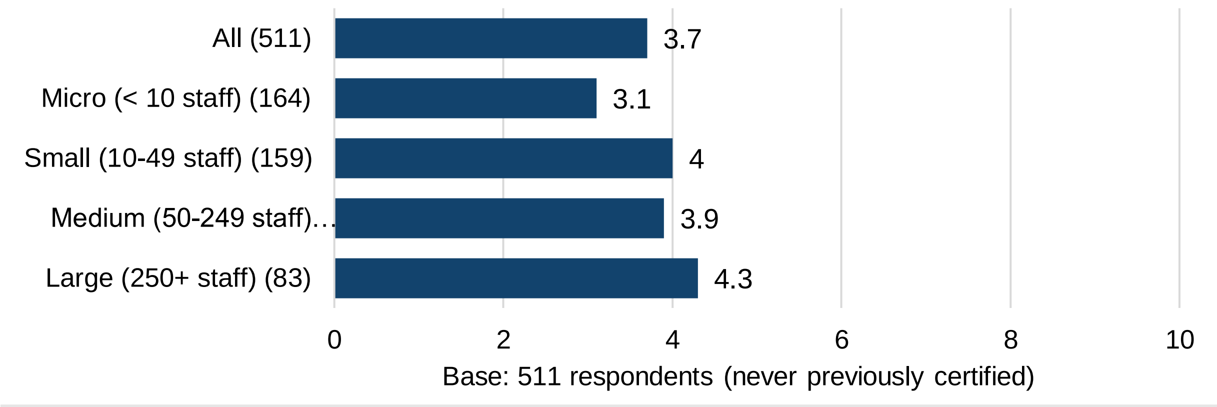
All organisations surveyed for this evaluation were asked, on a scale from 1 (not at all concerned) to 10 (extremely concerned), how concerned they are that their organisation might fall victim to a successful cyber attack in the next 12 months (Figure 5).

Figure 5 Extent of concern that the organisation might become the victim of a successful cyber attack

Current and lapsed Cyber Essentials users



Organisations that had never obtained Cyber Essentials



Levels of concern are moderate, with the mean rating among Cyber Essentials users being 5.8 (mode = 5). However, this level of concern is significantly higher than organisations that had never obtained Cyber Essentials, returning a mean rating of 3.7 (mode = 2). This affirms the idea that scheme users are potentially more informed about cyber risks and – hence – concerned about them.

For both survey audiences, the mean ratings given by small, medium and large organisations are significantly higher than those given by micro organisations. There could be a number of reasons for this, for example it may be due to the level of scrutiny on these organisations, cyber security being a higher Board priority, or that larger organisations have more ready access to dedicated specialist cyber security expertise.

4.3 Perceived impact of a possible cyber attack

As a result of being better informed about cyber risks and more concerned about potentially falling victim to a cyber attack, Cyber Essentials users appear to have a greater appreciation of the potential consequences of a possible attack on their organisation.

Firstly, all organisations surveyed for this evaluation were asked a hypothetical question – were they to suffer a major cyber attack the next day that became public knowledge, how significant an impact would that have for them in terms of:

- Reputational impact
- Financial impact
- Legal impact

Answers were sought on a scale from 1 'no impact' to 10 'significant impact' (Table 10).

Table 10 Perceived reputational, financial and legal impact of a possible cyber attack

Current and lapsed Cyber Essentials users	**Mean**	**Median**	**Mode**
Reputational impact (Base: 601)	8.0	9.0	10.0
Financial impact (Base: 602)	6.9	8.0	8.0
Legal impact (Base: 600)	6.6	7.0	5.0
Organisations that had never obtained Cyber Essentials	**Mean**	**Median**	**Mode**
Reputational impact	6.8	7.0	8.0
Financial impact (Base: 602)	6.5	7.0	7.0
Legal impact	6.2	7.0	7.0

The perceived significance of impact is rated highest in relation to reputation, followed by financial and then legal. The data reveal the mean ratings to be high for both survey audiences, although they are significantly higher among Cyber Essentials users than organisations that had never obtained Cyber Essentials. This suggests that scheme users have a greater appreciation or understanding of the impact of cyber incidents, which in turn can encourage them to put in place additional controls and processes beyond the Cyber Essentials technical controls – discussed further in chapter 6.

Breakdowns by size-band are shown in Table 11. The mean ratings given by small, medium and large organisations are significantly higher than micro organisations. This points to a more acute sense of concern and greater risk awareness among larger organisations, which may be reflective of having greater resources focused on cyber security risk management.

Table 11 Perceived reputational, financial and legal impact of a possible cyber attack (by size-band)

	All	Micro (<10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Current and lapsed Cyber Essentials users					
Reputational impact (Base: 601)	8.0	7.4	9.8	8.3	8.3
Financial impact (Base: 602)	6.9	6.4	6.9	7.2	7.5
Legal impact (Base: 600)	6.6	6.0	6.6	7.0	7.0
Organisations that had never been Cyber Essentials certified					
Reputational impact	6.8	5.2	7.1	7.7	8.0
Financial impact (Base: 602)	6.5	5.0	7.1	7.1	7.6
Legal impact	6.2	4.6	6.7	7.2	7.2

Research by Britain Thinks supports the data in this survey and found that almost two thirds (65%) of Cyber Essentials were in agreement that a cyber attack would result in a significant financial cost to their organisation, compared with 44% of those that had never obtained the certification.

This suggests that improved cyber security risk awareness as a result of being certified could be leading to a greater appreciation of the potential financial consequences.

5. Influence on Cyber Security Understanding and Confidence

This chapter assesses the difference that Cyber Essentials is making to organisations' understanding of cyber security risks, the steps they can take to reduce them, and their senior managements' understanding of the risks posed by cyber attacks. It also assesses the extent to which Cyber Essentials has directly contributed to scheme users' confidence in assessing and reducing cyber security risks, and being protected in the event of a common, unsophisticated cyber attack.

Key findings summary

The findings point to Cyber Essentials certification helping organisations to become more informed than they might otherwise have been about cyber security risks.

Most Cyber Essentials users believe that the scheme has directly improved their understanding of cyber security risks and their understanding of the steps they can take to reduce those risks. Most also believe it has directly strengthened their senior management understanding of the risks posed by cyber attacks, their confidence at being able to consistently implement steps to reduce cyber security risks, and their confidence in being protected in the event of such an attack. For some Cyber Essentials users, the scheme has opened their eyes to prior cyber security weaknesses and gaps which the technical controls have helped to plug.

As a result of having a better understanding of cyber security risks and the extent to which this could be a pervasive problem, organisations may be more cautious and feel compelled to do more to boost their organisations' cyber resilience (explored further in chapter 6).

It is important to note that the comparison survey of organisations that had never obtained Cyber Essentials reveals similarly high levels of perceived understanding and confidence in cyber security matters to those of scheme users. This suggests a likely overconfidence bias or that these organisations may be less informed about cyber security risks, especially where they do not hold other schemes, standards or accreditations.

5.1 Understanding of cyber security risks and steps to reducing them

This section examines the impact of Cyber Essentials on building organisations' understanding of cyber security risks in more detail, including the steps they can take to reduce those risks.

Firstly, Britain Thinks (2020) found that through the process of becoming Cyber Essentials certified, users of the scheme – particularly smaller businesses – gained a better understanding of the risks posed to their organisation by cyber threats and described cyber security as something they previously "knew they needed" to prioritise but lacked a clear understanding of how to approach it. This points to the scheme helping organisations to move away from a position of being less informed to more genuinely informed about cyber security risks.

Strategic stakeholders interviewed for the evaluation (comprising government representatives and key industry organisations) consider Cyber Essentials to be valuable for improving understanding of cyber security risks, especially among smaller organisations as they begin their journey to becoming more cyber resilient. Moreover, it is felt that even if an organisation fails to achieve certification, the feedback they receive can help to pinpoint improvements needed, thus encouraging further understanding and prompting action-planning to help that organisation meet the technical controls in the future.

On a scale from 1 ‘no understanding’ to 10 ‘complete and full understanding’, all organisations surveyed for this evaluation were asked to rate their understanding of the types of cyber security risks that could affect their organisation, along with the steps their organisation can take to reduce those risks. The results are shown in Table 12.

Table 12 Understanding of cyber security risks and steps to reduce them (averages)

Current and lapsed Cyber Essentials users	**Mean**	**Median**	**Mode**
Understanding of current cyber security risks (Base: 603)	8.5	9.0	10.0
Understanding of steps to reduce them (Base: 602)	8.4	9.0	10.0
Organisations that had never held Cyber Essentials	**Mean**	**Median**	**Mode**
Understanding of current cyber security risks (Base: 515)	7.7	8.0	8.0
Understanding of steps to reduce them (Base: 515)	7.8	8.0	8.0

Mean ratings are high, and higher still among Cyber Essentials users compared with organisations that had never obtained certification. This provides further evidence of the role of Cyber Essentials in elevating firms’ appreciation of cyber security risks.

With respect to organisations that had never obtained Cyber Essentials, it is important to factor in that there may be an element of overconfidence bias at play, as introduced in section 2.4. In other words, where these organisations lack awareness of the risks, they can only rate their understanding based on what they perceive to be the threat level.

To further justify this, it is worth noting that approximately half of scheme users taking part in the follow-up interviews stressed that the certification process highlighted security weaknesses they had prior to becoming certified. For example, one organisation described the process as a “huge learning curve” and another stated that Cyber Essentials “opened their eyes to the threats” that they hadn’t realised they had faced under earlier practices.

“I wouldn’t have considered some of the risks that became apparent, for example to do with open ports on the network. I hadn't really thought about that.”

Private business, small employer

"We're a very small business and I'm a mechanical engineer, not an IT specialist. I set up the cyber security to the best of my knowledge and thought I was doing quite well. I engaged with a local IT specialist and we found interesting holes in our cyber security."

Private business, micro employer

Breakdowns of the above chart by size-band are shown in Table 13. Whilst there is little difference across the bandings among scheme users, mean ratings among small, medium and large organisations that had never obtained Cyber Essentials are significantly higher than micro organisations. This suggests that these micro organisations currently have the lowest levels of cyber risk understanding and could stand to gain most if they were to become certified.

Table 13 Understanding of cyber security risks and steps to reduce them (by size-band)

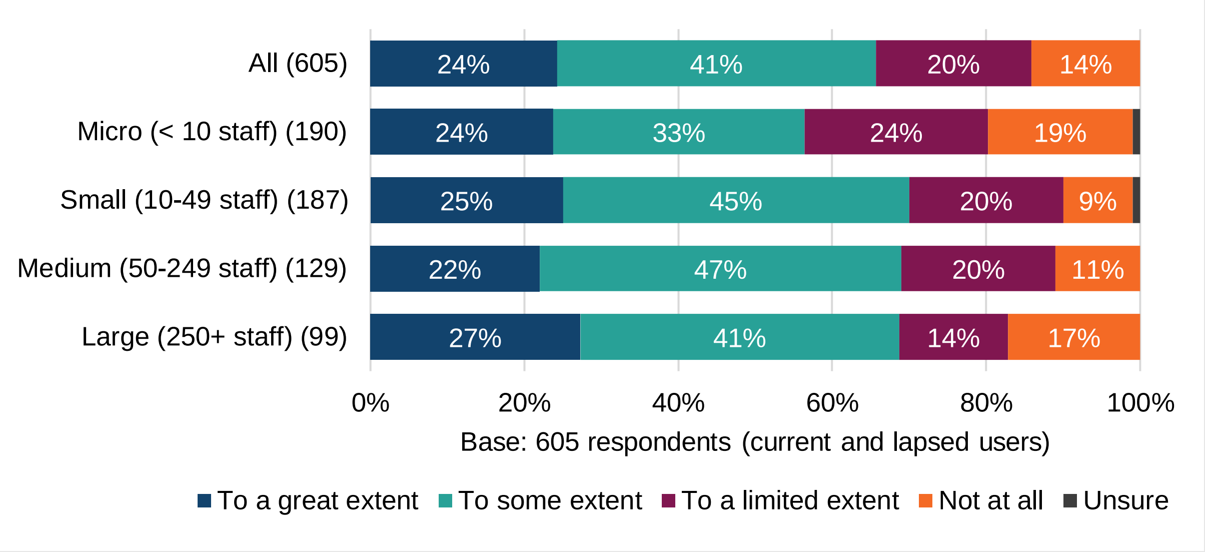
	All	**Micro (<10 staff)**	**Small (10-49 staff)**	**Medium (50-249 staff)**	**Large (250+ staff)**
Current and lapsed Cyber Essentials users					
Understanding of current cyber security risks (Base: 603)	8.5	8.5	8.5	8.4	8.5
Understanding of steps to reduce them (Base: 602)	8.4	8.4	8.5	8.4	8.5
Organisations that had never been Cyber Essentials certified					
Understanding of current cyber security risks (Base: 515)	7.7	6.8	7.8	8.1	8.6
Understanding of steps to reduce them (Base: 515)	7.8	6.7	8.0	8.3	8.8

Direct perceived influence of Cyber Essentials on understanding

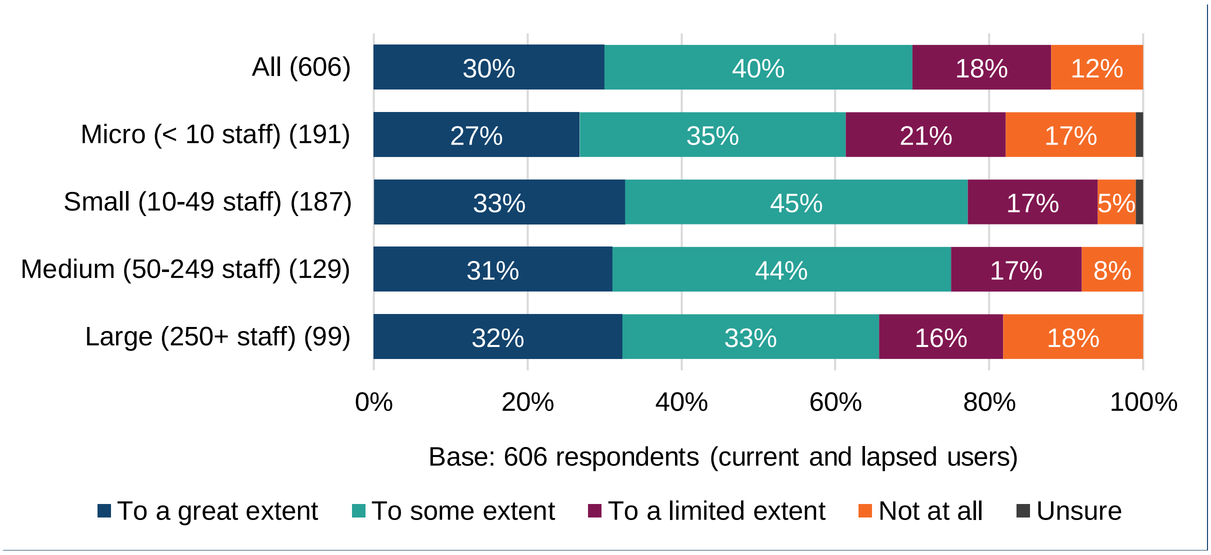
Cyber Essentials users were then asked the extent to which they believe Cyber Essentials has directly improved their understanding of cyber security risks and steps to reduce them (Figure 6).

Figure 6 Extent to which Cyber Essentials has improved understanding of cyber security risks and steps to reduce them (by size-band)

Understanding of cyber security risks



Understanding of steps to reduce cyber security risks



The findings point to the scheme making a positive difference, with 85% of organisations of the view that it has directly improved their understanding of cyber security risks. The picture is similar across the size-bands.

An even greater proportion (88%) believe that Cyber Essentials has directly improved their understanding of the steps they can take to reduce cyber security risks, again with a similar picture by size-band. The data clearly point to Cyber Essentials enabling large organisations to increase their understanding of steps to reduce cyber security risks as much as any other size of organisation. This is an important observation to counterbalance a view – as sometimes raised anecdotally – that Cyber Essentials is more oriented towards SMEs.

Several organisations interviewed following the survey affirmed that the scheme's technical controls allow for easier understanding of basic cyber security principles.

"It's the organisation of ideas that allows us to achieve better security. It's a formal structure which enables us to operate in an organised fashion, which we did not have before."

Private business, small employer

For some, joining the scheme has not so much increased their understanding of cyber security, but provided confirmation that they are already doing the right things by clearly laying out good practice.

"We were already quite proficient in matters of security before becoming certified, but Cyber Essentials is a valid, useful and helpful tool and we want to maintain it."

Private business, micro employer

Interviews with large organisations using Cyber Essentials found, in one case, that the scheme has raised their understanding of cyber security risks "to a higher level" and in another that Cyber Essentials helps them to set targets by identifying gaps and which cyber security elements they need to focus on as a business.

5.2 Senior management understanding of risks posed by cyber attacks

Existing evidence suggests that there is a positive relationship between organisations that adopt the Cyber Essentials technical controls and the involvement in, and understanding of, cyber security risks on the part of their senior management team.

For example, the DCMS Cyber Security Longitudinal Survey: Wave 1 revealed a positive relationship between greater board involvement (i.e. more frequent board-level discussions or updates about cyber security) and having in place all five of the technical control areas required to attain Cyber Essentials certification. Wave 2 noted that businesses meeting these were even more likely to report board-level cyber security training.

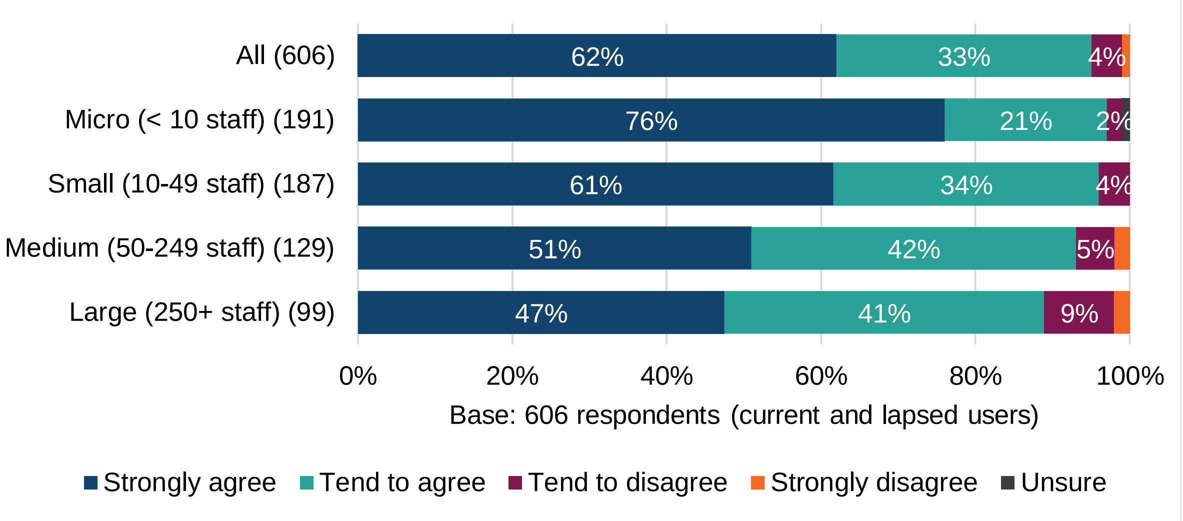
Additionally, analysis undertaken on the Cyber Security Breaches Survey 2023 found that, among businesses using Cyber Essentials, their board was more likely to say that they prioritised cyber security (93%) than businesses that did not use Cyber Essentials (70%). Similarly, scheme users were more likely to have taken action to identify cyber risks than non-users (93% versus 48%).

Britain Thinks (2020) reported that three in four surveyed Cyber Essentials users found certification to have had a positive impact on their senior management's understanding of the risk posed by cyber attacks. Certified organisations were also more likely than non-certified organisations to agree that their senior management appreciated the risk posed by cyber attacks, at 92% compared with 73%

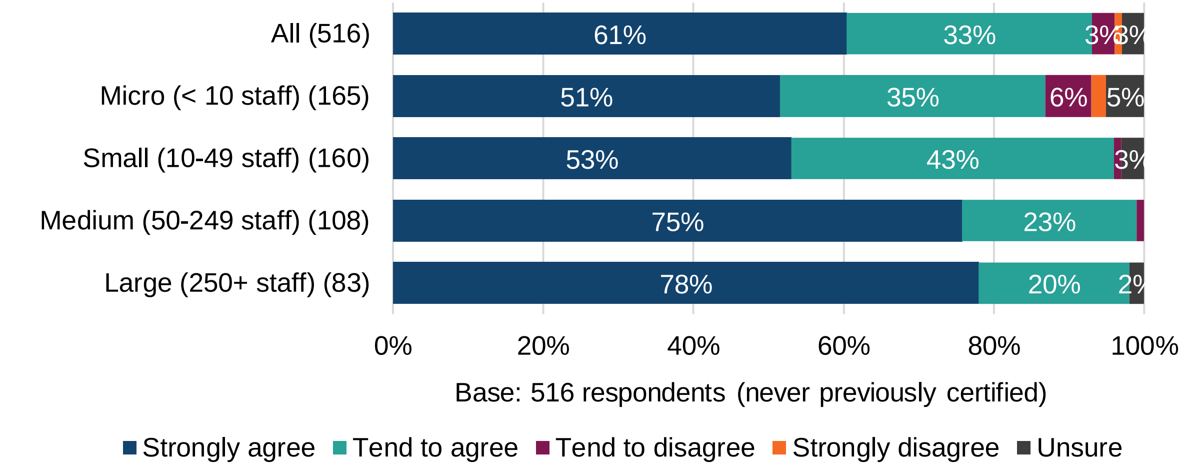
To examine this area in more detail, all organisations surveyed for this evaluation were asked the extent to which they agreed or disagreed that their senior management understands the risks posed by cyber attacks (Figure 7).

