UK CYBER SECURITY COUNCIL®

JUNE 2023

THE EQUALITY ROADMAP

ELEVATING WOMEN IN CYBER

To celebrate International Women's Day in 2023, we held our Elevating Women in Cyber Symposium.

This paper is a culmination of the talks, workshops, and discussions that took place around the topic of encouraging more women to join and remain in the cyber security sector.

Contents

Introduction

We live in a digital society. The UK is a digital economy. Our government, businesses and homes are intrinsically linked to digital processes, integral for the functioning of everyday life in the UK.

Cyber security is, therefore, a key strategic sector for the UK, both for the economy and the long-term security of the nation's homes, businesses and critical infrastructure.
The sector contributes over £10billion a year to the economy, and recorded double-digit growth in 2021/22. The UK is now the third largest exporter of cyber security services globally, with exports more than doubling since 2018.

A failure to properly invest in resources in cyber security would not only threaten the growth of the sector but would present a fundamental and critical risk to economic growth generally, and would mean a genuine, real threat to the UK's prospects. And yet, despite its growth and critical importance, the cyber security sector still faces a diversity problem.

Our Diversity Problem

The DCMS/Ipsos MORI 2021 report into Cyber Security Skills in the UK Labour Market found that the 'cyber sector workforce continues to lack diversity relative to the rest of the digital sectors', and that 'relatively few cyber firms have adapted their recruitment processes or carried out any specific activities to encourage applications from diverse groups'.

Included in this, of course, is gender diversity. The cyber sector remains relatively non diverse in terms of gender; just 22% of the workforce across cyber firms is female, compared to 28% in other UK digital sectors and 48% of the total UK workforce. Just 13% of those occupying senior cyber roles are female.

When looking at the experiences of people in the sector, 37% of women report experiencing barriers in their careers related to diversity and inclusion (compared to 18% of men). 19% of women working in cyber experienced a 'gender-based incident', as opposed to just 1% of males.

NCSC/KPMG found that a significantly higher proportion of women (7%) than men (2%) were considering leaving the sector altogether. The same report found that among cyber firms there was a low awareness of gender diversity as an issue which should be tackled. Indeed, some employers admitting to never having considered the issue.

So what?

But why does this matter? Why should it matter that there are more men than others working in cyber? Is it simply about positive optics for our companies and our sector, or is it about something else?

In 2023 we sit on a wealth of evidence that shows the impact that diversified workforces have. Research has shown that the most gender-diverse businesses are likely to have higher financial returns than those who scored more poorly on diversity metrics.

A more diverse workforce fosters increases in productivity, creativity and innovation – all vital in our fast-paced and ever-changing sector, especially at a time when those threatening our cyber security are themselves becoming more diverse.

It matters because, on top of the kind of sector we want to be and our place in creating a fairer society, diversity brings with it different experiences, perspectives, ideas, attitudes and innovation. A study conducted in 2015 found that groups made up of a diverse range of individuals tend to outperform expert groups that consist of individuals from a single cultural, ethnic or gender group.

As Dr. Claudia Natanson, the chair of the UK Cyber Security Council has said, “a less diverse workforce can stifle innovation and can lead to intrinsic biases within organisations, which cyber criminals can – and will – take full advantage of.”

Improving diversity in cyber security is not something that needs to be done for its own sake. Diversity is not something that should be achieved because it looks good for our companies and our industry. Rather, it should be desired because it is a critical business need, especially for our profession.

In short, a more diverse cyber security workforce means better cyber security.

Elevating Women in Cyber

It is against this backdrop that the UK Cyber Security Council recently held, on International Women's Day, our Elevating Women in Cyber Symposium. Its aim: to celebrate, empower and share the stories of those who identify as women within cyber.

At the event, the attendees heard from a range of speakers working in the cyber profession, at different stages of their careers and from different backgrounds, all changing our industry (and our society) for the better. We heard from women who'd experienced 'non-typical' routes into cyber, who had transitioned in from other sectors. We heard from women who were helping others into the sector, inspiring and enabling the next generation of cyber professionals, and we heard from those working to change our industry for the better, from the inside.

It has been written that the industry needs to feel inspired and connected. It is within our nature to want to feel as though we belong, that we are a part of something. Attendees at the symposium reported that it was the first time they had been in a room full of female cyber professionals, all with their own stories of struggle and success.

Those feelings of being connected and inspired, the feelings of belonging and being in the right place, are just some of the aspects that made the event such a success. This paper comes off the back of this event. It is being written to give momentum to the hope that progress is being made, a feeling that was tangible at the event itself.

