APRIL 2023

THE DIVERSITY PROCESS FLOW

ETHNIC MINORITIES IN CYBER

In cyber security, as in most computer science disciplines, we often start with a process flow diagram,

if this then that, else this etc, so we can establish a process, predict outcomes, and prepare for undesirable incidents. In your organisation and more specifically, in your cyber workforce, what is your diversity process flow?

Let’s start at the beginning. Are there people in your team from an ethnic minority background? If no, why is that? If yes, are they a minority within your team? If yes, follow the previous answer to our next question. Is it due to your recruitment processes, the language you use externally and internally, perceived or literal barriers in your organisation, education, a lack of role models, or something else?

If this is the point where your process flow struggles, because you haven’t honestly considered the question, we implore you to read on.

Why do we need diversity?

Cyber threats know no borders, attacks can come from anywhere in the world, and with threats on the rise and sophisticated actors developing new ways to control, infiltrate, and expose our systems, coupled with a skills gap of over 14,000 people per year and growing; ensuring we are safe to live and work online is no small feat.

A lack of ethnic minorities in cyber only compounds these issues as professionals and businesses alike miss out on key insights, experience, views, and contributions from people of colour and those from ethnic minority backgrounds. In fact, companies with a diverse workforce are 35%* more likely to experience greater financial returns than their respective non-diverse counterparts, and 70%* more likely to capture more markets.
*Forbes

What can be done?

If we are to tackle global issues, we need a globally inclusive approach.
What does that look like in real terms?
What does that mean for the cyber security sector, and what is the UK Cyber Security Council doing about it?
That is what this paper seeks to answer.

In October 2022, the UK Cyber Security Council held their Ethnic Minorities in Cyber Symposium, the second event of its kind, where we brought together our team, cyber professionals, government officials, academics, business men and women, third sector representatives, students, and partners, to share ideas and put forward practical steps we can all take to increase diversity within cyber security.

Language: Job descriptions and Jargon

When we refer to cyber, often several terms mean the same thing, or one term has many different interpretations, and for someone on the outside looking in, this barrier of protected information can feel hard to penetrate. At the Council we talk of the 16 specialisms within cyber, but this isn’t consistent across the board. With varying job titles, roles, and descriptions, alongside complex terminologies to get to grips with, what can we do to ensure those who are new to cyber can get in on the ground level?

Outside of job descriptions and jargon, some of the terminology we use within cyber is problematic, black-listing vs white-listing, black-hats vs white-hats, a divide has been established where white is good and black is other.

This creates an immediate barrier for those from ethnic minority backgrounds, in a sector where terminology isn't consistent and communication skills are essential, we need to take stock of our own use of language around cyber. Black vs white terminology has existed for centuries and continues to fortify barriers, using this language immediately negates a sense of belonging for people of colour.

Without a clear and consistent approach to roles, titles, jargon and requirements we create a barrier. If, for example, English is someone's second language how do we expect someone to be able to decipher these?

If we are to reach under-represented communities, we need to be speaking in language that appeals to them. We need to explain why cyber is a flourishing sector to work in, and challenge the established routes of lawyer, doctor, etc in order to succeed. One participant from our Symposium, Irfan Hemani, gave a keynote talk titled 'Why don't you be a doctor?'.

Here he spoke about the challenges he faced when pursuing a career in cyber, because his community didn't understand the benefits of this career path. This is something we are all responsible for changing. If we can consistently and eloquently communicate, with language that is inclusive to communities we need to reach, we can begin to welcome more diversity into cyber.

The Council are committed to inclusion, and this means everyone. We ensure we are inclusive in our approach to our internal communications, external marketing, online presence, virtual events and face to face interactions. We use accessible language, to include everyone in the conversation. We create useful documents such as the cyber security glossary available on our website, to help people understand the language of the profession.

There are a multitude of qualifications, both at further and higher education, alongside professional certifications, online courses and accreditations. This makes the landscape very confusing. For many individuals studying in the UK from overseas, understanding which course will secure which role is a complex task. When coupled with the visa implications of trying to secure a 5-year residency in the UK having only a 3 year degree programme, this can create a very stressful situation. If we are to shore up the UK's defences, we need diverse voices and talent to do so, but an uncertain future, a labyrinth of qualifications, and a visa cost in the thousands, can deter great talent from studying in the UK.

There are also several barriers around passing security clearance without a job offer, or without applying from within the UK. As well as the process for applying for some government roles taking months, and requiring UK residency.

