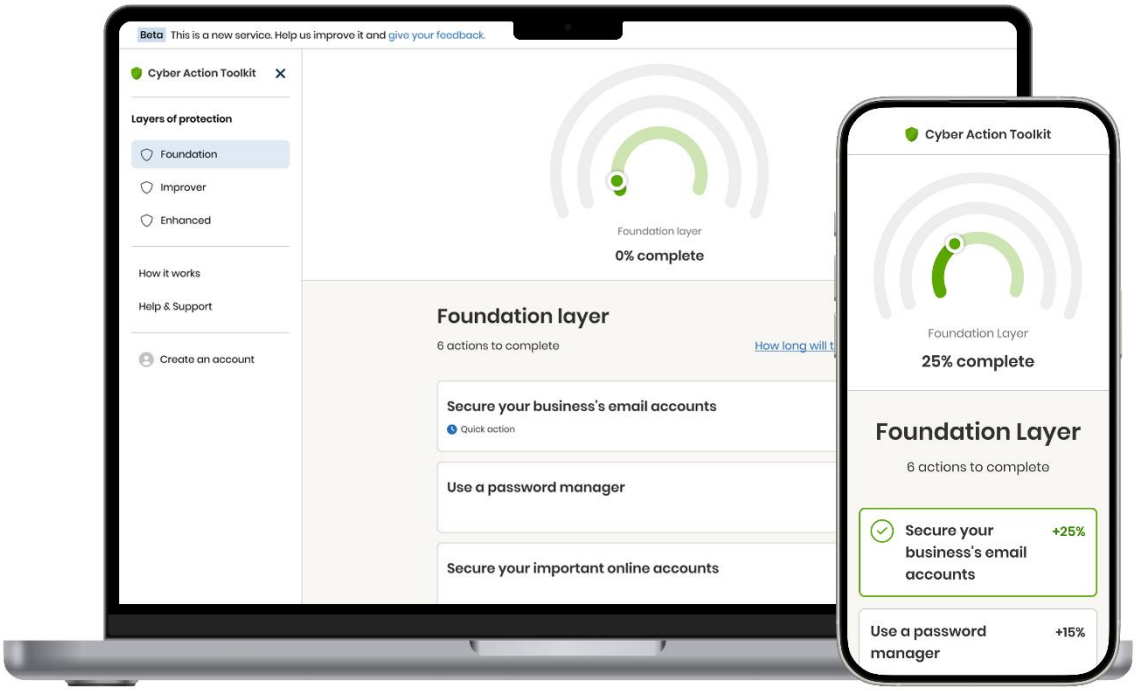
National Cyber Security Centre
a part of GCHQ

Motivating small organisations to take action

Using an evidence-based approach in the development of action-based guidance for the UK's small organisations.



Contents

Contents 1
Executive Summary 2
1.0 Introduction 3
2.0 The approach 4
3.0 Research to date 5
4.0 Overall Conclusions 12
5.0 Next steps 13
6.0 Acknowledgements 13

Executive Summary

This paper presents the innovative development and evaluation of an action-based, gamified toolkit – based on current cyber security advice and guidance from the National Cyber Security Centre (NCSC) – designed to enhance the cyber resilience of small organisations in the UK.

Recognising the limited engagement and resource constraints of this demographic, the NCSC adopted a user-centric, evidence-driven approach to create accessible, manageable, and motivating guidance tailored to small organisations' needs.

Through iterative research phases – ranging from initial discovery to private beta testing – the toolkit has demonstrated significant improvements in user engagement and action completion rates. Private beta research has shown a meaningful increase in self-motivated participation across a diverse range of small organisations. Additional qualitative analyses have confirmed that gamification and actionable guidance substantially encourage organisations to undertake cyber security measures, with a high level of technical correctness in implementation. **The findings affirm that simplified, visually engaging, and rewarded guidance effectively address barriers faced by small organisations, providing a scalable model for wider industry adoption.**

The upcoming public beta aims to expand the toolkit's reach, ultimately fostering a more resilient UK economy by supporting small organisations on their cyber security journey.