A single event, while wonderful and necessary, will not change the industry. Tangible efforts and measures need to be put in place to support the attraction of women into cyber security, and to retain them once they are there.

This paper, which touches on these issues, therefore acts as a signalling call, as part of a movement, to ensure that more women feel able and empowered to seek, attain and enjoy a career in cyber security.

The stories that were part of the symposium form an essential part of this movement, and should be shared widely and loudly. Women entering into the profession would entirely benefit from role models and case studies of those who have succeeded before them in pushing the boundaries of what can and should be achieved.

At present, cyber security remains – in the words of Lindy Cameron, CEO of NCSC – 'a very male profession'. But with the right actions, policies and attitudes, alongside an accompanying sense of community and solidarity that events like the symposium can engender we can, together, change things for the better.

Progress?

This paper seeks to build on the progress that is already being made, not to deny its existence. Progress is already being made, both in attitudes to diversity and to cyber security in general.

Post-COVID, many in the private sector have changed their attitudes towards cyber security and its importance to businesses. According to a report by PWC, nearly all businesses surveyed (96%) have shifted their cyber strategy due to the pandemic, with 50% of UK organisations agreeing that 'cyber security will now be baked into every business decision'.

This presents an opportunity for a change in the way things have been done and in the attitudes that have previously predominated in the sector. As more focus is put on cyber security and more acknowledgement of the fact that it needs to be taken seriously we can build in the fact that more diversity is needed in order to succeed.

There are steps being taken to achieve this; the government's National Cyber Strategy 2022 acknowledged the need for the UK to have a diverse workforce, pledging to prioritise a 'range of concrete actions'. These include support for more women entering the workforce, while building on extracurricular activities such as the CyberFirst Girls Competition.

Organisations like Women in Cybersecurity run alongside schemes like Black Codher in helping to empower and enable more women to enter our industry, giving the skills, knowledge and confidence to do so. While some businesses admitted to never having considered gender diversity, some are making big changes. 39% of cyber firms who tried to recruit in the year after January 2020 say they made changes to recruit more women.

Big business is leading on this: KPMG run a Women in Cyber community, enabling women to feel part of something collective, where they can seek support and advice; Deloitte run their Global Women in Cyber network, which aims to 'promote gender diversity in the cyber security industry by inspiring others, developing our people and building a community'; BAE systems have developed the Women in Cyber group, committed to 'improving the proportion of females within the wider industry' by working with schools and universities; while the Tech Talent Charter commits organisations to improving diversity and inclusion measures at a corporate level.

However, improving our cultures and practices will not be enough if limited to big businesses. DMCS/KPMG found in 2022 that if the two largest cyber businesses were removed from their sample the proportion of females in the workforce falls from 22% to 17%.

Statistics show that 82% of UK firms offering cyber security services are classed as 'micro' businesses – that is, firms with between 1-9 employees. This highlights the need for change across all segments of our sector, from the smallest businesses to the largest.

Barriers to recruitment
A lack of female candidates?

Despite the progress being made in these areas, research has highlighted various barriers and challenges when it comes to increasing workforce diversity in the cyber sector.

Gender diversity is commonly regarded as a difficult issue to tackle. One of the reasons for this is due to a perceived lack of applications from women, with DCMS/KPMG finding that various employers remain of the opinion that there 'was little they could do to improve diversity in cyber teams'. Cited in their 2021 report, concerning neurodiversity, one cyber firm stated, "we haven't discriminated … because we haven't had anyone apply to consider." It was noted that similar opinions were raised relating to female applicants.

This may well be the case. Evidence shows that only 12% of undergraduate students studying cyber security courses are female, rising to 17% of postgraduate students.

On the other hand, some recruitment agents felt that the hiring managers for cyber roles needed more education on unconscious bias and concepts such as blind recruitment, and more knowledge on best practice in writing unbiased job profiles.

This combined with a lack of understanding about the cyber labour market and the different pathways taken by those with cyber skills. This is the case even when firms did undertake formal open job recruitment.

KPMG/DCMS noted the continuing preference for recruiting 'via personal networks and word of mouth recommendations, particularly for senior roles'. This would have large effects on achieving diversity, for the obvious reasons that in an, as yet, male-dominated industry the personal recommendations will tend to promote male colleagues.

It was reported that where recruitment was put out into a formal application process it was done as a fall-back option, used only when networks and personal recommendations failed to find someone suitable.

Where job postings were made public it was found that job descriptions were 'widely regarded to be unrealistic in terms of their requirements'. Recruitment agents outside of the sector reported feeling hiring managers did not understand the labour market and the recruitment pool available.