When we're recruiting for cyber roles, we need to be conscious of these barriers; we need to look at how we're encouraging overseas applicants if we are to fill the 14,000-job gap per year in the sector. Alongside this we need to look at how we're promoting cyber security within schools, before reaching university what is the perception of our industry?

The Council have developed a career route map looking at the 16 specialisms within cyber which can be used by schoolteachers and lecturers to educate their pupils on cyber security pathways. Through the Council's outreach and diversity work, we will be creating education resources for all ages and backgrounds, to ensure young people with an interest in problem solving, communicating, and computing, are encouraged to pursue a cyber career; and those working within other sectors can change career and develop a passion for cyber security.

Education: Labyrinths and Lifelong Learning

There are a multitude of qualifications, both at further and higher education, alongside professional certifications, online courses and accreditations. This makes the landscape very confusing. For many individuals studying in the UK from overseas, understanding which course will secure which role is a complex task. Coupled with the visa implications of trying to secure a 5-year residency in the UK having only a 3 year degree programme, can create a very stressful situation. If we are to shore up the UK's defences, we need diverse voices and talent to do so, but an uncertain future, a labyrinth of qualifications, and a visa cost in the thousands, can deter great talent from studying in the UK.

There are also several barriers around passing security clearance without a job offer, or without applying from within the UK. As well as the process for applying for some government roles taking months, and requiring UK residency.

When we're recruiting for cyber roles, we need to be conscious of these barriers, we need to look at how we're encouraging overseas applicants if we are to fill the 14,000-job gap per year in the sector. Alongside this we need to look at how we're promoting cyber security within schools, before reaching university what is the perception of our industry?

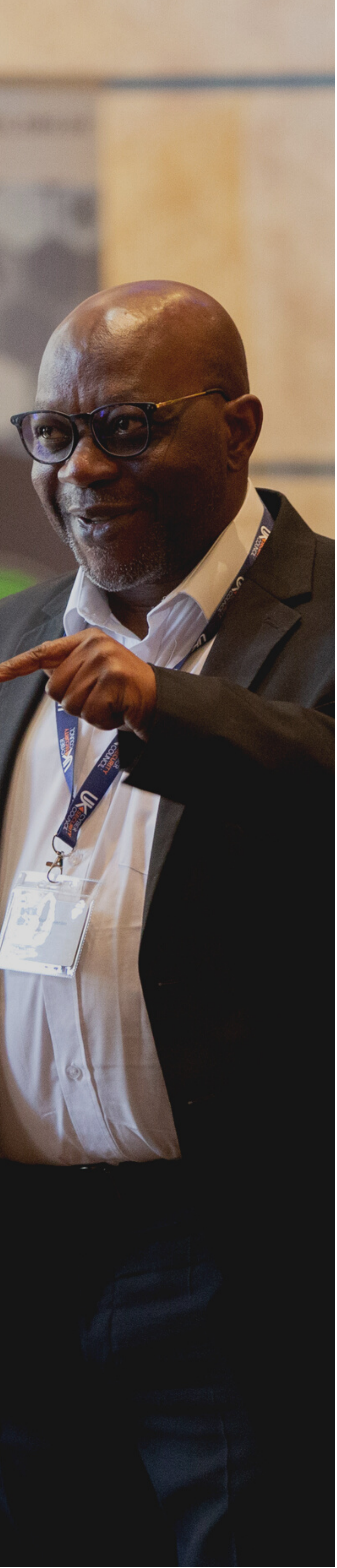
The Council have developed a career route map looking at the 16 specialisms within cyber which can be used by schoolteachers and lecturers to educate their pupils on cyber security pathways. Through the Council's outreach and diversity work, we will be creating education resources for all ages and backgrounds, to ensure young people with an interest in problem solving, communicating, and computing, are encouraged to pursue a cyber career; and those working within other sectors can change career and develop a passion for cyber security.

Perception: Recruiting and Role models

If we’re using the right language, breaking down educational barriers and welcoming a new cohort of cyber professionals, we then need to ask ourselves what is happening in the sector at large that stops bright talented minds from working with us? What is the wider perception of cyber security?

You don’t have to look much further than your TV subscription services to begin to see the problems. Shows like Mr Robot do a fantastic job of showing what a cyber skillset can achieve, but how representative is this? With so many specialisms outside of penetration testing or ethical hacking, the perception is reinforced again and again that cyber = hacking, and it’s our job to bust this myth. With an increase in social engineering attacks, interpersonal skills like communication and developing training are just as vital as coding to protect a company from all angles, but these skills are not at the forefront of our recruitment drive.