Figure 7 Extent of agreement that senior management understands the risks posed by cyber attacks (by size-band)

Current and lapsed Cyber Essentials users



Organisations that had never obtained Cyber Essentials



At first glance, the results reveal little difference between the two survey groups. Almost all (95%) of Cyber Essentials users agree that their senior management understands the risks posed by cyber attacks, along with a similarly high proportion (94%) of organisations that had never obtained Cyber Essentials. Further research would be needed to understand this more fully, but possible reasons for the high proportion among the latter group are as follows:

- An element of overconfidence bias at play, including an assumption that their senior management is fully up to speed
- A perception that their organisation is unlikely to come under attack or that they would not make a likely target for cyber criminals (leading to a false sense of security about the risks they face and their understanding of those risks)

- A perception that they already have robust cyber security risk management arrangements in place, for example, through other cyber security schemes, standards or accreditations

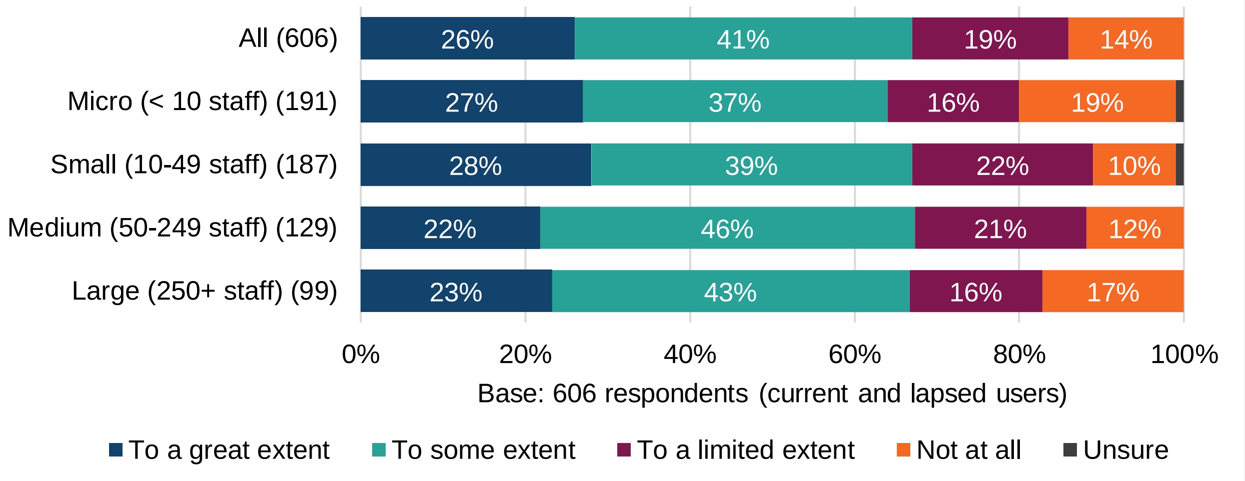
The proportion of micro sized Cyber Essentials users agreeing that their senior management understands the risks posed by cyber attacks is significantly higher than other size-bands. It may be the case here that senior leaders are more directly involved in aspects of cyber security in these smaller organisations.

Among organisations that had never obtained Cyber Essentials, a significantly higher proportion of medium and large organisations than micro and small organisations strongly agree that their senior management understands the risks posed by cyber attacks. Further qualitative research would be needed among organisations that had never obtained Cyber Essentials to more fully understand this, especially among larger organisations. It may be, for example, that having more dedicated in-house IT expertise, or other cyber security standards and accreditations in place besides Cyber Essentials, could be helping some organisations to feel they better understand the risks posed by cyber attacks.

Direct perceived influence of Cyber Essentials on senior management understanding of risks posed by cyber attacks

Cyber Essentials users were asked the extent to which they believe the scheme has directly strengthened their senior management's understanding of risks posed by cyber attacks (Figure 8).

Figure 8 Extent to which Cyber Essentials has strengthened senior management understanding of the risks posed by cyber attacks (current and lapsed users by size-band)



Most say that that the scheme has directly strengthened senior managers' understanding (86%), with a similar pattern by size-band.

This points to Cyber Essentials playing a meaningful role in shaping senior level attitudes, which could – from there – influence wider organisational attitudes and cyber security resilience practices – explored further in chapter 6.

5.3 Confidence in assessing and reducing cyber security risks

Strategic stakeholders interviewed for this research (comprising government and key industry organisations) asserted that Cyber Essentials can build confidence in organisations' cyber security posture and offer peace of mind. This is considered especially likely among:

- Smaller organisations that have no other cyber security protection in place, may be concerned about their level of risk exposure or nervous about how to manage cyber security
- Organisations dealing with substantial amounts of sensitive data, such as those in the finance or health sectors
- Small charities for which the consequences of a data breach could be operationally and reputationally damaging

One stakeholder made the point that smaller organisations are less likely to have dedicated IT departments and that the job of managing cyber security often falls to someone who may lack expertise in this area. They added that the Cyber Essentials certification process can unlock access to guidance and help to boost confidence and proficiency in managing risks and identifying what improvements are needed.

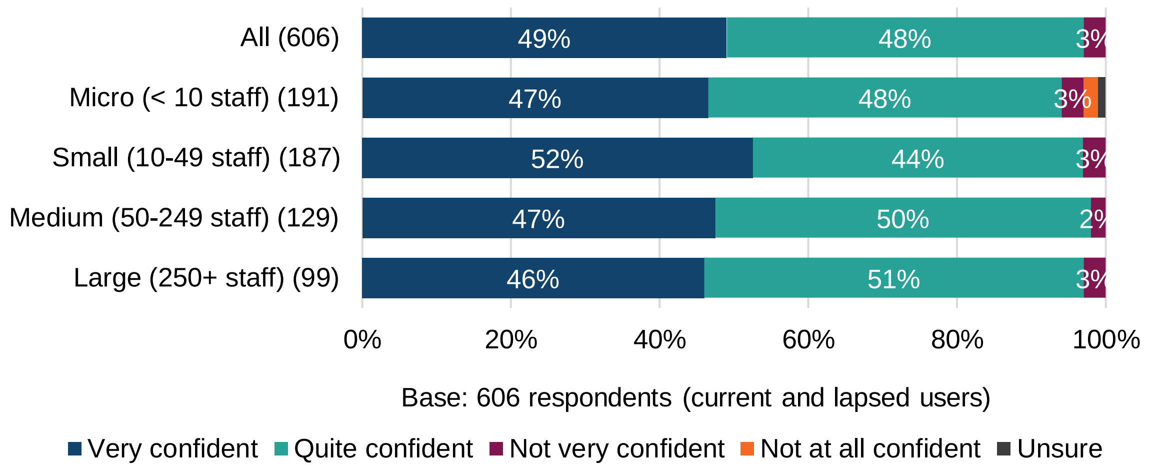
At the same time, several stakeholders suggested that the scheme may be less likely to boost the cyber security confidence of larger organisations that already have strong expertise within their security apparatus, or other schemes and standards that they work to, such as ISO 27001. That said, one stakeholder argued that larger organisations are not an exception when it comes to security pitfalls since many “may not be getting the basics right”, which Cyber Essentials can help to pinpoint.

Confidence in consistently implementing steps to assess and reduce cyber security risks

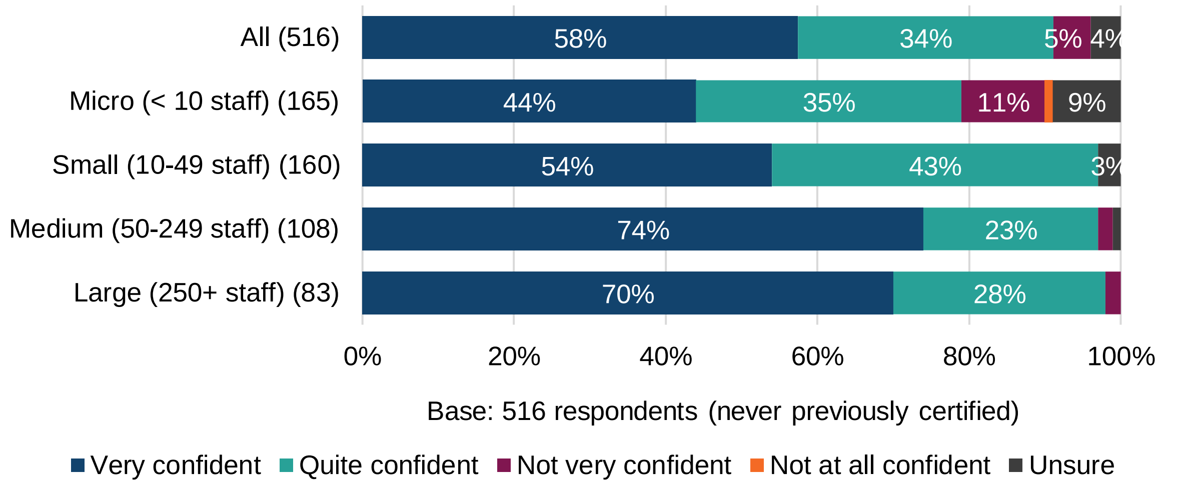
All organisations surveyed for this evaluation were asked how confident they are that they consistently implement steps to assess and reduce cyber security risks (Figure 9).

Figure 9 Confidence that the organisation consistently implements steps to assess and reduce cyber security risks (by size-band)

Current and lapsed Cyber Essentials users



Organisations that had never obtained Cyber Essentials



Almost all Cyber Essentials users (97%) say they are confident, along with a similarly high proportion of organisations that had never obtained Cyber Essentials (94%). Interestingly, the latter group appears more inclined to state that they are “very confident.”

This follows a similar pattern to the results presented in the previous chapter and is evidence of a likely overconfidence among organisations that had never obtained Cyber Essentials. This could be exacerbated where these organisations are less informed about cyber security risk, as described in section 5.1.

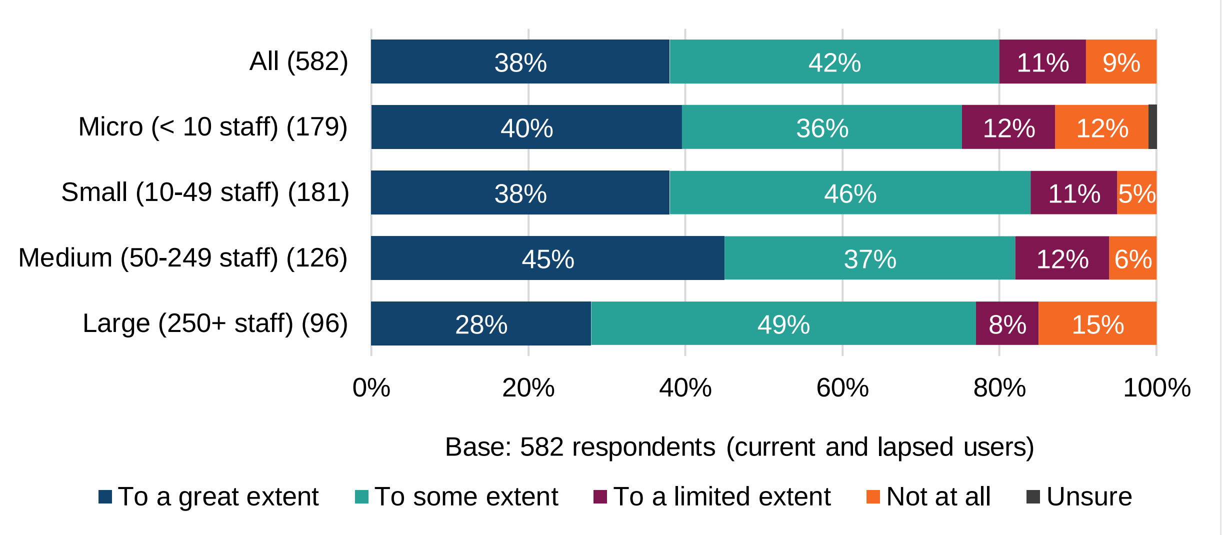
At the same time, Cyber Essentials users may be developing a better understanding of cyber risk and in turn realising the extent to which cyber security risk is a pervasive problem. This could make these organisations more cautious and could stimulate a desire to want to do more to boost their confidence in assessing and reducing risks.

Among scheme users, confidence levels are similar across the size-bands. However, among organisations that had never obtained Cyber Essentials, small, medium and large organisations are significantly more confident than micro organisations. These results suggest that – should these micro organisations become Cyber Essentials certified in the future – they could stand to gain most in terms of confidence.

Direct influence of Cyber Essentials on confidence that organisations consistently implement steps to assess and reduce cyber security risks

Cyber Essentials users were asked the extent to which they believe the scheme has directly improved their confidence at being able to consistently implement steps to reduce cyber security risks (Figure 10).

Figure 10 Extent to which Cyber Essentials has improved confidence in consistently implementing steps to assess and reduce cyber security risks (current and lapsed users by size-band)



Base: 582 respondents (current and lapsed users)

Most (91%) believe that the scheme has boosted their confidence, with similar levels across the size-bands. It is important to note that where larger organisations make more extensive use of other schemes and standards (Table 9, section 3.3), this could represent a confounding variable, making it harder to disaggregate the effects of Cyber Essentials alone on their confidence levels.

Most organisations interviewed following the survey say they are keeping on top of Cyber Essentials scheme requirements regularly and through established internal processes, which is helping to increase their confidence more and more. Among CE Plus users in particular, the scheme and associated external audit has helped to boost confidence by validating actions already being taken.

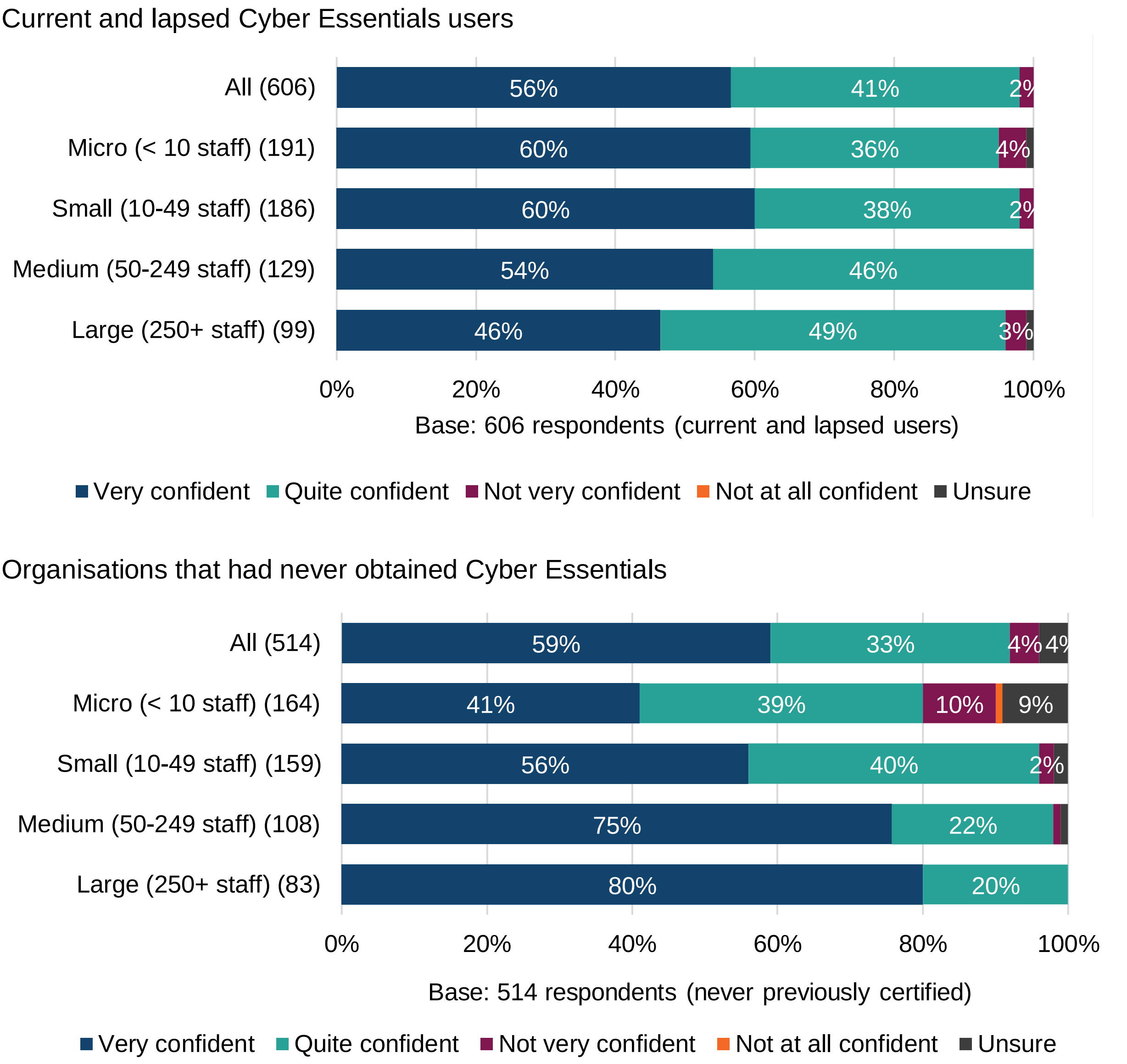
> "It's mainly a case of undertaking continual reviews of progress with regards to vulnerability management. We plan ahead more so now than being reactive, which is what used to happen."
>
> **Private business, large employer**

Other organisations interviewed following the survey described how cyber security practices have become more deeply embedded within their organisations as a "business as usual" approach. This involves IT teams helping staff to understand their collective role in adopting a cyber security posture through stronger protocols and procedures. These are explored in more detail in the next chapter, spanning wider cyber security practices.

5.4 Confidence in protection from a common, unsophisticated cyber attack

All surveyed organisations were asked how confident they are that their organisation is protected in the event of a common, unsophisticated cyber attack (Figure 11).

Figure 11 Confidence that the organisation is protected in the event of a common, unsophisticated cyber attack (by size-band)


Current and lapsed Cyber Essentials users

Organisations that had never obtained Cyber Essentials

Almost all Cyber Essentials users are confident (97%) with similar results across the size bands. Among organisations that had never obtained Cyber Essentials, confidence is similarly high (92%) and there is a greater tendency for these organisations to say they are very confident that they are protected.

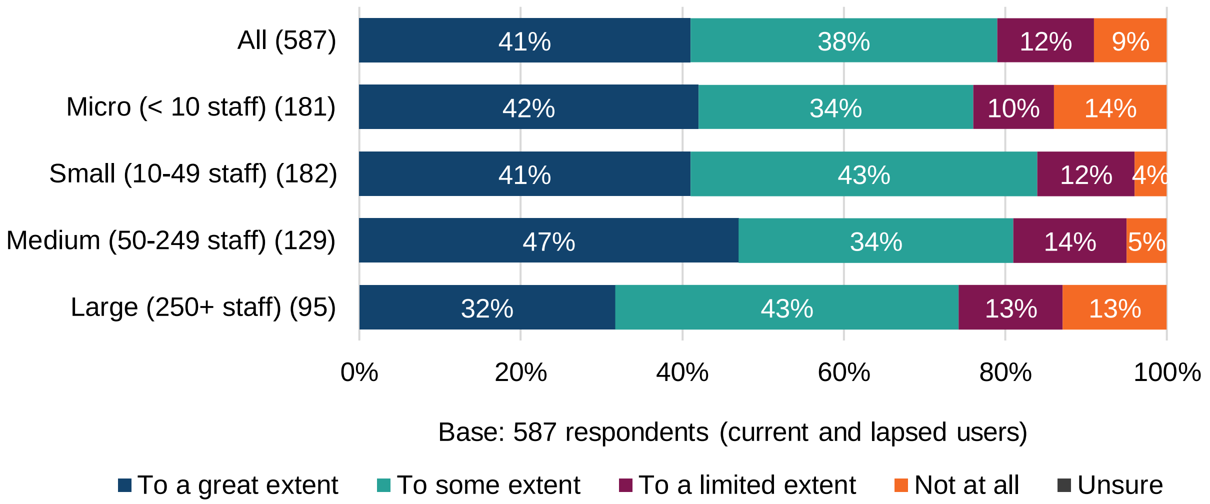
The reasons for this are potentially complex and may include:

- Overconfidence among organisations that had never obtained Cyber Essentials
- Potential for these organisations to think they are better protected than they really are, especially where they may not be fully appreciative of cyber security risks
- An assumption that they are less likely to be targeted by a cyber attack, which in turn downplays the perceived level of protection that they need

Direct influence of Cyber Essentials on confidence that organisations are protected in the event of a common, unsophisticated cyber attack

Cyber Essentials users were asked the extent to which they believe the scheme directly improved their confidence in being protected in the event of a common, unsophisticated cyber attack (Figure 12).

Figure 12 Extent to which Cyber Essentials has improved confidence in being protected in the event of a common, unsophisticated cyber attack (current and lapsed users by size-band)



Most (91%) believe that the scheme has directly improved their confidence, with similar levels across the size-bands.

6. Stimulation of Wider Cyber Security Practices

Building on evidence of Cyber Essentials users' deeper understanding of cyber security risks and greater confidence in reducing them, this chapter examines how, and the extent to which, Cyber Essentials users have implemented additional preventative actions beyond the technical controls. It then looks at how the scheme has contributed to wider cyber resilience and the different ways good cyber security practice has become embedded within organisations that use it. Finally, it summarises views on negative or unforeseen consequences.

Key findings summary

Through a heightened sense of concern about cyber security risks, Cyber Essentials users appear more compelled to adopt wider cyber security practices within their organisations. Most surveyed scheme users report having taken additional preventative actions beyond the scheme's technical controls and agree that the scheme has directly strengthened how seriously their organisation takes cyber security. For example, the scheme has prompted a more serious attitude and approach to cyber security through regular and open conversations on cyber security protocols and why they are important.

