10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

techUK Response

Cyber First Programme: Call for Views

09 August 2024

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

About techUK

techUK represents the companies and technologies that are defining today, the world that we will live in tomorrow. The tech industry is creating jobs and growth across the UK. Over 1000 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new and innovative start-ups. The majority of our members are small- and medium-sized businesses.

Executive Summary

CyberFirst has seen significant success in inspiring the younger generation to consider careers in cyber security and techUK welcomes this consultation exploring the future of this important umbrella of activity. techUK members have been significant supporters of CyberFirst since its inception, both in terms of resource and engagement; and industry engagement and buy-in to the scheme is a cornerstone of its success.

In the eight years CyberFirst has been running the programme has reached an impressive 260,000 of various age groups from KS2 to University levels and engaged with over 2,500 schools. This reach is hugely impressive and far exceeds the reach of any other scheme targeting the same age groups. Members have also commented that the real success of the scheme is often hard to quantify in terms of its impact on the wider cyber workforce, because it is engaging candidates often many years before they might enter cyber roles. The signs are positive though, particularly the increased uptake of A Level Computer Science in engaged schools.

CyberFirst also provides undergraduates with £4,000 per year in financial assistance and paid cyber security training during the summer through the CyberFirst Bursary. The scheme has been very successful and techUK and its members would encourage the government to continue providing this type of support to young people. The scheme has also had a significant and welcome impact in terms of improving gender diversity across the sector while plugging the cyber skills gap. Industry is keen to continue playing a role in the scheme's future success.

techUK recognises the rationale behind exploring new delivery models for CyberFirst in future, with a view to ensuring CyberFirst grows to be a truly national programme benefitting all facets of the cyber eco-system, and reaching as many students as possible, across all the nations and regions of the UK. techUK, as well as its sister organisations TechSkills, and our wider membership are keen to play a role in supporting the development of this new model in any way that we can, and we are encouraged by the early engagement instigated by this consultation. CyberFirst was born of a need to increase the number of candidates considering a role in cyber security, a need which has only grown in the following eight years in light of the complex and ever-developing threat in an increasingly digital world.

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

techUK
10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

There are a number of key challenges which must be overcome in developing this new model, including:

1. **The role of NCSC and DSIT**
   Arguably, the success which has been seen by CyberFirst has been possible because of NCSC convening power and brand association, along with Government funding and support. Industry is understandably more incentivised to fill roles as soon as possible and thus less likely to fund early-stage initiatives like some of those in the CyberFirst umbrella. NCSC, as the respected technical authority for the cyber sector in the UK, has a reach and ability to cut across commercial interests which might prevent collaboration through and with other organisations. Whilst a rebalancing of the roles and responsibilities for CyberFirst is a realistic and achievable goal, both DSIT and NCSC will need to play key roles in future, both in terms of settings standards, funding and coordination.
2. **Commercial Challenges**
   CyberFirst has grown to become a significantly broader umbrella of activity than when the scheme started. Any move to a more commercialised model or new entity is very likely to see significant changes to the existing offering, likely narrowing this to focus on those areas which are most commercially viable. Furthermore, setting up a new organisation or being adopted by another business, is likely to cost significant resource, money and time which organisations the size of NCSC and DSIT are arguably more able to cope with.
3. **Ensuring Industry Buy-in**
   Industry engagement is key to any future model CyberFirst could develop. There are countless initiatives working towards the same mission as CyberFirst and there is a significant risk that decoupling (even just in terms of perception) from NCSC/DSIT delivery makes CyberFirst a less attractive proposition to industry who might then focus their energies on other, disparate schemes or develop others. A key success of CyberFirst has been to corral effort around one scheme/goal avoiding duplicate effort and planning for long-term change.

techUK believes that it is possible to overcome the above challenges and further strengthen CyberFirst to build on the success achieved to date. There are significant opportunities to build on the excellent work done to date, for example in broadening the already impressive regional reach and targeting schools and students in places the scheme has struggled to engage previously. In so doing, there is a wider opportunity to strengthen the Public-Private partnership in cyber security further, playing a role in delivering strengthened resilience across all parts of the UK.