This publication intends to showcase the successful use of action-based guidance and gamification in a cyber security setting and the user-centric, evidenced-based delivery approach that has enabled its success.

Although the specific case study described herein focuses solely on the cyber security of small organisations, the NCSC foresees learnings from the publication of these results, and delivery approach, which can be utilised across industry.

1.0 Introduction

1.1 Strategic context

The National Cyber Strategy 2022 sets out the government's approach to protecting and promoting the UK's interests in cyberspace. Objective 2.2.6 of the National Cyber Strategy states:

> ***Technical advice, self-help tools and assured products and services to improve cyber resilience are easy to find and continually improving, with a particular emphasis on helping citizens, sole-traders and small organisations.***

Economy & Society Resilience, a directorate of the National Cyber Security Centre (NCSC) stood up a programme called Citizens & Small Organisations (C&SO) to deliver on this objective.

1.2 About small organisations

There are approximately 5.5m small organisations with 0-49 employees in the UK, which accounts for over 99.2% of the business population, 48% of UK employment and 36% of economic turnover.

Cyber attacks on this cohort therefore have a highly disruptive and financially degrading impact on the UK economy, and society at large. Internal research from the NCSC and the UK Government's Cabinet Office indicates that small organisations have limited threat awareness and research from the University of Portsmouth has shown that small organisations often consider cyber security not relevant to their size or not something they should invest time and resources into.

At the outset of the C&SO programme, a baseline for which actions that small organisations frequently take (and reciprocally, do not take) to improve their cyber security did not exist.

1.3 The problem: small orgs and cyber security

Research has shown that small organisations typically do not have the knowledge, resources or motivation to take action to improve their cyber security.

Moreover, the Cyber security breaches survey has explored the effectiveness of UK government's cyber security advice to small organisations and identified possible improvements.

They consistently show that UK government's existing offerings for small organisations could be improved for the following reasons:

- they have insufficient reach
- small organisations struggle to find relevant advice and guidance
- the guidance itself does not enable small organisations to take action to improve their cyber resilience

2.0 The approach

At the conception of the C&SO programme, the NCSC had sufficient evidence to indicate that change was required in its offering for small organisations. The solution, however, was not immediately obvious.

The approach that the NCSC has deployed to solve this problem is underpinned by three key principles:

- all decision making must be evidence-based
- the approach must be coordinated across UK government, and any solution must have cross-government utility
- the solution must be user-centric, designed with small organisations in mind

In practice, this meant conducting multiple rounds of research with small organisations (and other secondary users) to understand user needs, barriers, and motivations about cyber security. This iterative development process has allowed continual refinement based on user feedback as thinking has converged towards a solution.

3.0 Research to date

3.1 Pre-discovery

Prior to the Discovery phase, user research indicated that traditional cyber security guidance provided on the NCSC website was not having the desired impact for small organisations. Observations showed that small organisations tended to skim-read content, leading to a lack of actionable change.

Users were observed incorrectly assuming they had completed necessary security measures, and the NCSC website's broad array of content often caused distraction, further hindering engagement with the most relevant advice.

This observation led to the initiation of this work, focusing on further research with small organisations to understand how best to deliver guidance to them in a way that would motivate them to take action.

3.2 Discovery research

Research was conducted with small organisation owners and Cyber Protect Network officers to understand their needs, barriers, and motivations. Multiple concepts and ideas were tested in focus groups to understand what approaches would best motivate these audiences. These concepts included:

- learning about cyber security (eg via courses and gamification)
- action-based tools
- understanding business cyber security health
- receiving online assistance

Two key insights from the research were that small organisations want a clear 'to-do list' and prefer actions broken down into manageable steps. The key findings from the discovery phase were that small organisations were looking for:

- **Actionable lists of guidance**: Guidance that is broken down into manageable chunks that people can action when they are able to.
- **Tailored guidance**: Small organisations are more likely to engage and take action if the guidance feels tailored to them. Some level of personalisation is essential, since there are distinct differences within the small organisation community (eg those with employees vs those without).
- **Motivation to act**: Messaging that surprises or grabs attention – while feeling quick, relatable, and easy to act on – is most likely to spark interest. Users are more motivated to take action when they clearly see how it benefits them and their business.
- **Guidance design**: Visually engaging, intuitive, and structured guidance resonates well.
- **Accessibility and endorsement**: A service that is accessible, easy to share, and endorsed by relevant government and business partners is more likely to be used.