This would lead to unrealistic and impossible sets of criteria, with candidates unable to meet the demands for jobs which, in reality, encompassed '2 or 3' different jobs. It was felt that this would negatively effect workplace diversity, and lead to potential candidates becoming disillusioned, put off from applying and deflated about their chances of finding work in cyber roles. It is common knowledge that men are more likely than women to apply for jobs even where they do not meet all the criteria listed.

In cases where job adverts were made more accessible to diverse candidates the request often came from HR rather than the hiring managers. This was when HR was consulted, which is not always the case.

Moreover, as listed above, given the size of most cyber firms, it is likely that many will not even have a HR department capable of introducing measures to increase diversity and inclusion.

Given this, despite employers claiming a lack of applications from women, it is likely their recruitment practices possess an element of unconscious bias that is putting women off from applying and harming diversity.

Lack of visible routes

While employers might be unaware about the backgrounds of potential cyber applicants there is an accompanying lack of awareness about the opportunities and routes that one can take into the cyber profession, especially for those who come from a non-cyber/non-STEM background.

At a time when more males than females still study STEM subjects (with some suggesting barriers for females begin as early as primary school) it is imperative that the cyber industry highlights the different ways to break into a career in cyber security.

The UK Cyber Security Council is working to rectify this and has recently relaunched our Cyber Career Framework, alongside our Certification Framework and Career Mapping Tool will help both individuals and employers learn more about pathways into cyber.

The Council's programmes of chartership will also enable those seeking a career in the sector to identify a method by which they can qualify and practice, simplifying the journey into the industry.

The Council will continue to build on this work, and by doing so can change the view of what a typical cyber professional looks like and where they have come from.

Lingering stereotypes

Stereotypes around cyber and the people who work in the sector linger and hinder progress being made in terms of gender equality. What does cyber look like to you? For many, the word conjures up images of male hackers in hoodies, typing away furiously while sat in a basement. On the opposite side, a group of men in suits, looking at screens in the 'war room'. While these may be crude and comic characterisations, stereotypes do matter, because they affect how we feel instinctively about, in this instance, what a cyber person looks like.

The continuation of these stereotypes betray the narrative that cyber can be something different. Cyber is a fast-paced, exciting and vital industry where real differences can be made. There aren't many sectors that can match it in terms of what it can offer.

One method by which gender stereotypes reproduce themselves is through noninclusive language and terminology, as well as marketing imagery and materials. By changing the way cyber security is promoted, to be more inclusive and diverse, we can break down the stereotypes around our industry and what a cyber security professional looks like.

The importance of role models

Measures to increase the accessibility of job postings, improve recruitment practices, and even breaking stereotypes around cyber are all possible, and they all interlink and overlap, having an effect on each other. And yet there are other things that can be done to encourage and inspire more women to seek a career in cyber.

Attendees at the symposium were asked for their opinions on what they would like to have seen, and what would be beneficial for those seeking to enter the industry. One theme that came up time and time again was the importance of role models and mentors.

The history of cyber security is awash with the stories of women who have made vast achievements in our industry, right from the start. From Ada Lovelace to Hedy Lamarr, to Joan Clarke, to Parisa Tabriz, there are stories of inspirational women who have broken down boundaries and succeeded and achieved great things in our sector.

Yet, no less inspirational are the stories of those in attendance at the symposium, women each with their own story of succeeding in an industry that is still male dominated.

More numerous than these are the stories of cyber professionals who were not at our event this Spring. These stories should be told and amplified, not just in order to inspire the next generation of women, but also to create that increased sense of belonging, community and solidarity that it essential to us all.

At the symposium we heard some of these stories, from current cyber professionals. In the room throughout the day there was a sense of shared feeling and experience, and ultimately, of belonging. Increasing the number of female role models and mentors who can share their stories, their experiences and their advice will lead to better female representation in our industry.

It would be misleading to say that no work is being done in this area. There are fantastic organisations leading on this, progress is being made, and this represents something on which the Council can build.

Moreover, this is one of the ways the Council can adhere to its foundational pillar of Outreach and Diversity – creating a platform by which we can hear the voices of female cyber professionals that are so essential to driving the change we want to see.

Recommendations

This paper has looked at some issues regarding the attraction, recruitment and retainment of women in cyber security roles, and from it we recommend a number of measures that can be put in place in order to ensure that progress is being made.

To see these recommendations succeed will require both collaboration and individual work from a number of parties: government, the Council, employers, recruitment bodies, industry representatives, academia, outreach programmes, and individuals.