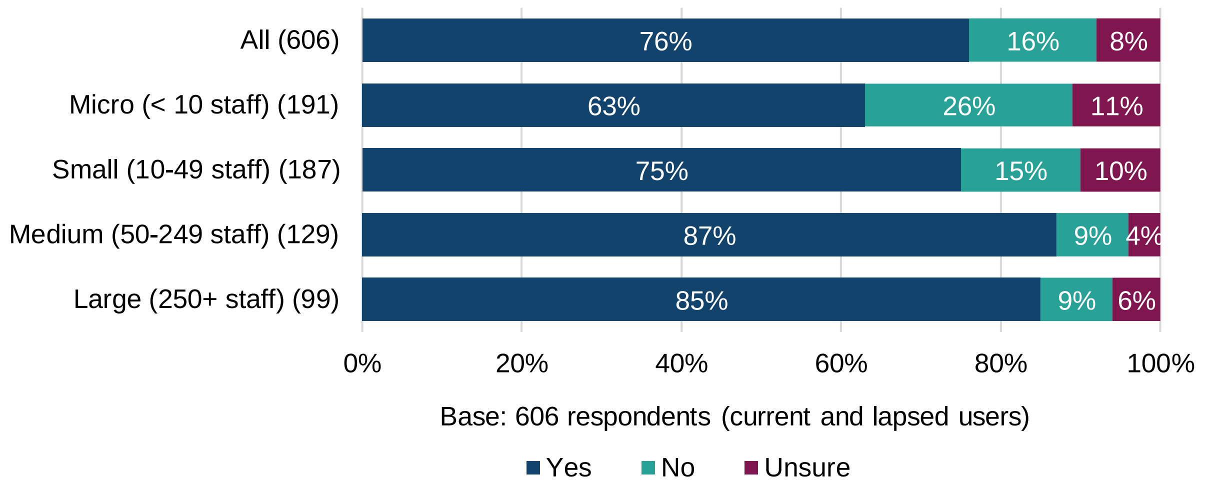
Cyber Essentials also appears to be guiding organisations that had never obtained certification, with a small minority having drawn upon its published guidance to strengthen their own security. Furthermore, among 53 surveyed organisations certified to ISO 27001 but not Cyber Essentials, more than four in ten say that their organisation currently only meets some of the Cyber Essentials technical controls, pointing to the potential value of the scheme for these organisations.

6.1 Taking additional steps beyond the technical controls

The evidence to date has found that Cyber Essentials is helping scheme users become more cyber risk aware, more appreciative of the potential consequences of a cyber attack, and more understanding of the risks their organisation can face and steps to reduce them. This process, combined with stronger senior management buy-in, may be seeding a more holistic approach to cyber security, including practices beyond the technical controls.

Surveyed Cyber Essentials users were asked whether they have taken additional steps, beyond the scheme's technical controls, to improve cyber security (Figure 13).

Figure 13 Whether taken additional steps beyond the technical controls to improve cyber security (current and lapsed users by size-band)



Approximately three quarters (76%) report that they have taken additional steps. The proportion of small, medium and large organisations taking additional steps is significantly higher than micro organisations, which could be explained for example by having more dedicated resources to plan and deliver those.

Interviews with a sample of Cyber Essentials users following the survey (summarised below) explored how the scheme is helping to catalyse additional steps. Further examples can be found in the case studies (section 9).

Types of preventative actions taken

Examples of additional steps mentioned by surveyed organisations to improve their cyber security and resilience are many and varied, with the most common being implementing ISO 27001. Other actions include putting in place additional software, standards, training, internal controls and review processes, penetration testing and infrastructure change. Organisations also report adopting new policies and procedures, carrying out additional risk assessments to ensure their defences stay up to date, and thinking regularly about how to improve their cyber security posture.

> “One of the requirements is to make sure all software is updated within 14 days of a security patch. It has meant we now have procedures in place to do this.”
>
> **Non-governmental Organisation, large employer**

For a small minority of interviewed organisations, becoming certified has not led to them take additional steps. Two interviewed organisations explained that they see the self-assessment as more of a “tick-box” exercise for securing contracts, as opposed to a tool which fosters stronger cyber security risk management. They also mentioned that they feel ISO 27001 offers more guidance on how to achieve and implement cyber security measures. This of course may depend on other factors such as the assessor and scope of assessment which were not examined as part of this evaluation.

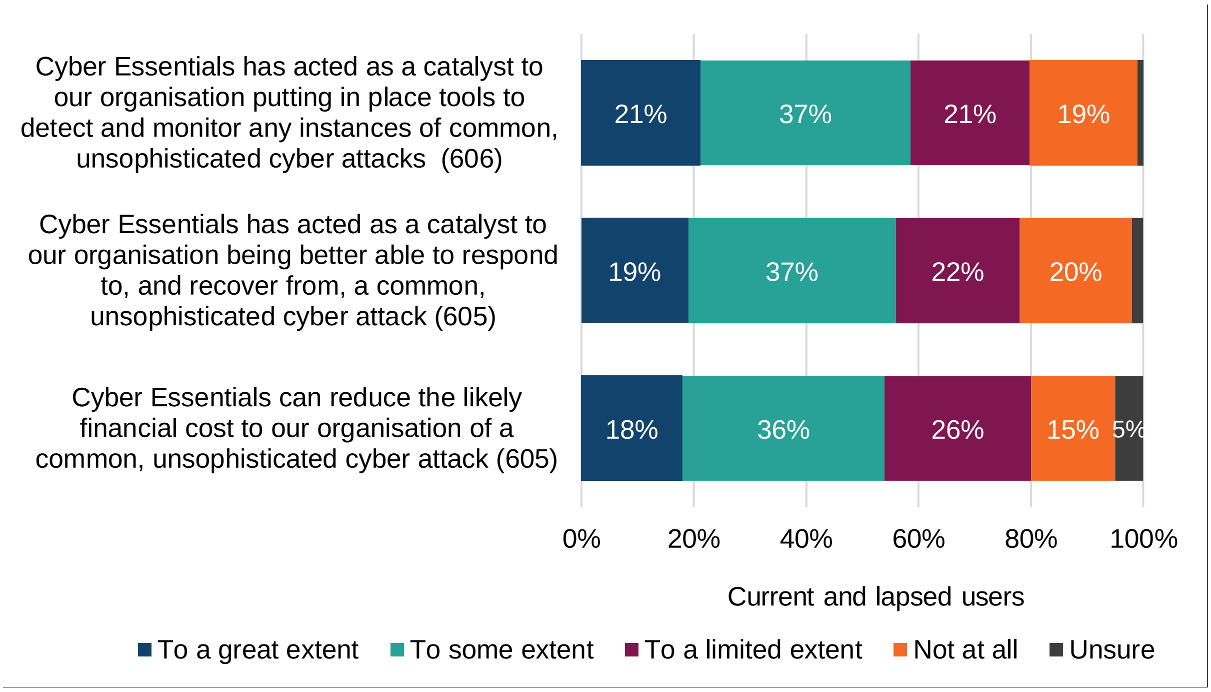
6.2 Catalyst to cyber resilience

Whilst the main aim of Cyber Essentials is to protect organisations against a common, unsophisticated cyber attack, scheme users report that it is also helping them to undertake the following:

- Detect and monitor instances of a common, unsophisticated cyber attack
- Respond to and recover from a common, unsophisticated cyber attack
- Reduce the likely financial cost to their organisation from such an attack

Most scheme users believe the scheme has worked successfully in these respects (Figure 14).

Figure 14 Extent to which Cyber Essentials is a catalyst to cyber resilience (current and lapsed users)



When probed further on how Cyber Essentials can help scheme users to reduce the financial cost to their organisation of a common, unsophisticated cyber attack, they explained this in terms of reducing the likelihood of a successful attack which means reduced costs in terms of response, recovery, and other losses. They also mentioned the value of having the bundled insurance in place as an additional safeguard, discussed further in section 8.2.

Breakdowns of the above chart by size-band are shown in Table 14, with similar results across the bands.

Table 14 Extent to which Cyber Essentials is a catalyst to cyber resilience (current and lapsed users by size-band)

STATEMENT A: Cyber Essentials has acted as a catalyst to our organisation putting in place tools to detect and monitor any instances of common, unsophisticated cyber attacks

	All (606)	Micro (< 10 staff) (191)	Small (10-49 staff) (187)	Medium (50-249 staff) (129)	Large (250+ staff) (99)
To a great extent	21%	19%	22%	24%	19%
To some extent	37%	28%	42%	40%	41%
To a limited extent	21%	28%	17%	19%	20%
Not at all	19%	23%	18%	16%	17%
Unsure	1%	2%	1%	1%	2%

STATEMENT B: Cyber Essentials has acted as a catalyst to our organisation being better able to respond to, and recover from, a common, unsophisticated cyber attack

	All (605)	Micro (< 10 staff) (191)	Small (10-49 staff) (186)	Medium (50-249 staff) (129)	Large (250+ staff) (99)
To a great extent	19%	17%	19%	23%	16%
To some extent	37%	31%	42%	39%	37%
To a limited extent	22%	24%	20%	19%	25%
Not at all	20%	24%	16%	18%	20%
Unsure	2%	4%	3%	1%	1%

STATEMENT C: Cyber Essentials can reduce the likely financial cost to our organisation of a common, unsophisticated cyber attack

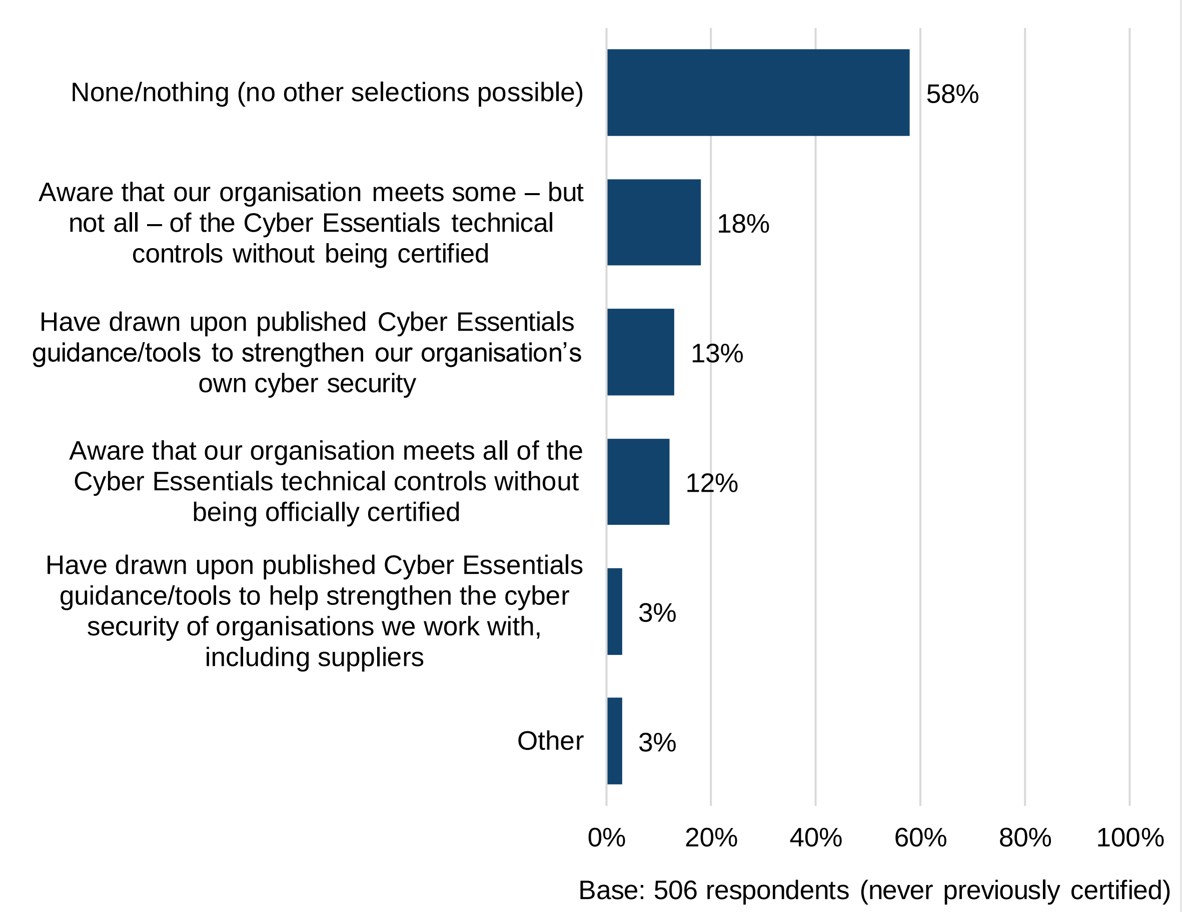
	All (605)	Micro (< 10 staff) (191)	Small (10-49 staff) (186)	Medium (50-249 staff) (129)	Large (250+ staff) (99)
To a great extent	18%	18%	17%	22%	14%
To some extent	36%	27%	45%	40%	29%
To a limited extent	26%	32%	19%	22%	33%
Not at all	15%	18%	12%	13%	18%
Unsure	5%	4%	7%	2%	5%

Use of Cyber Essentials scheme information and technical controls among organisations that had never obtained certification

Cyber Essentials scheme information is referred to by some organisations that have never obtained certification – appearing to help them with their cyber security journey.

Among these surveyed organisations, a small minority (13%) have drawn upon the scheme's published guidance to strengthen their own security, and 3% have used it to strengthen the cyber security of organisations they work with, including suppliers (Figure 15).

Figure 15 Use of Cyber Essentials scheme information and controls among organisations that had never obtained certification



Base: 506 respondents (never previously certified)

Analysis also involved looking at the use of Cyber Essentials by a small, weighted base of 53 organisations that had never obtained the certification but do use ISO 27001. Of these:

- Just under a quarter (24%) said they have drawn upon Cyber Essentials guidance to strengthen their own cyber security or that of their supply chain
- More than four in ten of this small cohort (42%) say that their organisation only meets some of the Cyber Essentials technical controls

This indicates that Cyber Essentials adds value to an organisation's cyber security even where they already have other schemes and standards in place.

Cross-tabulations of Figure 15 by size-band are presented in Table 15.

The proportions of small, medium and large organisations saying that they already meet some – but not all – of the Cyber Essentials technical controls are significantly higher than that of micro organisations. This points to micro organisations being less likely to have embarked on a cyber security journey and thus have lower perceived awareness of cyber security risks.

Furthermore, the proportion of medium and large organisations that have drawn upon published Cyber Essentials guidance and tools to strengthen their organisation's own cyber security is significantly higher than micro and small organisations. It may also be the case (as mentioned by one industry stakeholder interviewed for this evaluation) that cyber security specialists within larger organisations are using the scheme's guidance as an additional checklist without feeling the need to become certified, or that they otherwise see value in the scheme's technical controls but encounter obstacles to becoming certified. Meanwhile, smaller organisations simply may not have come into contact with the guidance or may not have understood it.

Table 15 Use of the Cyber Essentials scheme among organisations never certified (by size-band)

Weighted Bases	All (506)	Micro (< 10 staff) (161)	Small (10-49 staff) (159)	Medium (50-249 staff) (105)	Large (250+ staff) (81)
None/nothing (no other selections possible)	58%	69%	57%	53%	45%
Aware that our organisation meets some – but not all – of the Cyber Essentials technical controls without being certified	18%	8%	17%	23%	33%
Have drawn upon published Cyber Essentials guidance/tools to strengthen our organisation's own cyber security	13%	10%	8%	20%	19%
Aware that our organisation meets all of the Cyber Essentials technical controls without being officially certified	12%	11%	15%	10%	9%
Have drawn upon published Cyber Essentials guidance/tools to help strengthen the cyber security of organisations we work with, including suppliers	3%	3%	2%	3%	5%
Other	3%	4%	4%	3%	3%

Responses self-classified as 'other' include: Assisting client in becoming Cyber Essentials certified, completing an internal assessment of cyber security, considering becoming Cyber Essentials certified, consulting with external IT support for advice, installing other antivirus software.

6.3 Embedding good practice across the organisation

Cyber Essentials appears to be acting as an important vehicle to scheme users putting in place a more holistic approach to being cyber resilient.

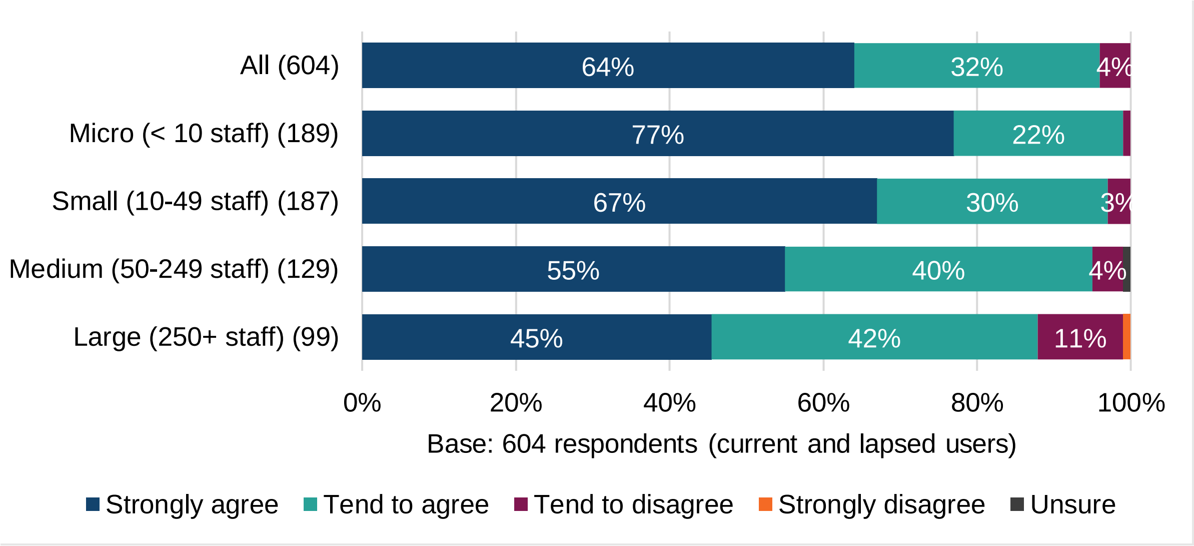
Based on data from the Cyber Security Longitudinal Survey: Wave 2, organisations adhering to one or more cyber security schemes and standards are more likely to say that their board integrates cyber risk considerations into wider business areas, with this being the case among 66% of Cyber Essentials users and 69% of organisations with ISO 27001. On a separate point, three in ten very large businesses with 500+ employees (31%) said that they include cyber security in their annual reports, even more so among those certified to CE Plus (39%) or ISO 27001 (30%).

Analysis undertaken on the Cyber Security Breaches Survey 2023 found that, among businesses that use Cyber Essentials, their board is more likely to have conducted training or an awareness session for cyber security (59%) compared to businesses that do not use Cyber Essentials (15%). Similarly, they are more likely to have a Formal Incident Response plan in place (66% versus 18%).

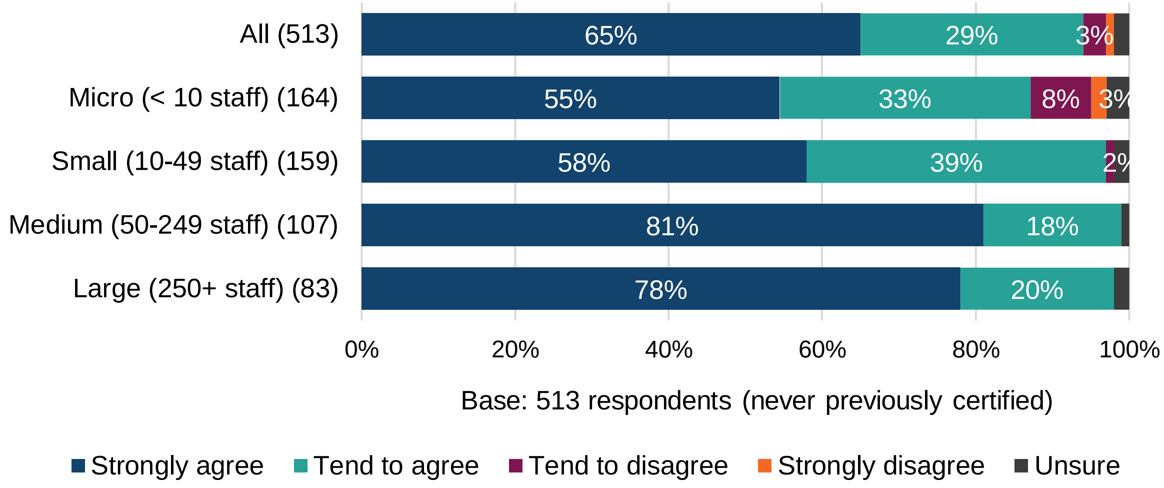
To examine this area in more detail, all organisations surveyed for this evaluation were asked the extent to which they agree or disagree that their whole organisation takes cyber security seriously (Figure 16).

Figure 16 Extent of agreement that the whole organisation takes cyber security seriously (by size-band)

Current and lapsed Cyber Essentials users



Organisations that had never obtained Cyber Essentials



Most Cyber Essentials users (96%) agree that their organisation takes cyber security seriously. Perhaps surprisingly, the proportion is similarly high (94%) among organisations that had never obtained Cyber Essentials.

Again, this brings up the likely issue of overconfidence bias among the latter group. Building on the findings presented in section 5.1 of prior cyber security weaknesses or gaps coming to light upon becoming Cyber Essentials certified, this suggests that organisations that had never obtained the scheme may not be as well informed, with possible complacency.