3.2.1 Early toolkit design

Insights from the discovery phase led to the creation of a 'toolkit' that blends practical, 'action-based guidance' with gamification features.

Action-based guidance breaks down complex, written advice into manageable 'layers,' 'actions,' and 'steps,' all of which are designed to prompt specific user behaviours.

As users work through the actions, they're able to self-report progress, and are given 'rewards' for doing so, which fosters motivation and enables extensive data collection.

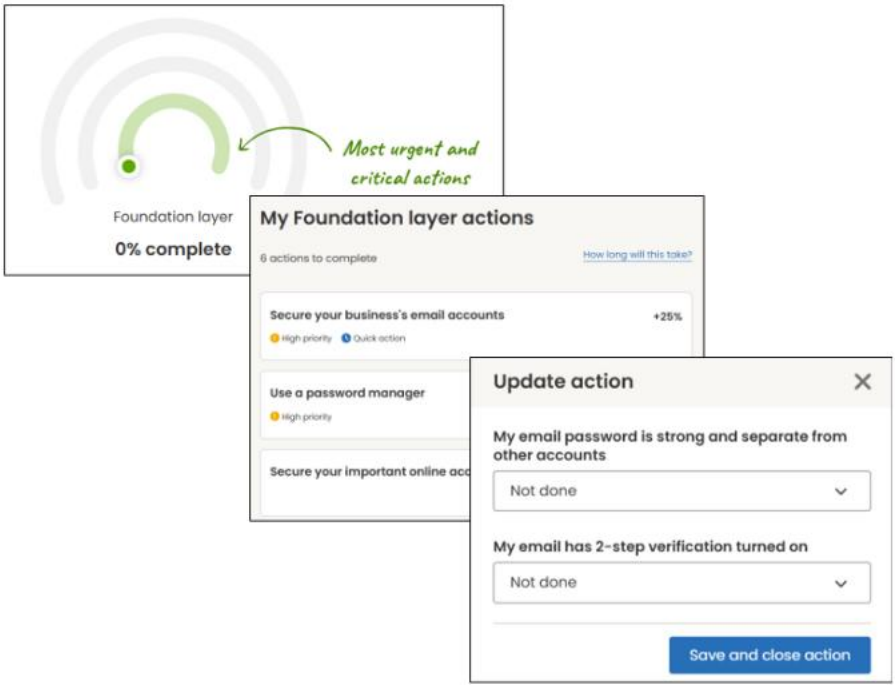


Figure 1: An example of the 'Foundation' layer showing content further broken down into 'actions' and 'steps'

3.2.2 Measuring impact: actions as a proxy for resilience

The ability to self-report progress offers valuable insights into small organisations and the steps they take to strengthen their cyber security. To measure the impact of the toolkit, an assumption has been made that:

Every action completed (correctly) increases the cyber resilience of the small organisation completing that action.

where all actions are based on existing NCSC advice and guidance.

This paper, and the results presented, focus specifically on the successful link between the toolkit concept and the number of actions taken to improve an organisation's cyber security and cyber resilience.

Quantification, and baselining, of the UK's small organisations' cyber resilience will allow more detailed measuring and reporting of improvement. This is a separate evidence base, which there remains a need to gather and investigate, but is out of scope of this paper.

3.3 Alpha: does 'action-based' guidance result in more action?

After conceptualising the idea of action-based guidance within a toolkit environment, the next step was to prove if it would lead to small organisations taking more action.

