Cyber Skills

An expansion of digital skills, cyber security is central not only to our national security, but also in realising the ambition 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. As such, local economies would benefit from an additional focus on investing in initiatives that increase both the number and diversity of individuals working in the cyber security profession, and providing necessary training and education to build understanding in the general workforce.

- In 2017, over 70% of large businesses, 64% of medium businesses and 42% of micro/ small businesses in the UK suffered a cyber breach.[47]
- We know that only 27% of UK businesses and 21% of charities have a formal policy or policies covering cyber security risks and many organisations lack the knowledge, understanding and confidence around cyber security to implement appropriate measures.[48]

Baseline

Working with your local employers, you should review what skills interventions and policies you can influence. This should include publicly funded provision delivered through HE/FE colleges, apprenticeships, and training providers.

Your baseline exercise should seek to identify gaps, where demand for cyber skills is not being met by the supply of individuals with relevant qualifications, and therefore where investment in a new programme/ provision would be beneficial. It is also important to analyse, where possible, the diversity of people in cyber roles and taking up cyber skills courses in the area, in order to design programmes that successfully engage the local community.

One particular challenge when developing your baseline is the variety of terms used to define 'cyber skills'. An initial definition of a cyber security skill has been set out in the initial Cyber Security Skills Strategy (2018). Cyber security skills have been defined as the combination of essential and advanced technical expertise and skills, strategic management skills, planning and organisation skills, and complementary soft skills that allow organisations to:

- Understand the current and potential future cyber risks they face.
- Create and effectively spread awareness of cyber risks, good practice, and the rules or policies to be followed, upwards and downwards across the organisation.
- Implement the technical controls and carry out the technical tasks required to protect the organisation, based on an accurate understanding of the level of threat they face.
- Meet the organisation's obligations with regards to cyber security, such as legal obligations around data protection.
- Investigate and respond effectively to current and potential future cyber attacks, in line with the requirements of the organisation.

Agreeing objectives

Alongside the cross-sector work with partners to develop initiatives that increase digital capability at all levels, you are encouraged to work with partners to identify, develop and scale up initiatives that address the cyber capability gap at all levels ranging from general awareness to cyber security practitioner. This includes a focus on boosting not only the number, but the diversity of those in cyber roles.

[47] DCMS/Ipsos Mori, Cyber Security Breaches Survey, 2018

[48] DCMS/ Ipsos MORI and Pedley, D., McHenry, D., Motha, H., Shah, J, Cyber Security Breaches Survey, 2018; Ipsos Mori Understanding the UK cyber security skills labour market, 2018

Designing interventions

DCMS is supporting interventions that look to develop the supply of homegrown cyber security talent, whilst funding specific interventions in the immediate term to help meet known skills gaps. This includes a range of initiatives sponsored by the Cyber Skills Immediate Impact Fund (CSIIF), which includes a full-time cyber retraining bootcamp for women, online training portals and a training programme for individuals retraining around existing work and caring requirements.

Alongside this, government has supported a range of bursaries for individuals undertaking both undergraduate and postgraduate courses in cyber security, while also delivering a £20m Cyber Discovery Schools Programme for 14-18 year olds.

Monitoring progress

DCMS will be evaluating all interventions to understand the effectiveness of these in developing a talent pipeline in the longer term, while addressing current cyber skills needs in the immediate term. Alongside this, you should set up evaluation and monitoring strategies that demonstrate the improvement in digital skills in individuals, and what wider effects these improvements have at a local level.

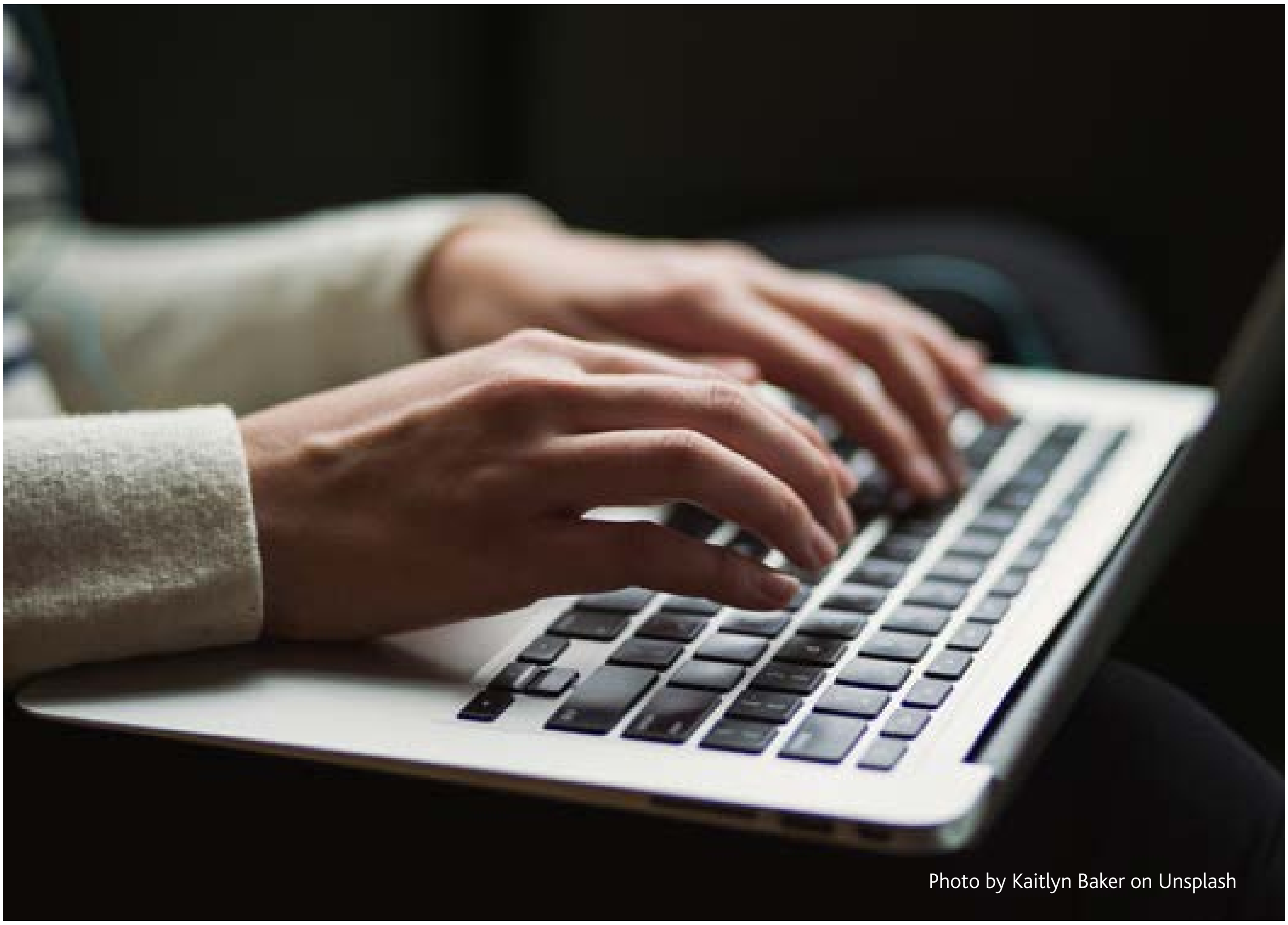

Photo by Kaitlyn Baker on Unsplash