It is noteworthy from the above charts that the proportion of micro organisations agreeing that their whole organisation takes cyber security seriously is significantly higher among current and lapsed users than those who had never obtained Cyber Essentials. This suggests that the scheme may have had a key enabling role in helping micro organisations to improve their awareness, understanding and attitudes towards cyber security – especially in the absence of any other adopted schemes and standards.

Also, in relation to the above charts, the proportion of medium and large organisations strongly agreeing that their whole organisation takes cyber security seriously is significantly higher among organisations that had never obtained Cyber Essentials than scheme users. Further research would be needed to explore this more fully, but possible reasons could be:

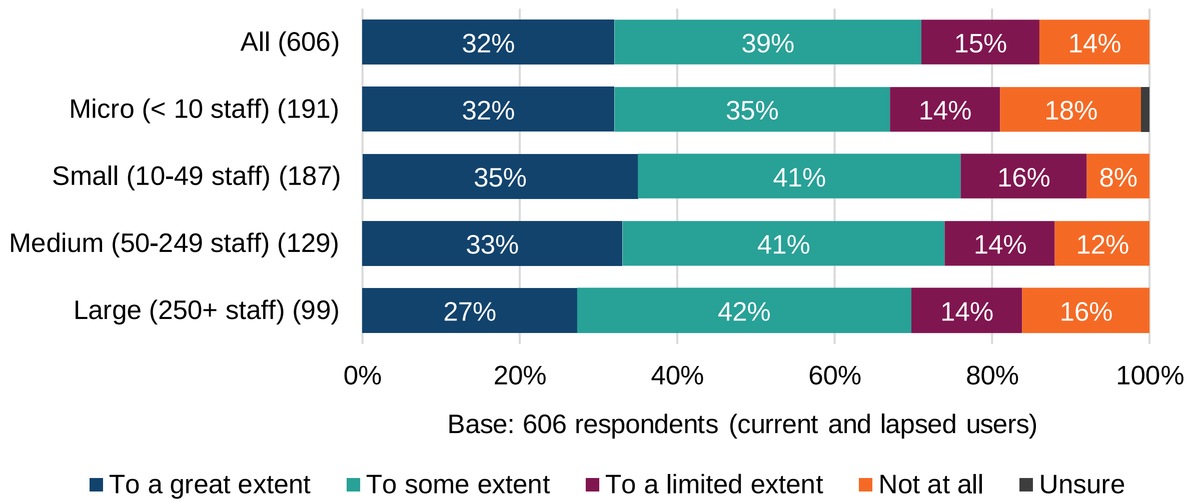
- An element of overconfidence bias at play among these larger organisations, including an assumption that their senior management is fully up to speed
- A perception that they already have robust cyber security risk management arrangements in place

Among scheme users, the proportion of micro and small organisations strongly agreeing is significantly higher than medium and large organisations. This could be the case for example where smaller organisational structures make it easier to cascade messaging in relation to cyber security procedures, actions and behaviours.

Direct influence of Cyber Essentials on how seriously organisations take cyber security

Building on the previous question, scheme users were then asked the extent to which they agree or disagree that Cyber Essentials has directly strengthened how seriously their organisation takes cyber security (Figure 17).

Figure 17 Extent to which Cyber Essentials has strengthened how seriously the whole organisation takes cyber security (current and lapsed users by size-band)



Almost three quarters (71%) agree that the scheme has directly strengthened the seriousness of their approach, with a similar pattern by size-band. This provides further evidence of the scheme's impact beyond the technical controls, expanded on below.

The remainder of this section explores the various ways that organisations have embedded a more holistic approach to cyber security.

A culture of shared cyber responsibility

Figure 17, above provides an early indication that Cyber Essentials could be encouraging organisations to adopt a more holistic approach to being cyber secure, explored more fully through the qualitative follow-up interviews.

For example, most scheme users interviewed following the survey described how becoming Cyber Essentials certified, including changes to processes, protocols and behaviours, has contributed to a more collective sense of responsibility for cyber security within their organisation.

This includes embedding the mindset that everyone has a degree of responsibility for their organisation being cyber secure. One interviewee mentioned that, owing to this increased understanding, staff have become more "vigilant" to activity that could lead to a potential cyber attack, such as individual email addresses appearing on their organisation's website.

Some organisations described how they are now far more proactive in discussing cyber risks internally, with greater and more frequent communications on the subject. One organisation mentioned that their IT team no longer works in a "siloed fashion" and is much more involved with other teams in helping them to understand not only what changes are being put in place, but why they are put in place. This is especially important given organisation-wide challenges that can occur in adapting to change (explored more fully in chapter 5 of the process evaluation).

> "Cyber Essentials has prompted us to put some operational processes in place to almost continually review the way in which we implement and document our cyber security. We make sure that all our staff understand the importance of cyber security and their responsibilities in helping to keep the company secure."
>
> **Private business, micro employer**

An action taken by some organisations after becoming Cyber Essentials certified involves subscribing to cyber security online learning courses to help staff members better understand what they can do to ensure their organisation is cyber secure, including the pitfalls to look out for and why certain processes are essential

6.4 Negative or unforeseen consequences

The Cyber Essentials scheme process evaluation (section 5.5.) examined how some of the largest and smallest organisations were found to face quite different obstacles to meeting the technical controls.

For the largest, the technical controls can prove difficult to implement across a broad network, especially where legacy hardware and software is prevalent. This takes time, considerable expense and the will to instigate changes. For the smallest, meeting the technical controls is a particular challenge given the perceived cost, time and expertise required to do so – especially where these organisations lack a dedicated IT resource or do not have a third-party IT consultancy in place.

Among Cyber Essentials users interviewed as part of this impact evaluation, the most common frustration is the financial cost of implementing changes required to become certified. That said, one user noted that the cost of a sophisticated cyber attack could be far greater.

Several others expressed that the burden of recertifying each year appears to be increasingly difficult. This may be due to the technical controls being updated to keep up with the changing threat environment.

Disagreement that Cyber Essentials stimulates a more serious approach to cyber security

Four interviewed organisations do not believe the scheme has increased how seriously they take cyber security. Their reasons are summarised as follows:

- Existing security measures within their organisation are already perceived to be more sophisticated than those forming part of the Cyber Essentials technical controls

- At CE (standard) level, self-assessment without external validation of security practices risks “devaluing” how seriously organisations take it

- The scheme is more of a “tick-box” exercise to enable them to win contracts

- Other cyber security schemes are perceived as more valuable, especially in an international operating context, for example ISO 27001

7. Strengthening of Assurance Mechanisms

This chapter examines Cyber Essentials as a supply chain assurance tool, including how organisations make use of the scheme with potential suppliers and partners, what support (if any) they provide to suppliers as part of the cyber security due diligence process, and perceptions of how their own clients and customers value Cyber Essentials certification.

It then looks in more detail at due diligence processes. This includes the extent to which time is saved when suppliers are Cyber Essentials certified – both on the part of clients conducting the due diligence and the suppliers themselves. This is followed by a brief look at the extent to which scheme users have noticed a reduction in cyber incidents since using Cyber Essentials to manage supply chain cyber risk.

Key findings summary

Firstly, Cyber Essentials take-up is principally being driven as a result of the scheme being mandated in government contracts. However, the scheme is encouraging organisations to consider cyber security more overtly as part of their purchasing decisions. A minority of surveyed organisations currently mandate certification among their suppliers, with even more planning to do so in the future. Most Cyber Essentials users say they are more likely to choose suppliers that are also certified than those without certification, as well as having greater confidence working with certified suppliers.

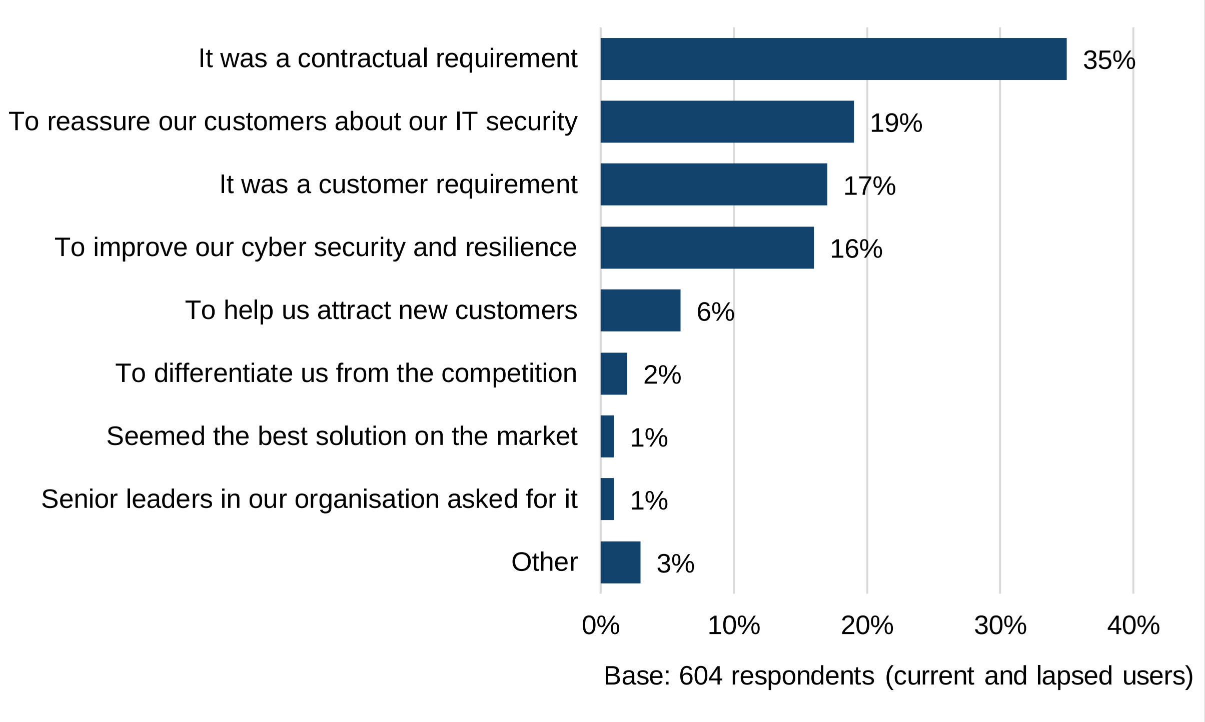
Cyber Essentials is also leading to time-savings in cyber security due diligence undertaken on potential suppliers, meaning this time can be used by organisations in other ways. Similarly, most surveyed organisations in the capacity of suppliers, report that being Cyber Essentials certified helps to reduce the due diligence burden placed upon them by their own clients/customers.

7.1 Mandating Cyber Essentials in contracts

Cyber Essentials has become mandatory for all suppliers of UK government contracts involving the handling of sensitive and personal information and provision of certain technical products and services.

This requirement appears to be strongly influencing scheme take-up, with ‘a contractual requirement’ being the single main reason mentioned by 35% of Cyber Essentials users for first becoming certified (Figure 18).

Figure 18 Single main reason for first becoming Cyber Essentials certified



Base: 604 respondents (current and lapsed users)

Responses self-classified as 'other' include: Nature of the business (cyber security company), insurance company requirement, to be able to audit the company, trade body requirement, wanting to lead by example, wanting to become a Certification Body.

Looking across the four size-bands, 'a contractual requirement' is the single main reason for first taking up Cyber Essentials in each sub-group (Table 16).

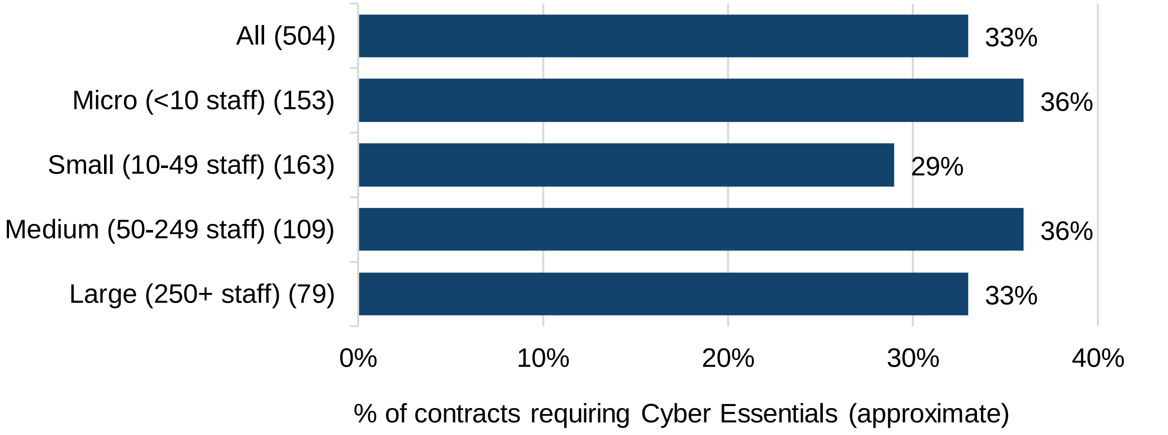
Table 16 Single main reason for first becoming Cyber Essentials-certified (by size-band)

	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base					
It was a contract requirement	35%	35%	34%	35%	38%
To reassure customers about our IT security	19%	21%	20%	15%	14%
It was a customer requirement	17%	18%	16%	13%	19%
To improve our cyber security and resilience	16%	9%	19%	20%	19%
To help us attract new customers	6%	8%	3%	10%	3%
To differentiate us from the competition	2%	3%	3%	1%	-
Seemed the best solution on the market	1%	-	1%	2%	1%
Senior leaders in our organisation asked for it	1%	1%	1%	1%	-
To obtain the packaged cyber liability insurance	-	1%	-	-	-
Was the cheapest solution on the market	-	1%	-	-	-
Previously suffered a cyber security incident	-	-	-	-	-
To plug a gap in PII cover	-	-	1%	-	1%
Other	3%	3%	1%	3%	4%

Proportion of contracts that are mandated

Cyber Essentials users report that, on average, a third (33%) of contracts they entered into over the preceding 12 months required their organisation to be Cyber Essentials certified (Figure 19). This positions the scheme as important in the market as a competitive differentiator.

Figure 19 Proportion of contracts entered into over the past 12 months that required Cyber Essentials (current and lapsed users by size-band)



Perceived prevalence of the scheme beyond public sector contracts

Several strategic stakeholders (comprising government representatives and key industry organisations) made the point that – outside of public sector contracts – Cyber Essentials does not tend to be “widely talked about”, suggesting that it would need to be more actively promoted across the private and third sector supply chains.

A small number of Cyber Essentials users interviewed following the survey would like to see greater uptake of Cyber Essentials. They feel that more needs to be done to make that happen and improve the cyber resilience of the UK economy, such as making the scheme mandatory in a wider set of situations.

> “Cyber security is becoming more important and the government approach of asking nicely is not working. Organisations only respond only when they are told they must comply, i.e. when it is mandated.
>
> **Private business, micro employer**

7.2 How Cyber Essentials is deployed as a supply chain assurance tool

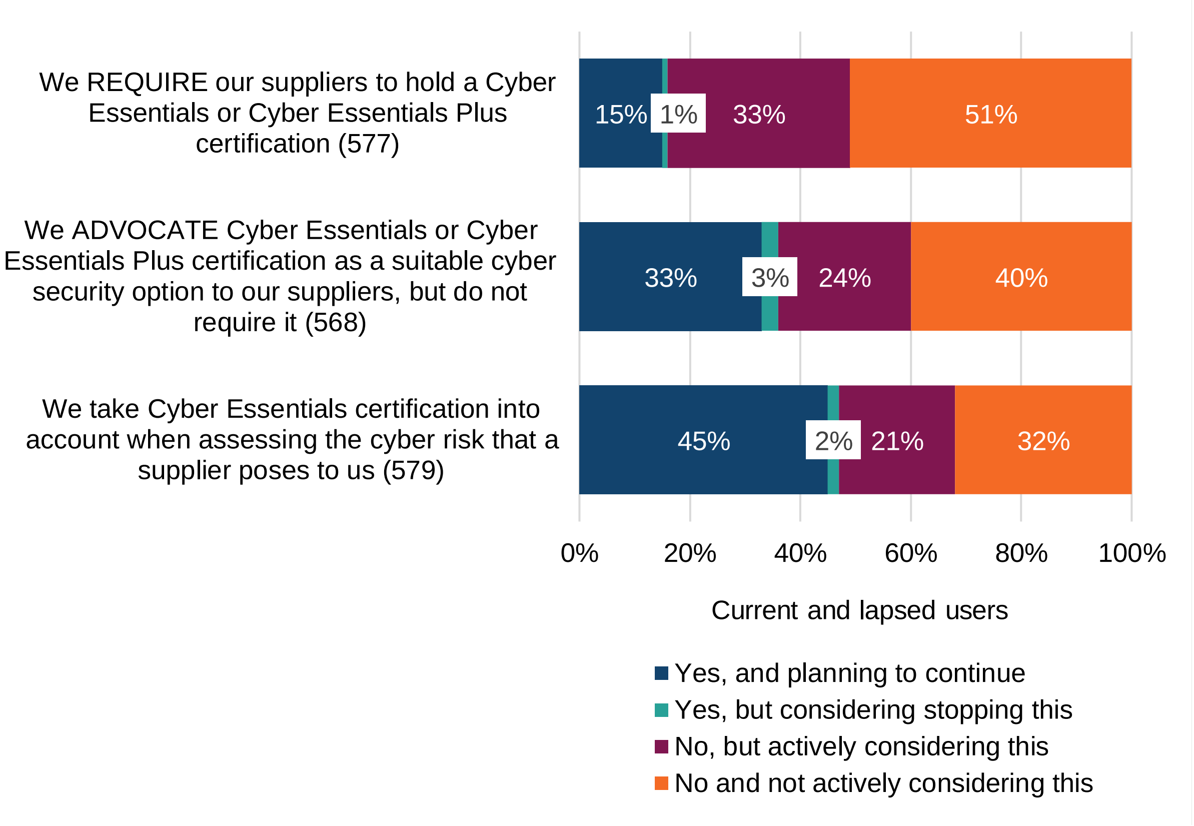
Surveyed Cyber Essentials users were asked three questions relating to the role of the scheme as a supply chain assurance tool – whether they: i) require it from their suppliers; ii) advocate it to their suppliers; and iii) take it into account when assessing the risk that a supplier poses to them (Figure 20).

It should be noted that, when analysed independently, relatively high proportions appear not to undertake these steps and are not planning to do so in the future (51%, 40% and 32% respectively).

However, from a base of 564 organisations giving an answer to all three questions, the proportion is lower, i.e. 152 (27%) neither require Cyber Essentials, advocate it, or take it into account when assessing the cyber security risks of suppliers, nor are they actively considering doing so in the future. In other words, the majority is taking at least one of these steps and/or considering taking further steps in the future.

Each of these three questions are analysed in detail (and in turn) below the chart.

Figure 20 How Cyber Essentials is used as a supply chain assurance tool (current and lapsed users)



Requiring Cyber Essentials

Firstly, 15% of scheme users currently require their suppliers to hold Cyber Essentials certification and plan to continue doing so, while only 1% of scheme users currently require it and are considering stopping this. This indicates that the majority of those currently requiring it are content to continue doing so to help manage supply chain cyber risk. This provides further evidence of confidence in the scheme among those that use it.

A third of all surveyed scheme users (33%) are actively considering mandating their suppliers to have Cyber Essentials in the future. This suggests that the scheme has potential to gain traction by embedding it in third party requirements, potentially meaning more organisations becoming certified and contributing to stronger cyber resilience across the UK economy.

Reasons given for uses actively considering mandating suppliers to become Cyber Essentials certified include:

- Ensuring a baseline level of security among their suppliers
- Offering peace of mind for their own organisation
- Helping to strengthen overall supply chain assurance

- Instilling confidence that suppliers are committed to cyber security and are taking it seriously

The main reason provided by the 1% or scheme users that are considering removing the requirement for suppliers to be Cyber Essentials certified is a concern about the cost impact on the part of the supplier.

Advocating Cyber Essentials

At present, it is more common for organisations to "advocate" (i.e. rather than mandate) Cyber Essentials from their suppliers, with 33% already doing so and planning to continue, and just under a quarter (24%) planning to do so in the future.

Taking Cyber Essentials into account when assessing cyber risks of supplier

The picture is mixed in terms of whether organisations take Cyber Essentials into account when assessing the cyber risk that a supplier poses to them. Some 45% already do this and plan to continue, signalling that Cyber Essentials could be acting as a useful benchmark in supply chain assurance processes. A further fifth (21%) plan to do this in the future and only 2% are planning to stop this.

Size-band analysis of Figure 20 is presented in Table 17.