3.3.1 Approach

To answer this, a research study was conducted with 67 microbusinesses. The study aimed to understand if the way that guidance was presented would affect the number of actions organisations would take to improve their cyber security.

The three conditions were:

- Control (the NCSC Small Business Guide)
- Condition 1 (new action-based guidance, presented as an article on the NCSC website)
- Condition 2 (the toolkit: a combination of action-based guidance and gamification)

In this research, users were presented with one 'layer' of content – the 'Foundation' layer. This layer included action-based guidance on topics such as 'Secure your business' email accounts', 'Use a password manager' and 'Secure your devices'. The Foundation layer included a total of 17 steps on average – the number of steps varies slightly depending on organisational size – and users were given 2 weeks to complete as many of these steps as they choose.

3.3.2 Results

Results showed Condition 2 (the toolkit) significantly outperformed others, with users completing more than double the number of steps than in the Control and in Condition 1. The Net Promoter Score (NPS), which measures user satisfaction and loyalty was also notably higher for Condition 2.

	Control (Small Business Guide)	**Condition 1 (Action-based guidance)**	**Condition 2 (Toolkit)**
Mean number of steps completed	*1.38*	*1.48*	*4.00*
Net Promoter Score	*23, "Good"*	*19, "Good"*	*48, "Great"*

Table 1: Summary of alpha study results

Additional qualitative research allowed us to understand users' motivations and barriers in greater depth, specifically in relation to individual actions, but also regarding cyber security as a whole.

Users reported how manageable, practical and motivating the content was within Condition 2. They also appreciated the accountability of being able to mark actions as complete, which motivated them to continue working through the toolkit. Seeing the resource was provided by the government provided reassurance and many noted that the service felt encouraging, with a low barrier to entry.

3.3.3 Interim conclusions & limitations

The alpha study demonstrated the toolkit's promise in driving action and provided valuable user data for continuous improvement.

However, the findings were somewhat limited. The sample size was small, with only 67 participants, all of whom were microbusinesses (1-9 employees). Participants were financially incentivised to take part in this research and therefore their motivation to act could have been influenced. In this study, it was also difficult to measure actual action taken due to reliance on self-reporting.

3.4 Private beta: so, does it work in the real world?

Noting the limitations from the described study, the next step was to test the hypothesis of action-based guidance with a wider user group. That is, a greater number of users who were not financially incentivised to take part, who had no strict time limitations on their involvement, and users from across the small organisation demographic.

3.4.1 Approach

The toolkit design was iterated based on the findings from alpha, and the content of the actions were refined. The private beta version included an additional layer of actions, with both the 'Foundation' and 'Improver' layers, which averaged a total of 30.5 steps.

The 'Improver' layer included action-based guidance on topics such as 'Remove unnecessary user accounts', 'Learn how to spot a cyber attack' and 'Check your antivirus and firewall'. A range of partners were used to promote the toolkit to their small organisation audience, ranging from large public sector organisations to cyber security networks, and private organisations.

3.4.2 Results

During the five-month private beta period, there were around 2,500 unique visitors to the service, according to Google Analytics data.

Users who did at least one step, completed an average of 7.9 steps, in comparison to 4.0 in the alpha study. The toolkit engaged small organisations of all sizes, from sole traders to 50+ employees, and the NPS improved to 52 ("Great").

	Alpha	Private beta
Average number of steps complete	4.0	7.9
Total number of steps (on average)	17	30.5
Average number of steps complete as % of the total number of steps presented	23.5%	25.9%
Net Promoter Score	48, "Great"	52, "Great"

Table 2: Summary of private beta study results

This qualitative data has provided a novel understanding of small organisations and how they interact with cyber security guidance, including which actions they take, which they don't, and the reasons for doing so. It has not been possible to extract this user analytics data from existing and previous offers, and this capability will help baseline our impact on cyber resilience in the future.

In addition to collecting quantitative data, 21 in-depth user research sessions were conducted. These provided deeper insights into user experience and led to the development of an audience segmentation for small organisations: 'Unengaged', 'Curious but uncertain', 'Explorers' and 'Proactive protectors'.