Establishing a New Organisation

6.Do you agree or disagree with the proposal to establish a new organisation to deliver CyberFirst? Strongly agree/agree/neutral/disagree/strongly disagree

7.Please give reasons for your answer. [Free text]

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

techUK
10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

8.Do you think industry donations are a viable way for CyberFirst to generate revenue to enable the scheme to scale up? Yes/No

9.Do you think philanthropic/charitable support is a viable way for CyberFirst to generate revenue? Yes/No

10.Do you think government grants are a viable way for CyberFirst to generate revenue? Yes/No

11.Do you think branding/assurance is a viable way for CyberFirst to generate revenue? Yes/No

12.Do you think CyberFirst assets are a viable way for CyberFirst to generate revenue? Yes/No

13.Do you have other suggestions for commercialisation options? [Free text]

techUK agrees that exploring options, including the foundation of a new organisation, is reasonable and could enable CyberFirst to develop a more commercial, sustainable model for the future. We would also suggest that DSIT explores the potential of a wider partnership or of CyberFirst being transferred to an existing organisation, as these could also be viable options with different opportunities and challenges. However, some members have been more sceptical about a new organisation being set up, on the grounds that a reduced NCSC role is likely be a large barrier to success.

Opportunities

Establishing a new organisation could offer numerous opportunities for CyberFirst, including:

- Developing a clearer commercial model by which industry (of all sizes and types) can engage at appropriate levels, through various means including via funding, support, placements and ultimately, jobs.
- techUK agrees that this model would open up new avenues for potential funding, including via charitable and philanthropic contributions, as well as the potential of continued Government support through grants etc.
- Members agree that a new organisation could be well placed to capitalise on potential new revenue streams. However, it is clear that if industry had to pay to use Cyber First materials the majority would not use them, and anything which limits the circulation of content would reduce the success of the scheme. Members understand the challenges for public sector organisations in developing these models and recognise the commercial skills within the private sector could be further utilised to this end.
- A new organisation could arguably be better placed to identify and prioritise areas which require support vs those which are already on a more sustainable footing. For instance, there are a number of parts of CyberFirst which are now well established within communities whereas some parts of the country are not touched at all. A new organisation could perhaps more effectively identify and funnel support/funding to those areas, schools, and communities which need it, whilst allowing those

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

techUK
10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

established initiatives to become increasingly self-sufficient through improved industry partnerships, etc.
- Members have also commented that a new organisation could play a larger role in helping UK cyber firms to navigate the myriad of wider skills initiatives and educational programmes that exist, aligning CyberFirst activity where appropriate.

Challenges

A new organisation is also likely to face a number of challenges that the current NCSC/DSIT model does not. As such, the scope, structure and remit of the organisation needs to be carefully considered to ensure the scheme continues to deliver a high-quality pool of future cyber professionals. These potential challenges include:

- DSIT and NCSC as Governmental institutions are able to cut through and engage more widely than private companies and enjoy exceptionally strong convening power. A new organisation is less likely to have this strength if not adequately supported. Therefore, it is vital the continuing support and engagement from DSIT and NCSC are agreed at the outset to ensure future success.
- Some members have expressed concerns that a new organisation would need to expend a significant amount of time and resource in setting up as an entity. Some have highlighted parallels with other DSIT funded interventions where new organisations have been set up and faced significant operational challenges which arguably require resources for things like HR, Technology, Staffing, Process Development which DSIT/NCSC as large public sector organisations can cope with more easily. Many of these costs are annual costs and as such any new organisation is likely to always have some focus on organisational survival whereas to date the sole focus of CyberFirst has been on the scheme itself. This underscores the need for continued support, engagement and oversight from DSIT/NCSC into the future model.
- Some members have suggested that moving towards a more commercial model will mean that inevitably some parts of CyberFirst fall away in favour of those aspects for which clearer value propositions can be developed. Members agree that this is a significant risk and something that will have to be accepted by NCSC and DSIT.
- Members have commented that this space is increasingly busy, with various organisations playing different roles. A new organisation could arguably be seen as a competitor to existing organisations in a way that NCSC/DSIT are not. Furthermore, a new organisation would need to spend significant time and effort building relationships with key stakeholders across Government and industry, as well as existing professional bodies including the UK Cyber Security Council, CIISEC, CREST and others.

Companies on the whole, find it far easier to offer support to these types of initiatives 'in kind' rather than in cash terms, so setting up a means for industry to contribute effort rather

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

than pay money has more chance of being successful, and resources that are free at point of use are a key component of this.