Table 17 How Cyber Essentials is used as a supply chain assurance tool (current and lapsed users (by size-band)

We REQUIRE our suppliers to hold a Cyber Essentials or Cyber Essentials Plus certification

	All (577)	**Micro (< 10 staff) (183)**	**Small (10-49 staff) (173)**	**Medium (50-249 staff) (125)**	**Large (250+ staff) (96)**
Yes, and planning to continue	15%	13%	13%	18%	18%
Yes, but considering stopping this	1%	1%	1%	2%	-
No, but actively considering this	33%	30%	32%	32%	43%
No and not actively considering this	51%	56%	54%	48%	39%

We ADVOCATE Cyber Essentials or Cyber Essentials Plus certification as a suitable cyber security option to our suppliers, but do not require it

	All (568)	**Micro (< 10 staff) (183)**	**Small (10-49 staff) (169)**	**Medium (50-249 staff) (122)**	**Large (250+ staff) (94)**
Yes, and planning to continue	33%	33%	34%	30%	37%
Yes, but considering stopping this	3%	3%	1%	5%	1%
No, but actively considering this	24%	18%	24%	27%	32%
No and not actively considering this	40%	45%	40%	39%	30%

We take Cyber Essentials certification into account when assessing the cyber risk that a supplier poses to us

	All (579)	Micro (< 10 staff) (183)	Small (10-49 staff) (175)	Medium (50-249 staff) (125)	Large (250+ staff) (96)
Yes, and planning to continue	45%	38%	41%	50%	58%
Yes, but considering stopping this	2%	3%	1%	3%	3%
No, but actively considering this	21%	17%	26%	18%	20%
No and not actively considering this	32%	42%	33%	28%	19%

Strategic stakeholders suggested that smaller organisations may be less likely to use Cyber Essentials as a supply chain assurance tool for the following main reasons:

- Mico organisations are potentially more cost driven than cyber security driven
- Where smaller organisations especially using suppliers that are much larger than they are, they may be less inclined to question their cyber risk or could think such a request would not be taken seriously
- Smaller organisations might be concerned that mandating the scheme could have a negative effect on their ability to do business with their suppliers
- Smaller organisations lack the time and resources to undertake appropriate due diligence

The proportion of medium and large organisations that currently take (and plan to continue taking) Cyber Essentials certification into account when assessing the cyber risk that a supplier poses, is significantly higher than that of micro organisations. There could be several factors driving this, for example:

- Larger organisations are potentially more dependent on complex supply chains, making cyber security in those supply chains important
- Larger organisations may be better placed to have the systems and resources to be able to assess cyber risk

Provision of support for supply chain businesses

Cyber Essentials users interviewed following the survey were asked if they provide any support for supply chain businesses that they require to have certification but do not have it already. Most said that they do not have the time or resources to do this. One organisation mentioned that they would expect a supplier to go through the same process that they did, since “it is not too onerous.” Another mentioned that they offer guidance in the form of a supplier checklist.

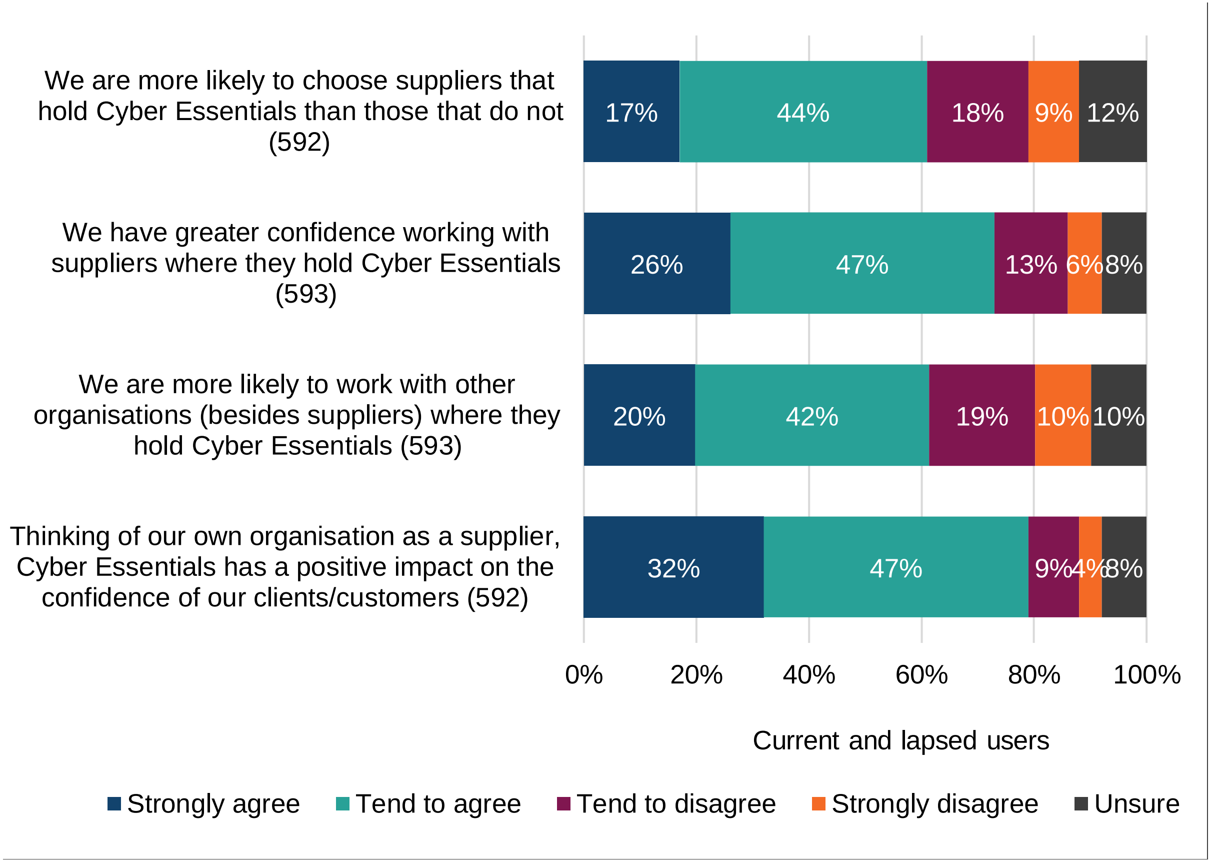
> "It depends on who the supplier is. For large organisations responding to open tenders, we don't offer support. When we deal with smaller suppliers or individuals, we will help them, for example by pointing them to IASME or our own Certification Body. We explain why they should adopt Cyber Essentials and why it would be useful for them."
>
> **Non-governmental Organisation, large employer**

7.3 Impact on supply chains and collaboration

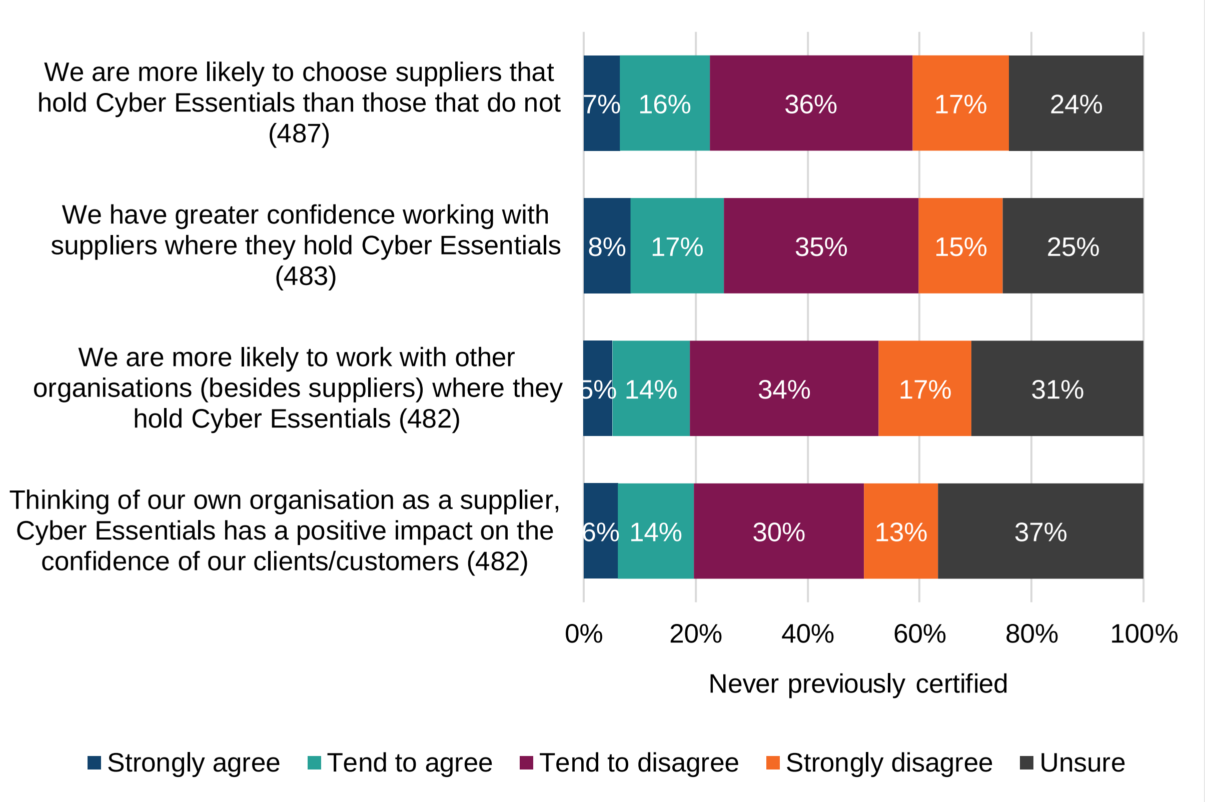
All surveyed organisations were asked to what extent they agree or disagree that Cyber Essentials influences business-to-business relationships in specific ways. The results are shown in Figure 21 and discussed in more detail below.

Figure 21 Influence of Cyber Essentials on supply chains and collaboration

Current and lapsed Cyber Essentials users



Organisations that had never obtained Cyber Essentials



Firstly, a general comparison between the two charts above indicates that Cyber Essentials users place greater value on the scheme when looking to work with suppliers and other organisations, and that they potentially place greater importance on the cyber security of their suppliers.

Analysis of each of the four statements from the above chart are set out in turn, below.

Influence of the scheme on choice of suppliers and confidence working with suppliers

Most Cyber Essentials users (61%) agree that they are more likely to choose suppliers that use the scheme than those that do not; furthermore, just under three quarters (73%) agree that they have greater confidence working with suppliers that use Cyber Essentials. This suggests that scheme users place value on the scheme itself. Having gone through the certification process and being clear on what the scheme does and the benefits it can bring, they may feel more compelled to want to ask the same of others.

Among organisations that had never obtained Cyber Essentials, it is noteworthy that more than a fifth (23%) of these organisations are more likely to choose suppliers that hold Cyber Essentials and a quarter (25%) have greater confidence working with suppliers that hold Cyber Essentials. This points to the scheme having a positive effect on supply chain assurance decision-making beyond certified organisations alone, even if – for whatever reason – these organisations choose not to become certified.

Influence of the scheme on working with other (non-supplier) organisations

Most Cyber Essentials users (62%) are more likely to work with other organisations (i.e. besides suppliers) where they use Cyber Essentials This is in contrast with just 19% of organisations that had never obtained certification.

Influence of the scheme on the perceived confidence of clients and customers

Thinking about their own organisations as suppliers, most Cyber Essentials users (79%) believe that the scheme has a positive impact on the confidence of their clients and customers. A fifth (20%) of organisations that had never obtained certification feel the same, suggesting that their clients may have expressed an interest in seeing it, or even mandated it in some cases. Again, similar results were reported by Britain Thinks, with the vast majority (83%) of Cyber Essentials users reporting that certification had a positive impact on the confidence of organisations' customers and investors.

Further insights on the role of the technical controls in mitigating risks within the supply chain

Over half of Cyber Essentials users interviewed following the survey mentioned that the scheme's technical controls have prompted them to increase security checks within their supply chain, for example implementing policies and procedures that their suppliers must adhere to. Many described how sharing of data within their supply chains is now subject to more strict controls, such as through the use of stable firewalls, suppliers needing to have malware protection in place, and using multi-factor authentication.

"We have been through it ourselves. We know what the baseline is and what position we want suppliers to be in before handling our data."

Registered charity, medium employer

Some organisations are concerned that the self-assessment associated with the standard CE level is not robust enough to ensure that adequate privacy and security practices are in place and are more reassured by CE Plus. Others simply don't deem it necessary to subject their suppliers to that degree of scrutiny.

"It is a cost that is unnecessary as long as the supplier has necessary protection."

Private business, micro employer

"A lot of our suppliers are goods or software only, no data are hosted externally."

Private business, small employer

7.4 Cyber security due diligence

Several strategic stakeholders interviewed as part of the evaluation are confident that, where suppliers are Cyber Essentials certified, this can reduce the burden placed upon them when responding to cyber security due diligence questionnaires or other processes. One industry stakeholder mentioned that Cyber Essentials certification was not currently reflected in their due diligence processes of suppliers, but did accept that it would likely lead to fewer cyber security questions being asked of them in the future.

Other stakeholders were less certain about whether Cyber Essentials would reduce due diligence. One made the point that – hypothetically – some organisations may want to undertake security checks that go beyond the five Cyber Essentials technical controls. This was put down to the prescriptive (rather than risk-based) nature of the technical controls, meaning that some organisations might want to enforce more complex protocols based on the risk environment and context.

> “We must remember that Cyber Essentials isn’t a silver bullet. It is a tool, but it isn’t the only tool. And in some circumstances, it may not be the right tool.”
>
> **Strategic stakeholder**

It is also important to bear in mind that organisations may have developed their own cyber security questionnaires or other forms of due diligence which they ask of all organisations irrespective of whether or not they are Cyber Essentials certified. This could be due to a lack of awareness about what the Cyber Essentials technical controls measure, meaning that due diligence is not always proportioned for certified suppliers.

Prevalence and scale of cyber security due diligence

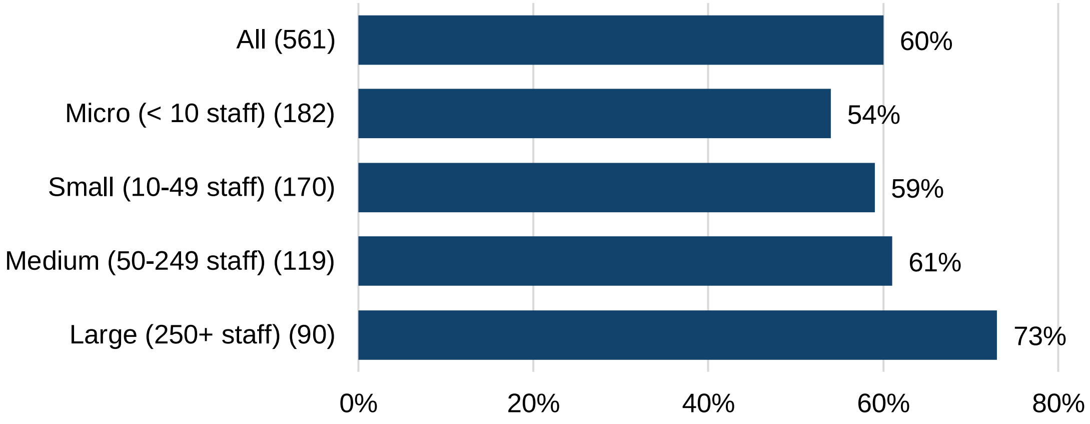
The Cyber Security Breaches Survey 2023 found that one in ten businesses took steps to formally review the risks posed by their immediate suppliers (13%). This was higher among medium businesses (27%) and large businesses (55%). Qualitative data from the Breaches survey suggests that where organisations receive messaging around supply chain risks from bodies such as the NCSC, or have the topic raised in audits, this helps to encourage them to take action in this area.

To indicate whether Cyber Essentials may have a role in influencing organisations to undertake cyber security due diligence among their suppliers, this evaluation asked scheme users about the time they spend on such activities.

Whilst the questions asked in this evaluation, along with the audience, are not directly comparable with the Breaches survey, the results point to Cyber Essentials users paying greater attention to supplier due diligence.

Most (60%) of current and lapsed users report spending any time at all conducting cyber security due diligence on potential suppliers (Figure 22).

Figure 22 Proportion of current and lapsed users spending time on supplier due diligence (by size-band)



Base: 561 respondents (current and lapsed users)

Of those undertaking any due diligence:

- Just under half (48%) report saving time where a potential supplier is CE certified
- More than half (59%) report saving time where a potential supplier is CE Plus certified

Time savings are summarised in Table 18. In summary, Cyber Essentials users report saving an average of:

- 22% of their time (58 minutes) on cyber security due diligence for each potential supplier that is CE certified
- 32% of their time (84 minutes) for each potential supplier that is CE Plus certified

It is important to note that all data are based on broad estimates, which may be subject to under or over estimation.

Table 18 Time saved in cyber security due diligence where potential suppliers are Cyber Essentials certified

Size-band	Base	Average minutes spent on cyber security due diligence per potential supplier NOT Cyber Essentials certified See Note 1	Percentage of time saved when potential supplier is Cyber Essentials certified per level		Time saved
All	287	264 minutes	CE	22%	58 minutes
			CE Plus	32%	84 minutes
Micro (< 10 staff)	84	216 minutes	CE	31%	67 minutes
			CE Plus	36%	78 minutes
Small (10-49 staff)	83	234 minutes	CE	21%	49 minutes
			CE Plus	32%	75 minutes
Medium (50-249 staff)	62	324 minutes	CE	18%	58 minutes
			CE Plus	33%	107 minutes
Large (250+ staff)	58	312 minutes	CE	16%	50 minutes
			CE Plus	25%	78 minutes

Note 1: The survey questionnaire asked for time spent on due diligence in hours, which was subsequently converted to minutes. Obvious outlier responses were removed from the dataset, although the numbers should be **treated with caution** as they cannot not be independently verified.

Nature of due diligence undertaken

According to several Cyber Essentials users interviewed following the survey, the most frequently mentioned form of due diligence is a checklist or questionnaire created for potential suppliers. Others carry out background checks on suppliers' history, ascertaining how often they update software, if they implement multi-factor authentication, how they store data, and whether they have certain policies and procedures in place to aid compliance, for example with UK GDPR.

A minority of organisations mentioned that their due diligence processes tend to be more closely aligned with ISO 27001 protocols. One organisation carries out a test exercise on suppliers that are due to hold large amounts of their data, checking systems for any vulnerabilities.

The thoroughness of supplier due diligence is often dependent on the type of supplier. For example, one organisation mentioned how they work with both a PR agency and an IT company, with the latter being subject to greater scrutiny due to holding more sensitive data.

"We recently launched a platform to review third party risk, and it has a question set that covers user awareness training, background checks, joins, leavers, process access control, encryption, live vulnerabilities patching, data location and physical security."

Private business, large employer

When asked whether having Cyber Essentials has changed their approach to due diligence, several organisations claimed that it has, bringing benefits.

"Cyber Essentials is great for normalising the level of security – it helps us to understand where a potential supplier is at with their cyber security processes."

Private business, small employer

One organisation said they look for CE Plus certification as a minimum, since an externally validated level of security provides them with more confidence and assurance, in turn reducing the due diligence burden via the number of questions they need to ask.

A minority of interviewees claimed that having Cyber Essentials makes no difference to the rigour of their supplier due diligence. For one organisation, the self-assessment aspect of the scheme does not provide them with confidence that suppliers are doing what they say they are doing or that they would take appropriate action in the event of a data breach.

Another mentioned having devised a platform to review third party cyber risk:

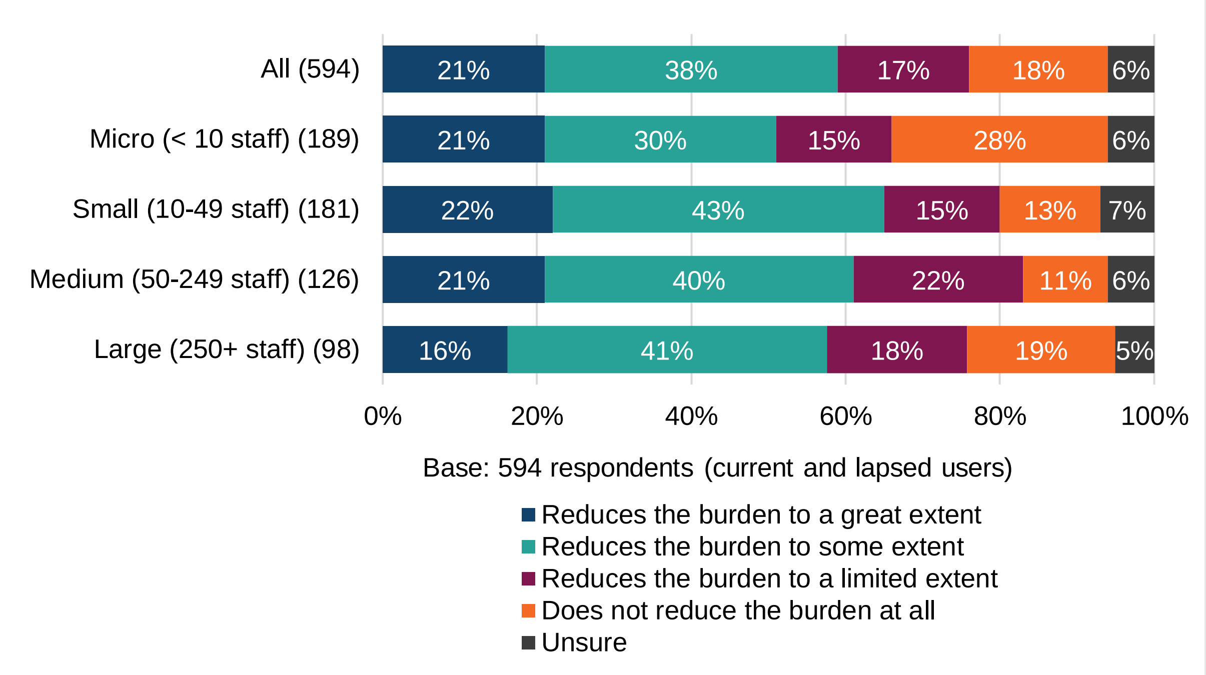
"[Our platform] has a question set that covers user awareness training, background checks, joins, levers, process access control, encryption, live vulnerabilities patching, data location, physical security. It's more aligned with ISO27001, which allows for flexibility whereas Cyber Essentials is very black and white in some respects."

Private business, large employer

Suppliers' experience of meeting due diligence requirements

Cyber Essentials users, in their capacity as suppliers, were asked to what extent – if at all – the scheme reduces the burden placed upon them to demonstrate cyber security credentials to their own clients and customers (Figure 23).