Recommendation 1: Expand the recruitment pool

Employers need to look beyond those with cyber and STEM backgrounds to include those from 'non-cyber' backgrounds in their recruitment process. Over 80% of those in cyber roles outside of the cyber sector have transitioned from roles in other parts of the business. It is imperative that these should not be excluded from job applications simply because they might not have a cyber-related degree.

Recommendation 2: Use formal job postings for recruitment

It has been noted elsewhere in this paper that formal and open public recruitment drives are often used as a fall-back option for cyber roles, to be used when networks and word-of-mouth recommendations do not provide suitable candidates. This has a negative effect on diversity as, in a male-heavy industry word-of-mouth recommendations and networks are likely to be predominantly male, especially when it comes to recruiting for senior roles.

Recommendation 3: Involve HR when recruiting

Where public job postings were used DCMS/KPMG found that there were aspects of job descriptions that had negative implications for diversity, from unrealistic person specification criteria to unreasonable demands of the job. Recruitment agencies and HR departments should work with hiring managers to ensure their job postings are gender-neutral and accessible to all.

Recommendation 4: Put more focus on non-technical skills

Organisations are starting to realise that non-technical skills are fundamental.

PWC found that new hires are expected to possess more than just technical knowledge. While security intelligence (46%) and the ability to work with cloud solutions (40%) are cited as the most important skills for new employees, this was closely followed by communication (38%), project management (38%) and analytical skills (37%).

If so-called softer skills are given a more prominent position in job vacancy adverts, and given equal weighting with more technical skills, there is every chance this will persuade a more diverse cohort of applicants.

Recommendation 5: Collaboration between big and small businesses

Big business is leading in terms of promoting and empowering women in cyber security. However, the fact remains that the majority of cyber companies in the UK are small or micro businesses, without the resources, time or money to put into a drive to recruit more women into the sector. Big businesses should work with smaller businesses to share resources and best practice when it comes to attracting and retaining women in cyber roles.

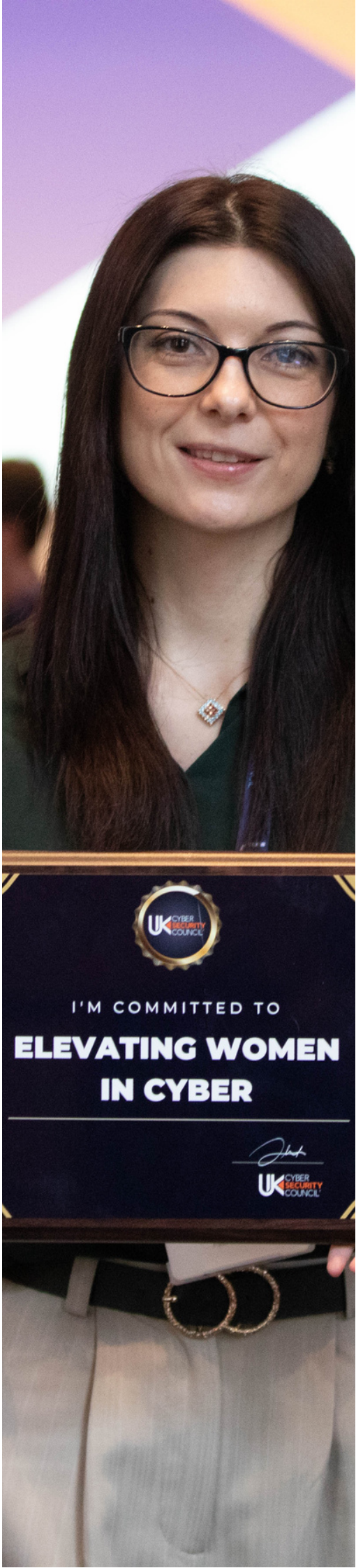
Recommendation 6: Focus marketing on a diverse workforce

Stereotypes persist around what cyber is and who works in it. To counter the image of the boys club that still haunts perceptions of cyber security, marketing and imagery should be focussed on inclusive images, where people from different backgrounds can see themselves as being part of our sector and can feel empowered to pursue a career in cyber security.

The Lifelong Learning Entitlement, scheduled to come in 2025, will allow many more people to train in cyber-focused courses. Changing the image of who cyber security is for before then is vital for us to seize the opportunity to attract more women into the profession, that the LLE can provide.

Recommendation 7: Promote role models and case studies

Research has shown time and again that people are attracted to roles in which they can see themselves. A study from 2019 found that early exposure to cyber security professionals that females can relate to could increase female interest in the industry. Indeed, some have even asserted that the lack of female role models is the primary reason for the gender gap in our profession.



Important work is being done and progress is being made, but more can be done, more can be written, more people can be showcased, more stories can be told.

UK CYBER SECURITY COUNCIL