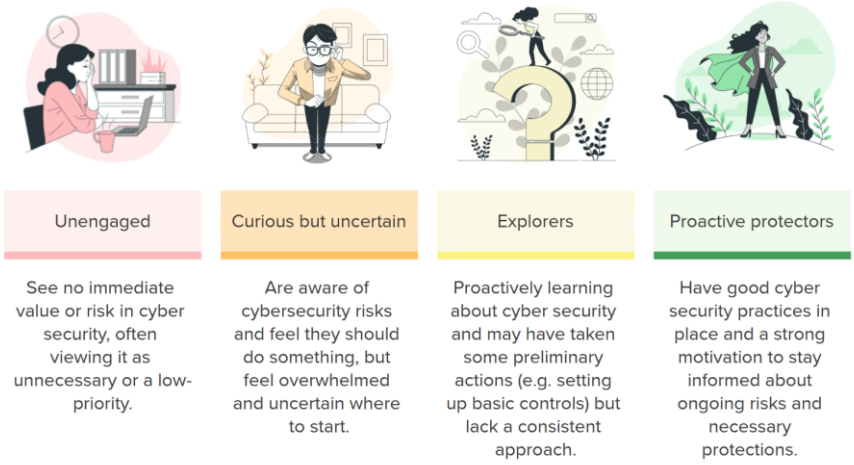


Figure 2: Audience segmentation developed during public beta qualitative research

This audience segmentation helped us understand the differences in attitudes and behaviour towards cyber security, allowing us to give context to where each organisation is in their overall cyber security 'journey'.

3.4.3 Interim conclusions & limitations

Overall, the results from private beta were encouraging. They validated the toolkit's effectiveness with a larger, more representative, and non-incentivised user group, showing users' self-motivation to engage with the toolkit.

The results are more encouraging considering that there were no email notifications, or nudges sent to the users. It can therefore be concluded that the results are a true reflection of users' self-motivation to complete the actions presented.

Within the qualitative research, it was observed that many users already had some interest or motivation to improve their cyber security. It was hypothesised that this is due to the marketing routes used. For example, the National Cyber Resilience Centre Group (NCRCG) proved to be one of the most effective marketing methods, with 21% of users sourced through this route. It is likely that this audience is cyber aware, or have recently been affected by a cyber incident, increasing their need and/or desire to improve their cyber security (more likely to be in the 'Explorers' or 'Proactive protectors' groups).

Any follow-on research, such as the public beta phase, should therefore aim to reach and impact all groups within the target audience, but particularly the 'Unengaged' and 'Curious but uncertain' groups. This will be challenging as those who typically engage with the NCSC's content could be considered 'Explorers' and 'Proactive protectors'.

3.5 Technical correctness: are small orgs doing this stuff properly?

When users are asked to self-report their progress, there are two inherent assumptions. Firstly, that users are reporting accurately; they have actually done the steps that they say they have. Secondly, that users are completing the steps technically correctly. That is, they are reviewing the guidance and implementing the advice in the way it was intended, ultimately improving their cyber security position.

To test these assumptions, a small-scale research study was conducted which aimed to understand if small organisations can implement actions from the toolkit technically correctly when left to implement them without support.

Six microbusinesses were recruited and given seven days to complete as much of the toolkit as they wished. Participants were intentionally given no direct steer on which actions to complete, in order to simulate as close to real-life, unobserved, conditions as possible.

Every action marked as 'Done' or 'Already done' was then assessed by a Cyber Advisor to check if they had been implemented technically correctly. All other responses such as 'Skip' or 'Not done' were discussed to understand why.