Figure 23 Extent to which Cyber Essentials reduces the burden to demonstrate cyber security credentials to customers



More than three quarters (76%) report that being certified helps to reduce the burden. This affirms that being Cyber Essentials certified results in time or resource savings, thus creating efficiencies in the due diligence process. There is little difference between the size-bands.

Suppliers' views on how Cyber Essentials reduces the due diligence burden

Most Cyber Essentials users interviewed following the survey expanded on how Cyber Essentials certification helps to reduce the administrative burden when working with new clients and customers. This can be particularly true for those with CE Plus, with one organisation mentioning that this demonstrates having been externally assessed to a recognised standard.

Others value the framework used by Cyber Essentials, which can make it easier to signpost to particular credentials, especially during contract negotiations. Several interviewees value the role of certification in giving clients peace of mind and acting as a stamp of approval that they are taking cyber security seriously.

> "It frees up time, whereas I might otherwise have had to fill in a questionnaire taking up to four hours to complete. That time can now be spent on other things that are more important."
>
> **Non-governmental Organisation, large employer**

For a minority, Cyber Essentials is not reportedly reducing the burden placed on their organisation, with key reasons being:

- Cyber security questionnaires are no shorter, despite their organisation being Cyber Essentials certified

- Outside of public sector contracts, clients do not ask for Cyber Essentials, meaning that due diligence processes are the same whether suppliers are certified or not
- Some clients and customers still want to see evidence of meeting other standards, such as ISO 27001, especially overseas clients that may not have heard of Cyber Essentials
- Becoming Cyber Essentials certified can actually increase the due diligence burden, due to having to demonstrate conformity to a wider range of security measures

> “Cyber Essentials isn't normally part of the conversation with our customers. Being certified doesn't reduce the time it takes to complete security check – it just increases the scope.”
>
> **Private business, medium employer**

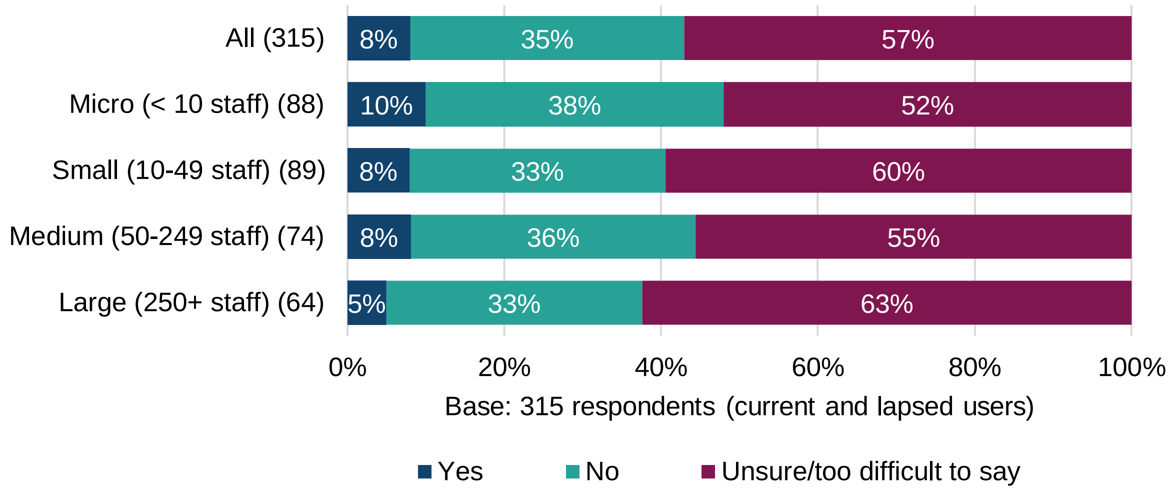
> “When we receive a due diligence questionnaire to complete, not a single one says ‘Have you got Cyber Essentials? If so, you don’t need to answer the rest of the questions.’ It may buy some goodwill with some customers, but others are still going to ask more.”
>
> **Private business, large employer**

7.5 Supply chain incident reduction

Finally in this chapter, a small minority of Cyber Essentials users (8%) say they have noticed a reduction in cyber incidents since using Cyber Essentials to manage supply chain cyber risk. More than a third (35%) have not noticed any reduction, and the majority (57%) feel it is too difficult to say (Figure 24).

These results illustrate how difficult it can be for organisations to measure cyber incidents, or indeed how to define them, let alone be able to reasonably determine whether there has been a notable reduction since using Cyber Essentials as part of supply chain risk management.

Figure 24 Whether organisations have noticed a reduction in cyber incidents since using Cyber Essentials to manage supply chain cyber risk (current and lapsed users by size-band)



8. Creation of Wider Value

This chapter explores other ways Cyber Essentials adds value to organisations that use it. In particular, it examines statistics and perceptions relating to cyber liability insurance, views on how the scheme contributes to organisations' market competitiveness, and the extent to which Certification Bodies are providing support.

Key findings summary

The Cyber Essentials scheme is encouraging strong growth in the cyber security sector, with increasing numbers of Certification Bodies and assessors positioned to provide cyber security support. Qualitative interviews reveal that Certification Bodies are generally providing useful guidance and advice.

The NCSC's Annual Review 2023 suggests that 80% fewer cyber insurance claims are made when Cyber Essentials is in place (based on 2022 claims data). This is compared with organisations that have the same insurance policy and do not have Cyber Essentials certification. This provides an indication of the scheme's efficacy.

Finally, most Cyber Essentials users (69%) believe that the scheme has increased their market competitiveness.

8.1 Growth in the cyber security sector

IASME has accredited over 340 Certification Bodies responsible for delivering the Cyber Essentials scheme through being trained and licensed to certify organisations. These companies comprise over 900 individual assessors who also have a role to provide information and guidance to the organisations they work with in the interests of encouraging better cyber security and reaching the scheme's baseline standard.

The numbers of Certification Bodies and assessors continues to grow, which represents strong impact of the scheme in terms of the scale of support and geographical coverage. This means that organisations have an increasingly strong external support network for cyber security should they need it.

Over a third of interviewed businesses mentioned that their Certification Body provides useful guidance and advice on a regular basis. They remarked that advisors provide support to help them attain certification and become better protected, therefore adding value to their organisation rather than simply acting as an intermediary to make a pass or fail assessment. Some said that Certification Bodies are good at answering any pressing questions, are always contactable, and produce helpful assessments and reports.

> "With CE Plus there are greater complexities, but both our advisors have been fantastic. We've recommended them to other organisations, including some of our partners.
>
> **Non-governmental Organisation, micro employer**

Some stated they have had little to no contact with their Certification Body. This is mostly in cases where their organisation has an in-house cyber security team or works with another specialist consultant. Others view the Certification Body as a “means to an end” in attaining certification.

Only a minority of businesses spoke negatively of their Certification Body, such as not providing timely updates on the latest technical controls which one organisation said cost the company a lot of money.

8.2 Cyber liability insurance

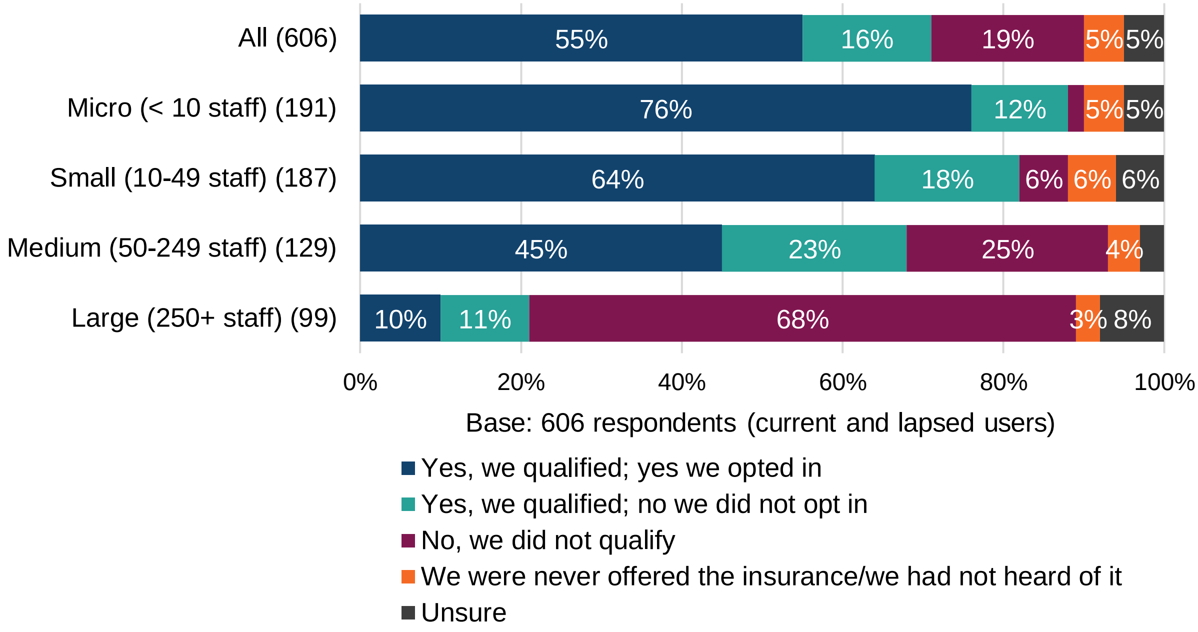
Subject to eligibility, organisations that achieve Cyber Essentials certification via the IASME Consortium or any of their approved certification providers are entitled to cyber liability insurance. Organisations are eligible if their entire organisation is certified, domiciled in the UK, has an annual turnover under £20m, and opts into the insurance. The policy offers £25K of cover, including access to 24-hour legal and technical incident response.

The NCSC’s Annual Review 2023 suggests that 80% fewer cyber insurance claims are made when Cyber Essentials is in place (based on 2022 claims data). This is compared with organisations that have the same insurance policy and do not have Cyber Essentials certification. This provides an indication of the scheme’s efficacy.

Strategic stakeholders interviewed for the evaluation (comprising government representatives and key industry organisations) view the packaged cyber liability insurance as a positive feature of the scheme. One stakeholder added that the insurance could be especially beneficial for smaller organisations that suffer a security breach, since they might not otherwise have the expertise or financial power to recover.

Cyber Essentials users surveyed for this evaluation were asked if their organisation qualified for, and opted in to, taking this insurance as part of their Cyber Essentials certification. More than half (55%) say that they did. Given the eligibility criteria, it is perhaps unsurprising that this decreases by size-band, however, the results point to those taking up the offer now standing to benefit from this additional protection (Figure 25).

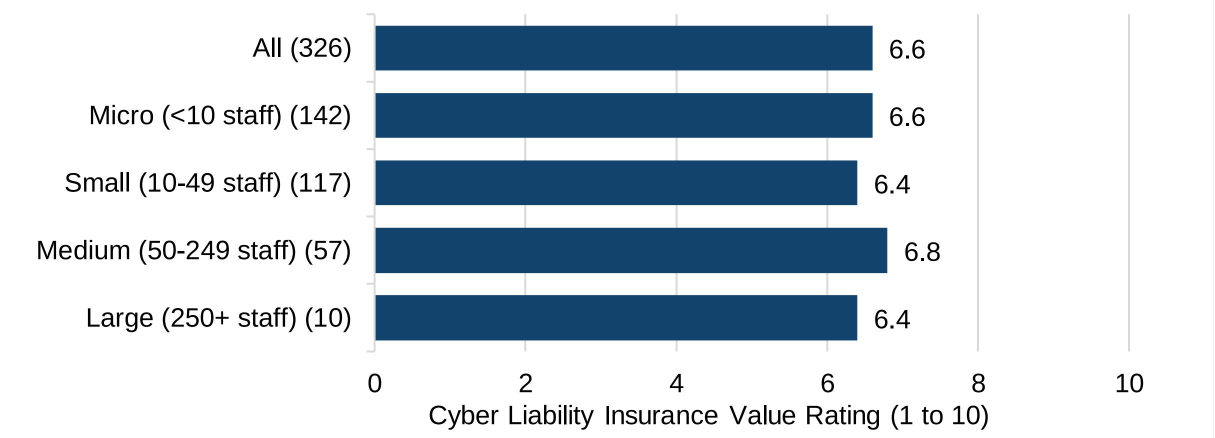
Figure 25 Eligibility and opt-in to packaged cyber liability insurance (current and lapsed users by size band)



Those Cyber Essentials users that qualified and opted in were then asked to rate how valuable they consider the packaged cyber liability insurance, on a scale from 1 'not at all valuable' to 10 'extremely valuable'.

The overall mean rating is 6.6 (mode = 10), indicating that the insurance is considered moderately valuable. It is important to note that ratings could be inversely affected here where organisations have not experienced a cyber attack and thus not had to make use of the insurance. There are no significant differences by size-band (Figure 26).

Figure 26 Value rating of packaged Cyber Liability Insurance



Insured Cyber Essentials users were asked during the follow-up interviews to give a reason for their scores.

For those giving above-average scores, reasons can be summarised as follows:

- It is useful to have an additional layer of dedicated cyber security insurance on top of existing cover

- The insurance comes at no additional cost

- The insurance reassures customers that sufficient cover is in place to help ensure continuity in the face of a cyber attack

- The insurance covers most types of cyber threats

"Cyber security is a serious risk and a serious subject, which is why the insurance is important because hacking and breach techniques are changing and becoming more sophisticated on an almost daily basis."

Private business, micro organisation

Organisations providing a below average rating gave the following reasons:

- The £25,000 indemnity threshold is not viewed as sufficient to cover potential cyber attacks (one organisation estimated the cost of total failure to their systems and claimed the insurance would not be enough to cover expected losses)

- Existing insurance is already in place at a higher level

Several interviewees gave a more arbitrary response, having never had to use the insurance.

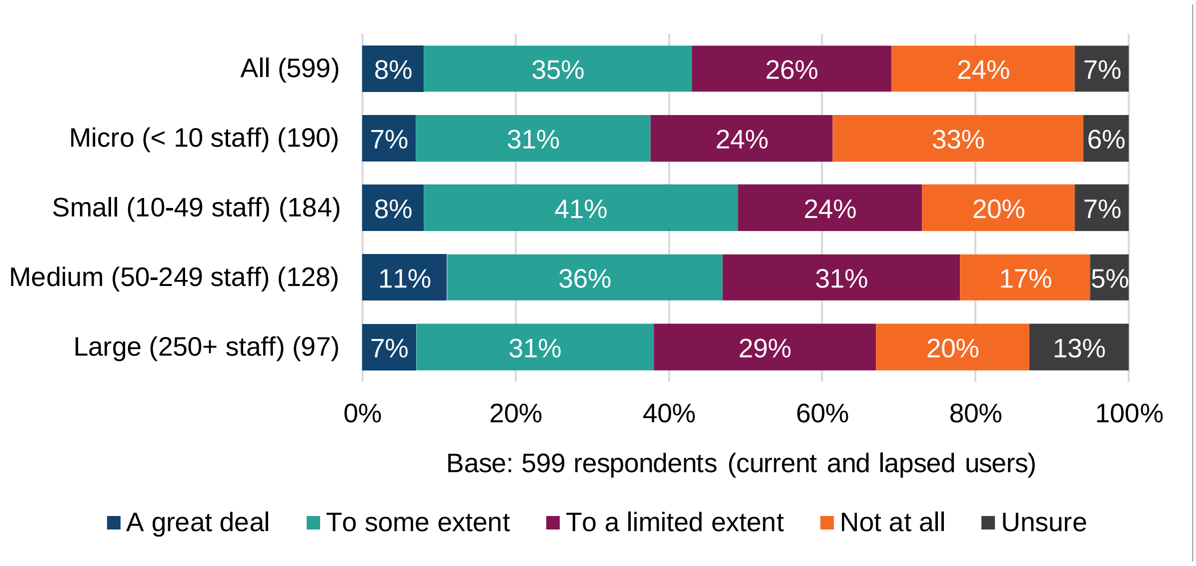
"Until you actually have to deal with an insurance company on a claim, you don't know how good they are."

Private business, small employer

8.3 Market competitiveness

Surveyed Cyber Essentials users were asked the extent to which they believe the scheme has increased market competitiveness (Figure 27).

Figure 27 Extent to which Cyber Essentials has increased market competitiveness (current and lapsed users by size-band)



More than two thirds (69%) believe that the scheme has increased their market competitiveness. The proportion of small and medium organisations that have experienced this is significantly higher than that of micro organisations. This benefit is likely to be prominently felt when seeking to enter into contracts that mandate Cyber Essentials, which could be a more common occurrence among larger organisations.

Cyber Essentials users interviewed following the survey expanded on how the scheme has helped their market competitiveness. This includes certification being perceived as "achievable", which makes the cost-benefits clearer to see, gaining additional credibility since their organisation is taken more seriously, and experiencing increased commercial activity since becoming certified.

"If we look at our local competitors, there are only a couple of other companies that do what we do and are certified as well. I think it adds something else to our credibility as an organisation."

Private business, micro employer

9. Case Studies

The three case studies presented in this chapter offer an in-depth look at the cyber security journey of three organisation. This includes obstacles overcome, how the scheme has positively impacted each organisation, and what their messages would be to other organisations considering becoming certified.

9.1 Cafcass

- **Non-governmental organisation**
- **Large employer (>1,000 staff)**
- **Base: London**

About the organisation

The Children and Family Court Advisory and Support Service (Cafcass) advises family courts in England about the welfare of children and what is in their best interests. It works with almost 144,000 children annually whose future is decided by the family courts by providing a service that prioritises their safety, their voices and their needs.

Steps to becoming Cyber Essentials certified

Cafcass took its first steps to becoming Cyber Essentials certified in 2019 when it began looking at best practice guidance around cyber security to tighten existing arrangements. It also wanted to set a good example to its suppliers.

“We wanted to demonstrate our awareness and our security stance so that when we were requiring Cyber Essentials from our suppliers, it wasn't a one-way street.”

Michael Convey, Senior Architect and Security Manager

Cafcass found the assessor at their certification body to be extremely helpful throughout the initial certification process, advising them on what changes they needed to make. A mock assessment followed, which identified where aspects of cyber security could be strengthened. Cafcass initially gained Cyber Essentials certification in 2020.

“I think having that close relationship with the assessor is key to being successful. For us [each year] it really helps us to understand what we're trying to achieve and why we're trying to do it.”

Michael Convey, Senior Architect and Security Manager

Obstacles overcome

With staff operating across England and most working remotely, the biggest obstacle to Cafcass initially becoming Cyber Essentials certified was building appreciation of the scheme's importance for good security hygiene. Another was changing certain habits, such as ensuring that staff always run the necessary updates and system restarts.

Obtaining buy-in from senior management was aided by Cafcass having a dedicated risk and assurance committee. Others bought in once they understood the benefits of the scheme in making the operating environment safer.

Impact

Cyber Essentials propelled cyber security to the forefront of the organisation and Cafcass sees the scheme as playing a key role in protecting not only staff, but the children and families with whom it works in terms of keeping their information safe.

Cafcass believes that Cyber Essentials has made it more aware of cyber security threats facing the organisation. It also believes that the use of multi factor authentication (MFA) has likely led to a reduction in the number of successful cyber attacks. Furthermore, the use of hardware and software tokens has improved security by preventing unauthorised access to the organisation and its supply chain.

> "We now apply security patches within 14 days of release. This means we haven't been exposed to many of the types of risks that could impact others."
>
> **Michael Convey, Senior Architect and Security Manager**

Cyber Essentials has also reduced the organisation's cyber security burden.

> "It frees up time, whereas I may have had to fill in questionnaires taking up to four hours to complete. That time can now be spent on other things, i.e. the real things that are important."
>
> **Michael Convey, Senior Architect and Security Manager**

Final message

Cafcass' message to other organisations considering becoming Cyber Essentials certified is not to worry about not getting everything right the first time around as it's a journey of continuous improvement.

9.2 Kirbys Solicitors

- **Private business**
- **Small employer (10-49 staff)**
- **Base: Yorkshire and the Humber**

About the organisation

Kirbys Solicitors is a well-established law firm committed to serving the legal needs of Harrogate’s people and businesses. Kirbys specialises in property, family law, disputes and commercial law, estates and private client matters.

Steps to becoming Cyber Essentials certified

Kirbys was already on its journey to becoming more cyber secure when one of its directors attended a free webinar by The Law Society. It covered such topics as money laundering and cyber security, and touched on Cyber Essentials certification, including the importance for businesses of taking measures to improve cyber security.

> “At the time I hadn’t heard about Cyber Essentials. We had recently invested in IT and I thought it was a good idea to pursue it. I also thought there was going to come a day when other businesses would wake up to the need for it.”
>
> **David Dow, Director**

Following a conversation with the firm’s outsourced IT specialist, Keydata Solutions, about Cyber Essentials certification, Kirbys took the decision to strengthen its current cyber defences. The firm’s current setup comprises Bitdefender Cloud Security (anti-virus), Mimecast Email Gateway (email threats and malware protection) backed up by Microsoft Windows Defender.

This included having Microsoft Exchange based in the cloud and Mimecast running in the background protecting against malware. The setup also includes multi factor authentication for remote working, more robust password protocols, tightened admin rights and disabled the ports on all their desktop PCs.

Kirbys found the Cyber Essentials Readiness Toolkit particularly helpful in preparing the firm for self-assessment and sought guidance from Keydata Solutions to understand some of the technical language. The Kirbys team found the overall certification process to be straightforward and obtained Cyber Essentials certification in 2021.

Impact

Having Cyber Essentials has prompted Kirbys to revisit its internal policies and ensure that fully up to date equipment and robust procedures are always in place. The firm has removed personal email addresses from its website to reduce risks and does not transmit bank details over email unless they are encrypted.

"Cyber Essentials has made us all more aware of potential threats to the business and we take these risks seriously. We have a monthly compliance meeting where cyber security is permanently on the agenda."