Finally, any future organisation would need to remain closely aligned with the goals of the National Cyber Strategy and wider Government interventions such as the Industrial Strategy, etc. A new organisation would need to play a significant role in wider efforts, policy development and advocacy for a more coordinated, joined up approach not only to cyber skills but also wider cyber hygiene and resilience for citizens across the entire UK.

techUK and its members are supportive of efforts to move toward either the foundation of a new organisation, or alternative options - which we suggest are explored - such as spinning out CyberFirst into an existing company which could mitigate against some of the set-up and maintenance challenges outlined above.

Organisational Structure

14.Do you agree or disagree that there should be a central body which raises and redistributes funds to regional partners? Strongly agree/agree/neutral/disagree/strongly disagree

15.Please give reasons for your answer. [Free text]

16.Do you have other suggestions for how a new organisation could be structured? Please provide details. [Free text]

CyberFirst has seen real success in key regions including those with longstanding CyberFirst presence (South-West England) and those with newer, partnership led presence (Greater Manchester). Arguably, the most successful model is the one which reaches the largest number of students, so any new organisation should be focused primarily on that, not a single way of doing business. Different regions, schools and communities all have different needs, different levels of industry presence and cyber expertise is concentrated in certain parts of the UK. Therefore, techUK would favour a model by which one organisation (either still NCSC or another entity suitably set-up if workable) has oversight of CyberFirst and focuses on those areas/issues of greatest need, whilst allowing innovative delivery models to exist in those areas CyberFirst already reaches. Some members have suggested that a regional first model, with the new organisation simply a provider of funds, would see varying levels of success between regions, whereas a more proactive central body model might be more appropriate, though there is some disagreement on this.

Similarly, members have highlighted that the big challenge for industry engagement with CyberFirst is that all companies operate in different ways. By definition, companies are commercial entities which are going to require a commercial business case for investment, in comparison to Government which has a clearer ‘public-good’ remit. A successful model in future will allow companies to engage on their own terms, with different levels of support/funding required dependent on scale, need, time and personnel. Doing this in a way

techUK
10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

that is as flexible as possible is likely to increase industry buy-in and multiply the success and reach of CyberFirst initiatives.

Members suggested that there are two clear reasons for industry engagement in CyberFirst. The first and most obvious is access to a future talent pipeline. Clarity as to how this can benefit participating firms is key to unlocking further investment. Secondly, for larger companies, engagement can be part of their CSR portfolios and promote societal value towards the larger shared mission of increased Cyber Resilience. Highlighting the support given by companies and accompanying benefits should also be made clear, creating a two-pronged value proposition for businesses.

Finally, some members have suggested that for some parts of CyberFirst, such as the CyberFirst Girls Competition and student placements for school-age children, industry is already investing significant time and resource of its staff which could be more widely recognised.

Mission

17.Do you agree or disagree that any new organisation should have a 'public good' mission and maintain these core objectives? Strongly agree/agree/neutral/disagree/strongly disagree

techUK members strongly agree that any new organisation needs to have a 'public good' mission at its heart. Furthermore, that mission should be focused on providing awareness and opportunities of cyber security careers to all students across the UK, improving engagement with those from underrepresented communities, whether through improved gender and ethnic diversity or reaching more students from deprived socio-economic backgrounds, and reaching all nations and regions of the UK. It is well documented that there is a gender diversity problem in cyber security, with a global shortfall in the number of women working in the sector. Cyber First has offered a unique opportunity for government to plug the skills gap and improve the gender diversity disparity in the sector by increasing the number of women being offered a place on the scheme. The programme has had a positive impact on gender diversity and members highlighted that industry has been able to engage with the programme by linking this activity to their corporate responsibility objectives making it easier for businesses to engage with the programme.

Some members have commented that too often we talk about CyberFirst as a national programme when in reality it cannot yet claim to reach all parts of the UK.

One concern (already mentioned elsewhere in this response) is that a new organisation is naturally going to be pre-occupied with its own survival and sustainability. NCSC, DSIT and industry partners must work together to minimise the risk that this takes away from the delivery mission highlighted above.