Instead, we see a focus on purely technical skills and ‘red team’ mentality, and much less visibility of those creating secure systems, managing vulnerabilities, and leading audit and assurance practices. This makes it incredibly difficult for HR professionals to recruit for cyber roles without specialist knowledge, creating unclear job descriptions and missing potential talent due only to their own lack of education. If every company, in every sector, needs an information or cyber security professional, which we’d strongly argue they do, where are HR professionals meant to go to acquire the knowledge they need for recruitment?



Where we come in

A focus for the Council is solving this issue. At the Council we encourage blind recruitment; removing any identifiers from applications means recruitment can happen without bias, allowing for more diverse teams and candidates who are assessed solely on their abilities. Alongside this recommendation, we will be offering recruitment support for those looking to hire cyber professionals.

This takes many forms, from blind recruitment to our professional title programme, meaning those with the aptitude and knowledge can put themselves through the Council's assessment process to achieve one of three titles – Associate, Principal, and Chartered.

This gives HR professionals a standard to measure against, and an assurance that the candidates they are recruiting have the essential knowledge for their specialism. It also allows for a recognised title for practitioners at every level, whether expert or entry level. This means HR professionals don't have to create long-winded and sometimes unnecessary recruitment procedures.

The Council also encourage diversity on recruitment panels, if we are to welcome people of colour and those from ethnic minority backgrounds into a company, we need to show that they will not be alone, that they are joining a company that values diversity, not hiring only to be perceived as inclusive. But championing diversity means more than hiring people with different backgrounds, we need to see diversity at every level, and ensure we retain talent.

Allowances must be made for those that require longer blocks of annual leave to visit their home country, those that require the same amount of time to celebrate Eid as others do to celebrate Christmas, those that are technically brilliant without having English as their first language, there are many ways to create an inclusive culture.

Consideration must be taken when we recruit, when we train, and when we retain, so a culture of diversity is developed within a company, not just at the front door. Diversity at every level means empowering staff to apply for promotions, to take on larger tasks, to train others and develop themselves, so they can secure their seat in the boardroom.

During our symposium we heard a lot about role models, or a lack thereof for people of colour. You will have heard the saying you can't be what you can't see and this rings true for so many. It can be intimidating and nerve-racking to join an organisation where no one looks like you so having a role model, someone to mentor you, encourage you, to share experiences, guidance and advice can be very comforting, especially for someone joining the profession for the first time. Where there aren't any role models in an organisation we need transparency, we need to make the career trajectory clear for those starting out.

There is no door that says 'welcome to the cyber sector' for newcomers. People find their way in through back doors and side doors, and we need to do better.

As a Council we are mapping not only the specialisms that exist, but the entry routes into those specialisms, the certifications, qualifications, and accreditations that underpin them, and providing a framework for cyber professionals, hiring managers, and those with no background in cyber to get into a thriving, rewarding, and growing sector. But we can't do this alone.

We need your help

To break down barriers we are working with industry, academia, career changers, cyber veterans, and people from all ages, backgrounds, and specialisms to make sure we get this right. We are supporting candidates to understand the landscape. We will provide recruitment support from creating the right CV, to interviewing successfully.

We aim to highlight candidate's experience whether paid or unpaid, and education whether formal or informal, to make sure people from all backgrounds get into the room. And for those already there, we're working with industry to make sure hiring panels are representative, that their language is inclusive, that barriers are removed, and that hiring managers understand what they are recruiting for. Meaning they can secure and retain professionals who excel in their role.

We need every person reading this paper to take up the challenge of increasing diversity within cyber, to look at their own recruitment processes, to speak to their teams, to shift the perception of cyber, champion their colleagues and role models, to work with the Council to demystify the sector.

We need every reader to educate themselves on the frameworks already in place, and to look around the room, every room, and ask themselves 'Is this good enough?', 'Have we achieved the diversity we set out to achieve?' And if the answer is yes, let's work together and build on that best practice, to support other organisations to do the same. If the answer is no, we hope we have provided some initial guidance on steps you can take, now and in the future.

We hope you will be a part of the conversation and will support our mission to increase diverse voices within cyber and come on the journey to a place where we can all see those from ethnic minority backgrounds flourish within our sector.

We’ll see you there.

UK CYBER SECURITY COUNCIL