David Dow, Director

Though Kirbys has a limited supply chain, it considers itself to be at high risk of potential future cyber attacks due to carrying out transactional work on behalf of clients.

"The risk is in the money that we transfer to other people. This makes us a target. So we have placed trust in Cyber Essentials together with robust policies and procedures to help us to protect client money and ensure it is more secure".

David Dow, Director

Kirbys also believes that an increased focus on cyber security will have a positive impact on the firm's market competitiveness and reputation.

Furthermore, having Cyber Essentials has made it easier for Kirbys to obtain separate Cyber Risk Insurance. The firm's Insurance Broker, William Cooper of Lockton Insurance Brokers, commented that by having Cyber Essentials in place, including email encryption, it sends a clear signal to prospective insurers that Kirbys takes cyber risk seriously and has put procedures in place to combat growing cyber risks.

Final message

As cyber awareness increases, Kirbys believes that more businesses will need, and can stand to benefit from, Cyber Essentials certification to show they have the right protections in place.

9.3 Marl International

- **Private business**
- **Medium-sized employer (50-249 staff)**
- **Base: North West**

About the organisation

Established in 1973, Marl International Ltd is based in Cumbria. Its main focus is delivering innovative LED lighting solutions to customers based in the UK and over 50 countries around the world.

Steps to becoming Cyber Essentials certified

Marl was first drawn to the Cyber Essentials scheme after an external evaluation highlighted gaps in the company's cyber security. On the basis that the company did not hold large customer databases, it set out to find a simple and cost-effective solution to bolster its cyber security posture. It became Cyber Essentials certified in 2015, before later upgrading to Cyber Essentials Plus.

> "Cyber Essentials was not difficult to achieve. When undertaking the self-assessment, we realised we had around 90% of it covered already, and you get all of the information you need to pass. Cyber Essentials Plus goes further because it involves external assessment and we found things out during the assessment that weren't quite right that we could then go and fix."
>
> **Hamilton Thurgood, IT Manager**

Obstacles overcome

As the scheme's requirements evolve year-on-year, Marl has needed to be responsive to those changes. But the company sees this as a positive and feels it has been able to consistently improve its security measures.

> "There's a questionnaire and audit we do in advance of re-certifying, which tells us any issues we need to resolve so we're ready. The assessor will go through everything and tell us anything else outstanding we need to fix."
>
> **Hamilton Thurgood, IT Manager**

Impact

Becoming Cyber Essentials certified has turned out to be a valuable endeavour, especially as many of Marl's clients now require Cyber Essentials for contractual purposes.

The scheme has led to several positive and lasting differences for Marl. For example, the company has taken a proactive approach to updating software and checking for vulnerabilities. Marl has also hired an internal auditor to carry out a comprehensive scan of the company's systems. This has allowed it to be in the best position possible when going through annual re-certification.

> "We have a check up on our system every month with internal audits. We also run a vulnerability scan that goes through every machine that is switched on and does a verification check."
>
> **Hamilton Thurgood, IT Manager**

Final message

Marl believes Cyber Essentials to be vital for SMEs, and since most companies cannot afford to spend thousands each year on cyber security, it represents a cost-effective solution to ensure a baseline level of protection against cyber threats.

10. Value for Money

Drawing on the report's findings, along with that of the preceding scheme process evaluation, this chapter examines the value for money of Cyber Essentials from the perspective of UK organisations and supply chains that are certified. This approach is taken given that: i) organisations pay for Cyber Essentials certification; ii) the government perceives its central spending on the scheme to be relatively small; and iii) the scheme's core objective is to help protect organisations of any size against the most common internet-originating cyber attacks.

Firstly, the preceding process evaluation report (section 3.2) identified that more than half (58%) of current and lapsed Cyber Essentials users considered that being certified represented good value for money.

The technical controls have been found from this impact evaluation report to be efficacious (chapter 3.1) and most Cyber Essentials users are confident that the technical controls are positively impacting their level of cyber protection and helping to mitigate cyber security risks within their organisation.

Most scheme users perceive a commercial benefit of being certified, in terms of reducing the financial cost to their own organisation of a common, unsophisticated cyber attack. Other commercial benefits are evidential when considering that organisations may not have been able to enter into some contracts without Cyber Essentials (section 7.1) and more than two thirds believe the scheme has increased their market competitiveness (section 8.3).

Additionally, the scheme is leading to more embedded and sustainable approaches to cyber security risk management, along with streamlined cyber security due diligence which reportedly takes less time to complete when suppliers are Cyber Essentials certified. Cyber Essentials also offers a range of hard-to-quantify benefits to organisations, notably perceived peace of mind against the potential reputational, financial and legal consequence of a cyber attack.

In terms of the scheme itself, growth is being helped by a rising trend in certifications, use of the technical controls by organisations that have never obtained Cyber Essentials, and supply chain assurance mechanisms, with a third of surveyed scheme users stating that they intend to mandate the scheme of their suppliers in the future. Furthermore, as evidenced by the Cyber Essentials scheme process evaluation, the scheme is open and accessible to organisations of all types and sizes to providing baseline protection. It has also directly contributed to the growth of the cyber security sector, with a network of over 340 Certification Bodies and over 900 assessors.

In summary, the evidence points to many wide-ranging benefits and value for organisations and supply chains of having the protections in place offered by Cyber Essentials. Whilst very difficult to prove or quantify in cost (£) terms, the scheme clearly demonstrates value for money for those organisations that use it. Using due judgment, it is also possible to say that the running of the Cyber Essentials scheme incurs minimal costs for the government for the impact it achieves.

Cost effectiveness for certified organisations

The true costs to organisations of becoming Cyber Essentials certified and implementing the technical controls extends beyond the assessment fee and can vary greatly between organisations and by employment size band. As noted in the process evaluation and based purely on survey research, the average costs are estimated as follows by employment size band: micro (£1,894) small (£4,741) medium (£6,267) and large (£31,459). The potential return on that investment needs to consider not just the financial and non-financial consequences of a cyber attack upon an organisation – which are difficult to quantify – but the potential for those consequences to be mitigated.

Firstly – whilst a subjective measure – it is evident that the scheme offers peace of mind against the potential reputational, financial and legal consequences of a cyber attack. Surveyed Cyber Essentials users were asked to rate the perceived reputational, financial and legal impact of a hypothetical cyber attack on a scale from 1 (no impact) to 10 (significant impact). The mean ratings for these scenarios are high (8.0, 6.9 and 6.6 respectively) backed up by evidence from Britain Thinks which found that almost two thirds of Cyber Essentials users (65%) agreed that a cyber attack would result in a significant financial cost to their organisation (section 4.3). Crucially, most scheme users (80%) are of the view that being certified can reduce the financial cost to their organisation of a common, unsophisticated cyber attack (section 6.2).

The scheme evidently yields further commercial benefits considering that a third (33%) of contracts that scheme users entered into over the preceding 12 months required them to be Cyber Essentials certified (section 7.1); and more than two thirds (69%) believe the scheme has increased their market competitiveness (section 8.3).

The scheme's ability to reduce the risks and potential consequence of a cyber attack is ultimately contingent on the efficacy of the technical controls at providing basic protection, which previous evaluation work has been found to perform well (discussed below).

Provision of strong baseline protection against common cyber threats

Research by Such et al (2015) – Cyber Security Controls Effectiveness: A Qualitative Assessment of Cyber Essentials involved analysing 200 internet-originating vulnerabilities. Of these, it was observed that 99% were mitigated using Cyber Essentials technical controls, but none were mitigated without them. Furthermore, most Cyber Essentials users (82%) surveyed for this evaluation feel confident that the technical controls are positively impacting their level of protection against common cyber threats and 80% are confident that they help to mitigate cyber security risks within their organisation (section 3.1).

Additionally, and as further evidence of the efficacy of the technical controls, the NCSC's Annual Review 2023 points to 80% fewer cyber insurance claims made when Cyber Essentials is in place (based on 2022 claims data). This is compared with organisations that have the same insurance policy and do not have Cyber Essentials certification.

Embedded and sustainable approaches to cyber security risk management

Cyber Essentials has directly strengthened surveyed organisations' understanding of cyber security risks and the steps they can take to reduce them (section 5.1); how well senior management understands the risks posed by cyber attacks (section 5.2); and organisations' confidence that they are better protected in the event of a common, unsophisticated cyber attack (section 5.4).

Qualitative evidence points to these practices stimulating wider cyber resilience practices for most surveyed organisations (chapter 6). For example, almost three quarters of Cyber Essentials users (71%) agree that the scheme has directly strengthened how seriously their organisation as a whole takes cyber security (section 6.3).

Streamlined cyber security due diligence

Where suppliers are Cyber Essentials certified, there is evidence of time savings as part of supplier due diligence processes. This means organisations have the opportunity to use time they would have been spent on due diligence processes in other ways.

Most surveyed Cyber Essentials users (60%) report undertaking cyber security due diligence with respect to their potential suppliers. Of these, just under half (48%) report saving time where a potential supplier is CE certified, while more than half (59%) report saving time where a potential supplier is CE Plus certified.

More widespread scheme use and resulting cyber resilience

There is evidence of a positive upward trend in Cyber Essentials certifications, increasing use of the scheme through supply chain assurance, and use of the scheme's technical controls by a minority of organisations that had never been certified.

Firstly, Cyber Essentials scheme certification has been growing steadily over the years. This has been driven mainly through being mandated in government contracts that meet certain criteria, notably where this involves handling personal information and providing certain ICT products and services. Trend data are steady but positive, showing growth increasing from 500 certifications per month in January 2017 to more than 3,500 in December 2023 (section 1.2).

Secondly, there is evidence that the scheme is reaching organisations in other ways, leading to the technical controls being adopted more widely. For example, the Cyber Security Breaches Survey 2023 found that a fifth (20%) of all surveyed private sector businesses reported adhering to the Cyber Essentials technical controls in all five areas – considerably higher among medium businesses (42%) and large businesses (61%).

Thirdly, among the 53 organisations surveyed for this evaluation that report being ISO 27001 accredited but not Cyber Essentials certified, 24% still draw upon Cyber Essentials guidance. This points to the scheme having potential value for organisations wherever they are on their cyber security journey, discussed below.

Among organisations that had never obtained Cyber Essentials, more than a fifth (23%) of these organisations are more likely to choose suppliers that hold Cyber Essentials and a quarter (25%) have greater confidence working with suppliers that hold Cyber Essentials (section 7.3). This points to the scheme having a positive effect on supply chain assurance decision-making beyond certified Cyber Essentials users alone.

Protection to all types and sizes of organisation

The scheme as intended is open and accessible to organisations of all types and sizes, and its technical controls are providing baseline protection to organisations ranging from the smallest taking their first steps in their cyber security journey, to large organisations seeking to plug gaps in their existing cyber security risk management protocols. Furthermore, 88% of Cyber Essentials users surveyed as part of that evaluation said they were confident in being able to meet the technical requirements for obtaining certification.

That said, it is important to recognise from the process evaluation that some of the largest and smallest organisations can face substantial yet quite different obstacles to meeting the technical controls, which potentially impacts on perceived value for money (process evaluation, section 5.5; also summarised in this report, section 6.4).

A standardised approach to implementing the technical controls

As examined in the process evaluation, Cyber Essentials' intentionally prescriptive rather than risk-based approach means that it can clearly define itself as providing a baseline cyber security solution. Cyber Essentials users follow the same assessment criteria and are assessed according to the same standard, and the technical controls continue to evolve in line with the threat environment. This approach appears to be working well and the scheme could see reduced take-up if it were to align itself overtly with certain types or sizes of organisations over others, for example moving to a risk-based approach.

Summary

The value for money assessment of Cyber Essentials is principally from the perspective of UK organisations and supply chains that are certified. This approach is taken given that: i) organisations pay for Cyber Essentials certification; ii) the government perceives central spending on the scheme (not quantified through this evaluation) to be relatively small; and iii) the scheme's core objective is to help protect organisations of any size against the most common internet-originating cyber attacks.

The Cyber Essentials scheme works to address the information asymmetry present in this market in two main ways:

1. **Understanding what cyber security controls to put in place:** By the government including achievable controls that stop up to 99% of internet-originating vulnerabilities (Such et al (2015)), organisations can focus their time on implementation and other productive activities rather than deciding on what to implement.

2. **Understanding cyber security when making investment and consumption decisions:** It has now allowed cyber security to be considered in purchasing decisions with 61% saying they are more likely to pick a supplier that uses Cyber Essentials.

In summary, the evidence points to many wide-ranging benefits and value for organisations and supply chains of having the protections in place offered by Cyber Essentials. Whilst very difficult to prove or quantify in cost (£) terms, the scheme clearly demonstrates value for money for those organisations that use it. Using due judgment, it is also possible to say that the running of the Cyber Essentials scheme incurs minimal costs for the government for the impact it achieves.

11. Conclusions and Recommendations

11.1 Conclusions

1. **Cyber Essentials is providing cyber security protection to organisations of all sizes, including larger organisations that use other schemes, standards and accreditations.**

A key test of Cyber Essentials is the extent to which it is contributing to improved protection of UK organisations against basic and common cyber attacks. Furthermore, having a baseline level of protection is hugely important to ensure organisations can operate as safely as possible online in a modern business environment.

Evidence assessed as part of this evaluation points to the scheme providing strong protection for Cyber Essentials users against the most common cyber attacks. For example, a recent evaluation by Such et al. (2019) into internet-originating vulnerabilities found that 99% were mitigated using the Cyber Essentials technical controls. Furthermore, 82% of scheme users surveyed for this evaluation are confident that the technical controls provide protection against common cyber threats, while 80% say that the controls help to mitigate cyber security risks within the organisation.

The technical controls appear to be adopted more widely than among certified organisations alone, with the Cyber Security Breaches Survey 2023 reporting that 20% of surveyed businesses claimed to be adhering to the Cyber Essentials technical controls in all five areas. In support of this, a minority (13%) of organisations surveyed for this evaluation that had never obtained Cyber Essentials are using the scheme’s information and guidance to strengthen their own cyber security.

Furthermore, among 53 surveyed organisations certified to ISO 27001 but not Cyber Essentials, 24% still draw upon Cyber Essentials guidance and more than four in ten (42%) say that their organisation only meets some of the Cyber Essentials technical controls. This suggests that Cyber Essentials can have strong impact where organisations may lack some of the fundamental controls from other certifications.

2. **Cyber Essentials helps to improve organisations’ awareness and understanding of the cyber security risk environment – thus enabling them to become more informed – and helps to boost scheme users’ confidence at mitigating the risks of a possible cyber attack.**

Evidence points to Cyber Essentials having a role in increasing organisations’ awareness of cyber security risks. Almost two thirds (64%) of scheme users are of the view that being certified better enables their organisation to identify when they experience a common, unsophisticated cyber attack. This is important to minimise the risks of a breach going unnoticed, which might be more harmful longer term.

Through having greater cyber security risk awareness, Cyber Essentials users appear more likely to consider their organisation at risk of suffering a cyber attack. This may account for scheme users providing a higher concern rating about the possibility of a cyber attack on their organisation (5.8 out of 10) compared to organisations that had never obtained Cyber Essentials (3.7 out of 10).

Most Cyber Essentials users (85%) believe that the scheme has directly improved their understanding of cyber security risks; an even greater proportion (88%) believe that Cyber Essentials has directly improved their understanding of the steps they can take to reduce cyber security risk; and more than three quarters (76%) believe that the scheme has improved how seriously their organisation as a whole takes cyber security.

Qualitative insights from strategic stakeholders and scheme users show praise for the role of Cyber Essentials in helping organisations on their cyber security journey. This includes building confidence in their cyber security posture, providing them with a baseline for tightening internal procedures and technical protocols, and offering peace of mind.

Most organisations surveyed for this evaluation (91%) say that Cyber Essentials has directly improved their confidence at being able to consistently implement steps to reduce cyber security risks. The same proportion also say that Cyber Essentials has directly improved their confidence in being protected in the event of such an attack. This additional confidence could be especially important for organisations that lack in-house expertise, most often the smallest.

The comparison survey of organisations that had never obtained Cyber Essentials reveals similarly high levels of understanding and confidence to that of scheme users. This points to a likely overconfidence bias, further justified from qualitative insights among scheme users that becoming Cyber Essentials certified opened their eyes to prior cyber security weaknesses and gaps which the technical controls have helped to plug. At the same time, Cyber Essentials users then have a tendency to be more cautious and concerned about the likelihood of a possible cyber attack, which encourages them to take further actions beyond the technical controls (see conclusion 3).

3. Cyber Essentials has stimulated wider actions, good practice and behaviours among organisations that use it, potentially born out of a heightened appreciation of the cyber security risk environment.

Approximately three quarters of Cyber Essentials users (76%) report having taken actions beyond the scheme's technical controls, potentially further strengthening their cyber resilience. This includes helping them to detect and monitor instances of a common, unsophisticated cyber attack; respond to and recover from a common, unsophisticated cyber attack; and reduce the likely financial cost to their organisation from such an attack.

Furthermore, almost three quarters (71%) of Cyber Essentials users agree that the scheme has directly strengthened how seriously their organisation takes cyber security, including a more holistic, organisation-wide and "business as usual" approach to cyber security where all staff are encouraged to play their part.

4. Cyber Essentials is being actively used as part of supply chain assurance to inform the supplier selection process, instil confidence and demonstrate basic cyber hygiene to the market.

Cyber Essentials appears to play a valuable role in helping the majority of surveyed organisations choose Cyber Essentials certified suppliers (61%) and have more confidence in those suppliers (75%). An even greater proportion (79%) believe it offers a confidence-improving standard for their own clients and customers and just under half (45%) say that they take Cyber Essentials into account when assessing the cyber risk that a supplier poses to them.

Some 15% of Cyber Essentials users have made it mandatory for their suppliers to become Cyber Essentials certified and plan to continue doing so. Furthermore, 33% are actively considering mandating Cyber Essentials in the future, indicating the scheme's potential to grow take-up, extend baseline protection and scale up resilience. Longer term, this could have the effect of making Cyber Essentials an important standard for any business looking to retain a competitive advantage.

Additionally, Cyber Essentials appears to be valued by organisations that are not in themselves certified. Indeed, almost a quarter (23%) of organisations that had never obtained Cyber Essentials say they are more likely to choose suppliers that hold Cyber Essentials; and 25% say they have greater confidence working with such suppliers.

5. Cyber Essentials is streamlining due diligence for some organisations and their supply chains, but this is not always the case.

Just under half of Cyber Essentials users (48%) report saving time where a potential supplier is CE certified, rising to 59% where CE Plus certified. Based purely on survey data, which may be subject to some over-estimation bias, scheme users save 22% of their time on cyber security due diligence for each potential supplier that is CE certified, and 32% of their time for each potential supplier that is CE Plus certified.

More than three quarters of surveyed scheme users (76%) have also found that being Cyber Essentials certified means they can save time on diligence asked of them by their own clients and customers. That said, some organisations were keen to assert that cyber security questionnaires can still be long and sometimes onerous, suggesting that commissioning clients may not have considered what Cyber Essentials already demonstrates in relation to their security criteria.

A challenge here is that Cyber Essentials is only one of a number of standards and adopts a prescriptive approach to the technical controls which may not meet the needs of all commissioning clients. This could potentially explain situations where the burden of due diligence has not been reduced.

6. **Cyber Essentials is contributing to wider value, through growth in the cyber security sector, peace of mind through the bundled cyber liability insurance, and stronger market competitiveness.**

The Cyber Essentials scheme's direct role in growing the network of Certification Bodies and Cyber Advisors is offering additional UK-wide support to organisations that need it, through information and guidance. This support is considered valuable for organisations that tap into it – including those seeking to become Cyber Essentials certified – as opposed to being focused on pass/fail assessment.

The bundled Cyber Liability Insurance is demonstrating efficacy, with 80% fewer cyber insurance claims made when Cyber Essentials is in place (based on 2022 claims data). Furthermore, more than two thirds (69%) of scheme users believe that the scheme has increased their market competitiveness.

11.2 Recommendations

The following recommendations are aimed at DSIT, IASME and NCSC to consider as part of a coordinated approach. Not all components of these recommendations may be appropriate or desirable depending on feasibility but they have been developed to respond to the main issues raised through the research.

1. **Continue to promote Cyber Essentials as an affordable and responsive cyber security solution aimed at organisations that may otherwise lack basic protection.**

Firstly, existing research has found the technical controls to be broadly effective at mitigating vulnerabilities and these should continue to respond to changes in the threat environment.

The scheme offers a baseline level of protection against common internet-originating cyber attacks which should continue to be a core focus as they not only protect smaller organisations without basic safeguards, but also some larger organisations with other standards and accreditations which may not cover some of these elements.

Cyber Essentials should continue to offer an affordable solution to smaller organisations that might otherwise lack awareness and understanding about the potential cyber security risks facing their organisations, or be under a misconception that they are not at risk or would not be adversely affected if they were targeted. This is especially important for smaller organisations that may not be able or willing to pay for other standards and accreditations such as ISO 27001.

2. **Continue to invest in the scheme's supportive approach to helping organisations gain and sustain certification, by growing the supportive network of Certification Bodies and assessors.**

Cyber Essentials users value the support they receive from Certification Bodies to help them become better protected, rather than taking a purely neutral approach as an intermediary and adopting a pass/fail approach to certification. This should be encouraged and could be usefully set out to all Certification Bodies and potential scheme users so there is an understanding of expectations.

3. Stimulate wider and more effective use of Cyber Essentials as a supply chain assurance tool.

The potential for Cyber Essentials to become more embedded as part of supply chain assurance is evident, with a third of all surveyed scheme users (33%) actively considering mandating Cyber Essentials of their suppliers in the future. This rises to 43% among large organisations.