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

techUK
10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

A new organisation will form part of the wider UK Cyber Eco-System, and we must ensure there is clarity on the division of labour between itself and organisations like the UK Cyber Security Council, UKC3 and wider industry/professional bodies. There could well be an opportunity here for a new organisation to offer more coherence to the sector in navigating existing offerings beyond CyberFirst and aligning existing and future efforts which too often are not joined-up or coordinated. To succeed here, the new organisation would need to be trusted and independent and have significant expertise in post from day-one. This must include advocating for improved approaches within Government which are too often siloed between departments, particularly between DSIT and the Department for Education.

Scope

18.Do you agree or disagree that CyberFirst should be expanded beyond cyber security to support the development of talent into other tech sectors? Strongly agree/agree/neutral/disagree/strongly disagree

19.Do you think there should be sector specific initiatives within the programme? Yes/No

20.If so, what age range should these target?

- *Under 10 years old*
- *10-12 years old*
- *13-15 years old*
- *16-18 years old*
- *Over 18 years old*
- *Other [Free text]*

techUK members believe there are significant learnings to be taken from CyberFirst which can benefit other technology areas, including AI, Quantum, etc. CyberFirst is a successful programme which includes content relevant across almost all emerging technology areas and has a reach which outstrips any other similar scheme. Therefore, as we look to fill future roles across these technology areas CyberFirst offers much potential to inform and improve Government and industry efforts to bridge key skills gaps.

Members have been broadly split on the question of adding other elements to the existing CyberFirst scheme. Some have suggested that this is a logical next step with the potential for offshoots like 'AIFirst' or 'QuantumFirst', all based on a joint mission to improve technology skills amongst the student population. Some other members though have argued that this approach would risk diluting the potential benefits CyberFirst poses to the Cyber Security sector. In an uncertain economic environment this approach could lead to smaller specific investment into cyber security skills at the expense of increasingly high-profile areas like AI, based on public awareness, topicality, etc. However, it is clear that we face similar skills shortfalls across the technology eco-system and therefore all Government backed approaches need to be increasingly joined-up/coordinated going forward.

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

techUK
10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Future Role of Government

21.Do you agree that NCSC should remain closely involved with CyberFirst?

Strongly agree/agree/neutral/disagree/strongly disagree

22.Please give reasons for your answer. [Free text]

23.Do you agree or disagree that DSIT should remain closely involved with CyberFirst?

Strongly agree/agree/neutral/disagree/strongly disagree

24.Please give reasons for your answer. [Free text]

25.Do you agree or disagree that the devolved administrations should remain closely involved with CyberFirst in their respective nation?

Strongly agree/agree/neutral/disagree/strongly disagree

techUK has been clear throughout this response that the success of CyberFirst to date is in part due to the role played by the NCSC and DSIT and is clear that this will need be retained to safeguard future success. This includes via funding, which techUK members believe will be required over the long term, particularly for those parts of CyberFirst which are less commercially viable and in terms of setting the standards and ensuring any new organisation retains strong convening power across industry.

Therefore, members agree that DSIT and NCSC need not only to be involved in the future of CyberFirst but also to some degree responsible for it. The risks of not ensuring this are reduced engagement and reach as well as a longer-term divergence from the UK Government's wider plans to develop cyber skills.

At the same time, it is clear that DSIT and NCSC believe they will play a narrower role in future. This is a reasonable and achievable position, however, it should also be well understood that with reduced responsibility and oversight will inevitably mean reduced influence over the future shape of the CyberFirst umbrella as a whole with industry partners playing a wider role in driving this.

techUK members all agreed that wider engagement across devolved and local administrations can only be of benefit to CyberFirst.

Some members have flagged that there is a need for more cohesion across government departments and not just NCSC and DSIT, particularly around ensuring that the curriculum for those in Key Stage 2 has the content required to start to support the emergence of the potential "next generation".

In doing so, there is also a need to ensure that the tutors and careers staff involved in Key Stages 3 and 4, also have the right level of knowledge to sow the seeds for that next generation. Industry could play an important part in terms of outreach, but it still needs to be overseen by DSIT and NCSC.

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org

10 St Bride Street
London EC4A 4AD
T +44 (0) 7331 2000

techUK.org | @techUK

Having industry more heavily involved in CyberFirst is needed, but some members have been sceptical as to how much influence industry could have in keeping the curriculum up to date. These members believe that without having NCSC and DSIT overseeing the curriculum, there is very little chance that industry will be able to make full use of the future talent, which will again continue to fuel the skills gap.

Contact: Jill Broom, Head of Programme – Cyber Resilience, techUK jill.broom@techuk.org