Of the 133 steps marked as 'Done' or 'Already done' the Cyber Advisor deemed that 93% were implemented technically correctly:

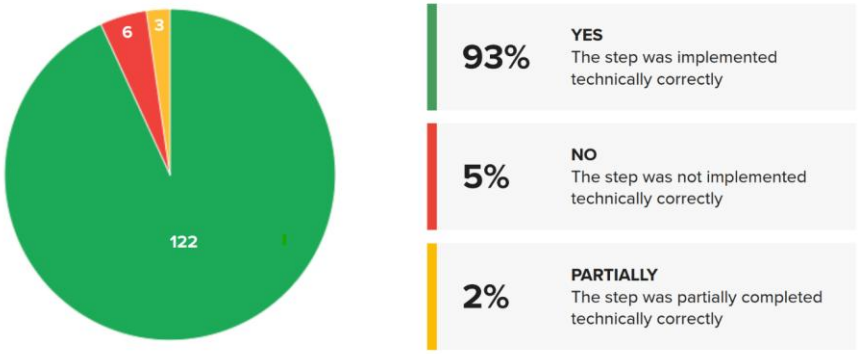


Figure 3: Graphical breakdown of technical correctness study results, as per Cyber Advisor's report

Although conducted with a limited number of participants, the results indicated that users are able to understand and implement the advice provided correctly and importantly, independently.

This research also provides a feedback loop of why small organisations were not able to complete particular steps, which can drive improvement if these themes become recurring in the future.

Repeating this exact experiment with a wider user group may seem logical, but it is impossible to guarantee which steps and actions users will complete without mandating. Therefore, comparisons for exact steps or exact actions are difficult to draw. A repeat experiment therefore becomes a choice between mandating action, which would not replicate 'real-life' conditions, and having a bigger sample size of the same, sporadic data. It could, however, be beneficial to extend this approach to users who have completed actions in the toolkit organically, and outside of the scope of an experiment.

4.0 Overall Conclusions

The results herein are both encouraging and important. Breaking messages into manageable pieces and using gamification aren't new concepts – our daily lives are increasingly shaped by short-form content and instant rewards for even the simplest tasks. However, the use of this combination of approaches in the cyber security world may be novel and has been proven to be motivating and effective for a typically uninterested audience.

Designing a toolkit in this way has enabled the collection of valuable data. This data has demonstrated that 'action-based guidance' combined with gamification elements effectively motivates small organisations to improve their cyber security.

The data extracted has enabled improvement of the content provided and the features and design of how it is presented. These evidenced-based improvement decisions will drive wider and richer engagement with the toolkit, thus further improving the cyber security of small organisations for the betterment of the UK economy.

Additionally, and crucially, the combination of quantitative and qualitative data has provided a novel understanding of the small organisation demographic. This can, and will, act as a baseline for comparison of improvement in future.

The evidence-based, user-centric approach taken within these research studies allowed for continuous improvement throughout, incrementally derisking the eventual outcome. The NCSC hopes that the publication of these results will inspire others, across industry, to consider using design methods which is are similar to the toolkit and realise the benefits of taking an evidence-driven approach.

5.0 Next steps

The public beta version of the toolkit concept, 'Cyber Action Toolkit', was released in October 2025. It includes three layers of protection; Foundation, Improver and Enhanced. If you are interested in using the service, please find a link below:

Cyber Action Toolkit

Cyber Action Toolkit has been intentionally designed to be a starting point in the cyber security journey of small organisations. The NCSC intends that upon completion of Cyber Action Toolkit many small organisations will progress to achieve Cyber Essentials. Cyber Essentials is the NCSC's recommendation for the minimum standard of cyber security for all organisations.

The public beta study will provide learnings on the toolkit's usage at scale and how well the toolkit operates as a gateway to Cyber Essentials. Crucially, by releasing Cyber Action Toolkit to around 20,000 small organisations by April 2026, the NCSC will continue evidencing delivery of National Cyber Strategy 2.2.6.

6.0 Acknowledgements

The NCSC would like to thank Fluent Interaction for their assistance with running the research quoted in this paper.

An additional thanks goes to the public and private sector partners who have marketed the toolkit throughout the rounds of research, and to all the small organisations who have taken part in the research to date.

If you are interested in sending Cyber Action Toolkit to your supply chain, please contact cat@ncsc.gov.uk