There is substantial room to grow this by creating a stronger narrative in this area, including how to achieve this and the benefits it can bring. A user guide could be developed to help organisations take this step and do so effectively. This could include guidance on why this is important, how to go about it with suppliers, and the potential cyber security benefits this can bring for both parties, such as greater protection, improved business confidence and peace of mind.

4. Help clients to identify how they could improve the efficiency of cyber security due diligence processes where their suppliers are Cyber Essentials certified.

There is evidence that cyber security due diligence is not always simplified for organisations that are Cyber Essentials certified. There may be genuine reasons for this, for example where clients have certain complex requirements, but in some cases clients appear to still be using extensive cyber security questionnaires which ask the same questions of all organisations – whether certified or not. This is likely to come down to clients not having identified where their requirements are already addressed by Cyber Essentials certification.

Guidance should therefore be provided to clients to encourage them to revisit cyber security due diligence questionnaires where possible to reduce the burden on certified organisations as far as reasonably possible. This should, in turn, provide more tangible benefits to certified organisations who then stand to be more positive about the scheme and may recommend it to other organisations.

5. Encourage more organisations to prioritise cyber security by conveying more tailored information about the benefits of being Cyber Essentials certified to different sizes and types of organisation.

Consider providing more tailored information, marketing and case studies (such as those included within this report) to different sizes and types of organisation. These should articulate a typical journey to becoming certified or strengthening existing levels of protection and the wider range of benefits this can bring, such as keeping information, money and people safe, having peace of mind, and being more competitive.

Additionally, consider a targeted marketing campaign to key enablers in the cyber security space, such as IT support sector businesses. With their buy-in, these organisations are well placed to promote it further to the organisations they work with. Other avenues of promotion could include trade bodies and online or offline forums aimed at directors and IT specialists.

6. Consider providing more basic information to organisations that have never been certified to help them better understand the Cyber Essentials scheme and why it would be a good investment.

Many organisations that have never obtained Cyber Essentials may lack basic cyber security awareness or be under a misconception about the risks they face. They may lack awareness of Cyber Essentials and consider that off-the-shelf antivirus software is sufficient on its own.

Whilst Cyber Essentials isn’t an equivalent to this type of product, more and better information should be provided to help explain what the limitations are of such products, how Cyber Essentials is different and how it is designed as a valuable investment in terms of affordable, baseline protection.

It would also be valuable to more clearly explain how Cyber Essentials is different to more complex risk-based schemes such as ISO 27001, i.e. in terms of providing a cost-effective solution to preventing the most common internet-based cyber attacks.

7. Continue to work with insurance providers to convey the latest evidence on the effectiveness of the Cyber Essentials technical controls and how the scheme contributes to organisational cyber resilience.

As the cyber threat environment continues to evolve, Cyber Essentials users might reasonably expect to benefit from reduced insurance premiums based on being more cyber secure. Furthermore, this could help to improve the perceived cost-effectiveness of the scheme for organisations that take it up.

Further work should therefore be undertaken in conjunction with insurance providers to build their understanding of the scheme and its nuances, with a view to certification being viewed more favourably as part of the policy risk assessment process.

8. Consider rolling out more targeted and high-profile marketing and communications stressing the potential hard-hitting consequences of a cyber attack.

Building on the Cyber Aware campaign, consider producing and running hard-hitting media adverts about the risks of a cyber breach – via television, radio or social media depending on the costs involved. These could be similar in style to past drink driving campaigns, pointing to the Cyber Essentials scheme as an important part of the solution to the main threats.

Appendix 1. Cyber Essentials Certification Characteristics

Appendix 1 describes the characteristics of Cyber Essentials certification among surveyed current and lapsed users, including level of certification and length of time certification has been held. For organisations never certified, it provides basic details of the proportion that had heard of the scheme prior to taking part in the evaluation, and the proportion that had previously considered becoming certified.

A1.1 Certification patterns

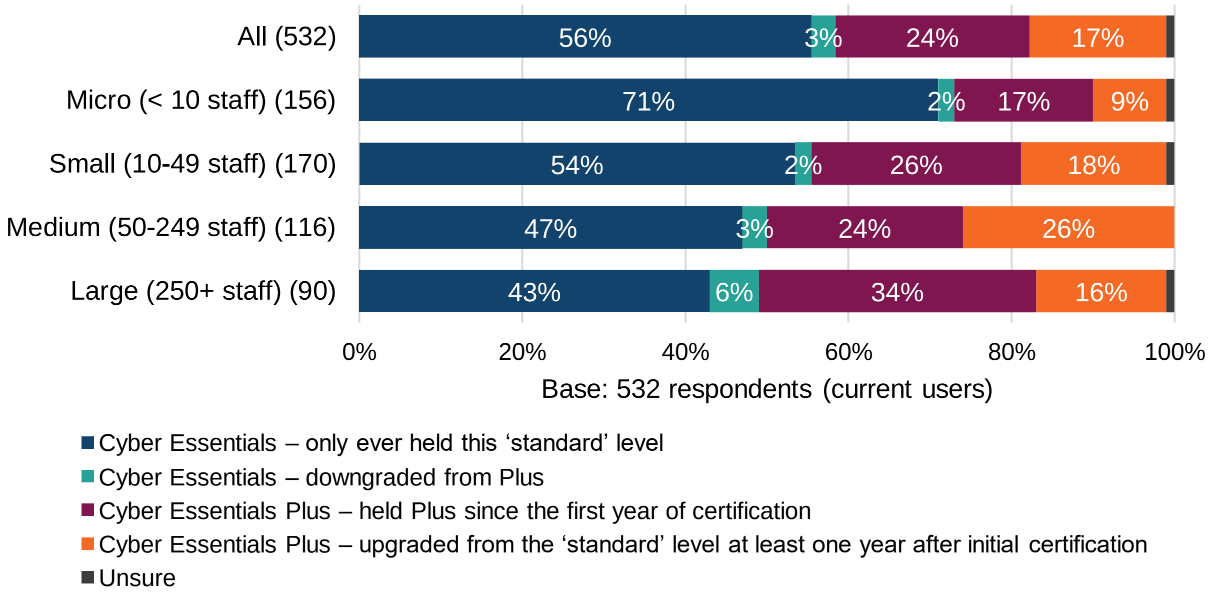
Level of certification

Among surveyed current users, most (59%) hold CE and the remainder (41%) hold CE Plus.

There is a much stronger prevalence of scheme users changing from CE to CE Plus (17%) than those changing from CE Plus to CE (3%). This points to Cyber Essentials encouraging a journey towards a more robust approach to cyber security.

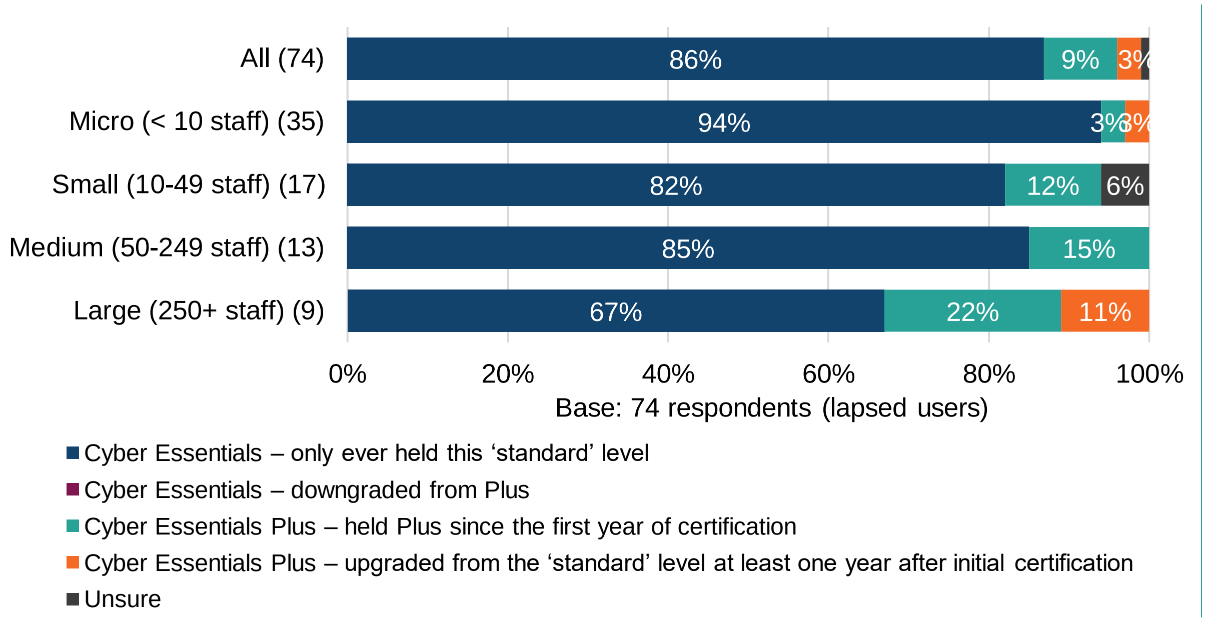
The proportion of micro organisations that have only ever held CE is significantly higher (71%) than other size-bands, which may come down to the additional cost of CE Plus and not having an identified business need for this level of certification. Similarly, the proportion of large organisations that have only ever held CE Plus (24%) is significantly higher than micro businesses (Figure A1.1).

Figure A1.1 Level of Cyber Essentials held among current users (by size-band)



Among surveyed organisations whose Cyber Essentials certification has lapsed, most (86%) had only ever held the standard level. Among medium and large organisations whose certification has lapsed, there is a greater prevalence of CE Plus having been previously held and the difference between large and micro organisations here is significant (Figure A1.2).

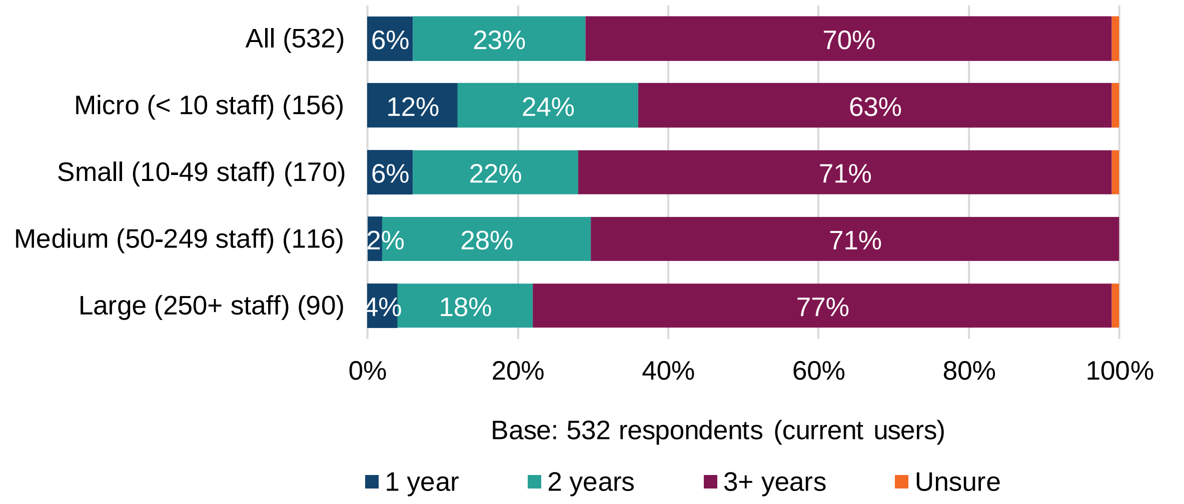
Figure A1.2 Level of Cyber Essentials held among lapsed users (by size-band)



Length of time certification held

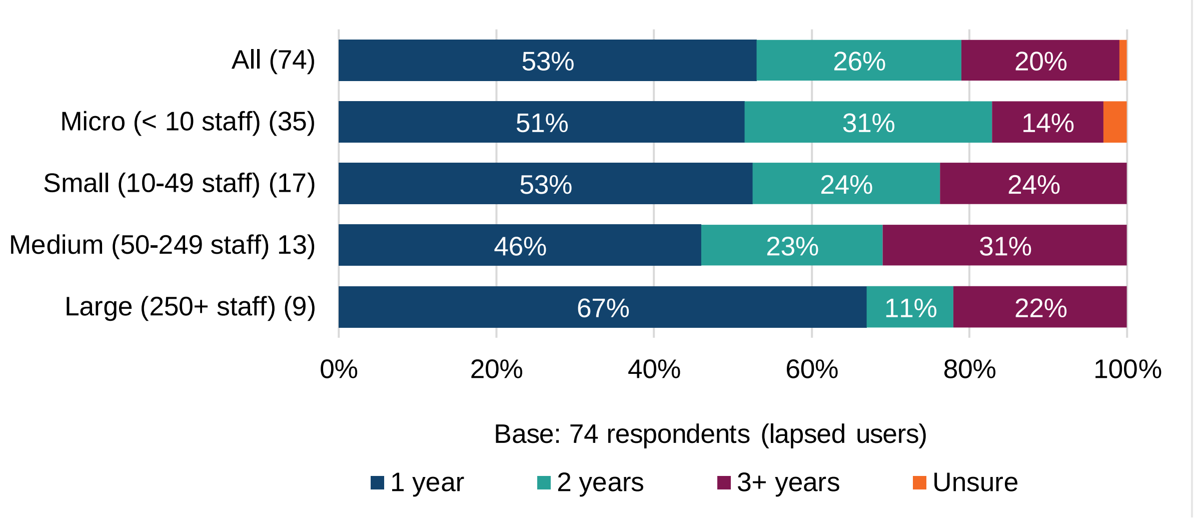
Most current Cyber Essentials users responding to the survey (70%) have been certified for three or more years (Figure A1.3).

Figure A1.3 Total time Cyber Essentials held among current users (by size-band)



Among the small sample of lapsed users responding to the survey, the picture is more nuanced, with cohorts having held their certification for varying lengths of time. Drop-offs were highest after one year (53% of the cohort), indicating that once organisations pass this threshold, they could be more likely to continue with the scheme (Figure A1.4).

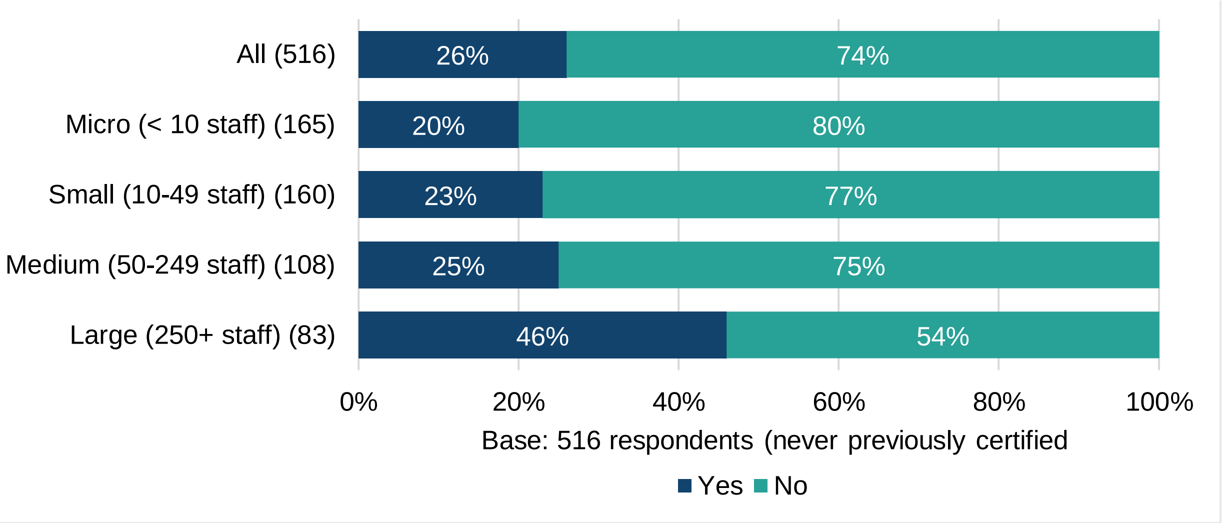
Figure A1.4 Total time Cyber Essentials held among lapsed users (by size-band)



A1.2 Prior awareness of Cyber Essentials among organisations never certified

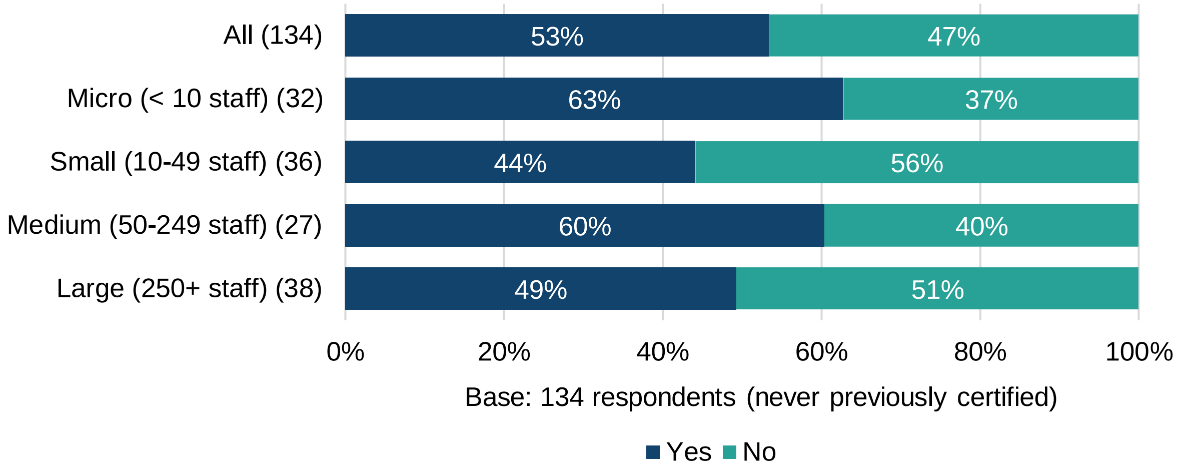
Just over a quarter of surveyed organisations that had never obtained Cyber Essentials certification (26%) had heard of the scheme prior to taking part in the survey – significantly more so among large organisations (Figure A1.5).

Figure A1.5 Whether previously heard of Cyber Essentials (never certified)



Of the 134 respondents that had heard of the scheme, more than half (53%) had considered obtaining Cyber Essentials (Figure A1.6).

Figure A1.6 Whether considered becoming Cyber Essentials certified (never certified)



Appendix 2. Survey Respondent Profile

The tables in Appendix 2 set out the unweighted (i.e. non-adjusted) survey respondent numbers taking part in this evaluation based on a range of profiling characteristics. These include relationship to the Cyber Essentials scheme, size-band, type of organisation, NUTS1 region, industry sector, financial turnover and job role of responding individuals.

Table A2.1 Relationship to the Cyber Essentials scheme

	Current users	Lapsed users	Never certified
Total valid organisation-level responses	532	74	516

Table A2.2 Size-band

	Current users	Lapsed users	Never certified
Micro (< 10 staff)	156	35	201
Small (10-49 staff)	170	17	158
Medium (50-249 staff)	116	13	101
Large (250+ staff)	90	9	56

Table A2.3 Type of organisation

	Current users	Lapsed users	Never certified
National or local government (inc. department/body/agency)	3	2	2
Academic institution	24	5	14
Private business	453	58	439
Non-governmental organisation (NGO)	6	2	4
Registered charity/trust	36	5	55
Other	10	2	2

Organisation types self-classified as ‘other’ include a mix of: Credit union, independent fostering agency, organisation limited by guarantee, not-for-profit enterprise, social enterprise activities, supplier.

Table A2.4 NUTS1 region where organisation based

	Current users	Lapsed users	Never certified
East of England	41	4	26
East Midlands	30	4	22
London	91	15	131
North-East	18	2	23
North-West	47	6	34
South-East	99	10	66
South-West	65	8	28
West Midlands	46	5	12
Yorkshire and The Humber	25	6	41
Scotland	30	6	54
Wales	25	4	50
Northern Ireland	10	3	28
Crown Dependencies	5	1	1

Table A2.5 Industry sector

	Current users	Lapsed users	Never certified
Accommodation and Food Service	2	1	8
Activities of Households as Employers	-	1	-
Administrative and Support Service	6	1	18
Agriculture, forestry and fishing	2	-	9
Arts, Entertainment and Recreation	3	2	35
Construction (includes civil engineering)	31	4	50
Education	46	7	31
Financial and Insurance	21	4	25
Human Health and Social Work	51	6	31
Information and Communication (includes computer programming, consultancy and related activities)	178	27	32
Manufacturing	33	2	52
Mining and quarrying	2	-	4
Other Service Activities	21	5	91
Professional, Scientific and Technical	89	9	15
Public Administration and Defence	8	1	2
Real Estate	5	-	17
Transportation and Storage	5	1	15
Utilities	7	-	4
Wholesale and Retail Trade	9	1	68
Other	13	2	9

Sectors self-classified as ‘other’ include: Advice and information charity, commodities, audio-visual Industry, Certification Body, consultancy, digital media, industrial services, mentoring, security, scientific contract research.

Table A2.6 Financial turnover

	Current users	Lapsed users	Never certified
Less than £250,000	75	23	115
£250,000 to £499,999	54	9	76
£500,000 to £999,999	56	9	27
£1m to £2.9m	124	12	62
£3m to £4.9m	41	5	21
£5m to £19.9m	91	4	60
£20m+	91	12	155

Table A2.7 Job function of respondent

	Current users	Lapsed users	Never certified
Owner/manager/director	247	48	144
IT/information/data security specialist	228	20	43
HR	4	-	13
Legal/compliance	20	1	10
Administrative	20	4	283
Third-party IT or information security support provider (on behalf of another organisation)	5	1	4
Other	8	-	19

Job roles self-classified as 'other' include: account manager, business development manager, company accountant, finance manager, forester, operations, marketing, sales, technical director.