CREST

Good practice guide for establishing equity, inclusion and diversity as part of national cyber security strategy

January 2023

CREST. Representing the technical information security industry

Published by:

CREST
Tel: 0845 686 5542
admin@crest-approved.org
www.crest-approved.org

Author

Allie Andrews
CEO, PRPR

Principal reviewer

Mike Spain
CEO & Founder — NeuroCyber

Warning

This Guide has been produced with care and to the best of our ability. However, CREST accepts no responsibility for any problems or incidents arising from its use.

Contents

Executive summary

The pandemic has revealed financial inclusion as a crucial bedrock in building resilience. Financial inclusion is one of the most powerful tools we have to fight poverty and lift up living standards. It is also crucial for empowering women.

Figures vary, but there is a significant gap between supply and demand in the cyber security workforce. The 2021 Cyber security Workforce Study from (ISC)2[1] looked at the Cybersecurity Workforce Gap — the number of additional professionals organisations need to adequately defend their critical assets – and found it stood at 2.72 million people. Some 60% of respondents agreed that staff shortages were putting their organisations at risk.

The financial sector has always been one of the largest demanders of cyber security talent. To meet this demand, ensure security of access to banking and other forms of financial services and help lift people out of poverty, it is crucial to attract more (diverse) people into the industry.

This guide describes the importance of having equity, inclusion and diversity at the core of National Cyber Security Strategy and provides advice on how to implement it.

A National Cyber Security Strategy (NCSS) sets out a nation's strategy to ensure a more resilient, trusted and robust cyberspace. Part of that is a clear plan to grow and nurture the talent pipeline, ensuring people have the right skills to fight ever-evolving cyber threats to national security. It is surprising how few NCSS documents mention harnessing the benefits of a more inclusive and diverse cyber security workforce.

There are many reasons why a more inclusive and diverse cyber security workforce will benefit the industry. For example, people from different genders, ethnicities and backgrounds could provide fresh, creative perspectives that are 100% unique to their background, influences and experiences to solve complex security problems. There is also a skills shortage, and it is growing. Put simply, most countries need to tap into more diverse talent, but more government and industry support is needed to make cyber security career entry points more accessible for these underrepresented groups.

This report lays out why equity, inclusion and diversity must rise up the agenda for National Cyber Security Policy and why they are essential to helping nations stay ahead of threats. It also provides advice on how to incorporate inclusion and diversity in National Cyber Security Strategy to ensure the best possible results, because recruiting and retaining more diverse cyber security professionals requires more than policy. It needs genuine collaboration with all stakeholders in the cyber security ecosystem. It may also need significant societal or cultural change at a national or workplace level, which takes time, but the rewards will be worth it.

2. Introduction

2.1 Background

This good practice guide provides advice on how to establish equity, inclusion and diversity as an integral part of National Cyber Security Strategy (NCSS) for the government department that is responsible for cyber security. It also aims to help the government department to scope and introduce an equity, inclusion and diversity programme as part of that strategy.

The report draws upon the best ideas from around the world, from what is already in operation and from current research. This includes current ITU and ENISA guidance, along with work carried out by the UK's DCMS.

The work has been commissioned by CREST International, as part of the Gates Foundation CMAGE (Cyber Security Ecosystem) Project.

2.2 Why equity, inclusion and diversity are important to financial inclusion

To increase the financial position of poorer communities around the world, it is essential to provide them with improved (secure) access to banking and other forms of financial services. In the past, traditional financial services have simply not been available to these communities because of limitations in the way they are delivered.

Because of this, an increasing number of financial services are now being delivered through challenger / neo banks, mobile money and microfinance services. However, these often digital-only services must be reliable and secure if they are going to support traditionally unbanked communities and increase the number of people and businesses with access to financial services.

The 2022 World Economic Forum Risk Report[2] highlights that those developing countries that are rapidly digitising, risk exposing their economies to "new and more intense cyber vulnerabilities, as new technologies and an ever-expanding attack surface enable a more dangerous and diverse range of cybercrime".

The delivery of reliable and secure services requires individuals that are skilled, knowledgeable and competent in cyber security. However, the world is experiencing a skills shortage in this area. Not enough people are entering the industry and there is an urgent need to upskill the existing workforce.

With the available talent heavily in demand, there are high costs and skills development is concentrated in areas where significant investment can be made. This combination of lack of availability and high cost means that countries with significant unbanked populations cannot compete on the international market for skills. Cyber security professionals will often want to work at the forefront of technology and where they can maximise their market value. This makes filling vacancies in emerging markets even more difficult. Even where people can be encouraged to work there, the employment costs may be prohibitive.

While this position does provide significant employment opportunities for local people, there are also obstacles such as a lack of money for education, physical disability and / or gender discrimination which make entry into cyber security employment very difficult.

To meet market requirements, these countries must draw on the widest demographic and work towards removing barriers that limit access to those with a low socio-economic background, physical or mental disability, or gender discrimination. We need to ensure a cyber security career is open to anyone with interest and ability, regardless of who they are.

2.3 Why equity, inclusion and diversity are important for the cyber security industry

2.3.1 The legal case

Having an equity, inclusion and diversity policy means an organisation is trying to ensure it meets legal obligations and avoids breaching any employment regulations relevant to their country. Most democratic countries have laws banning job discrimination related to gender, race, and ethnicity. Others such as, and certainly not limited to, the UK, United States, Canada, South Africa and members of the European Union have broad-based anti-discrimination legislation against gender, race, ethnicity, country of origin, religious beliefs, physical disability, and sexual orientation.

Getting it wrong can mean significant cost to an organisation. For example, a **female city banker sued French bank BNP Paribas** after years of unequal pay and poor treatment and received £2 million in compensation.

2.3.2 The societal case

Perhaps the biggest winner, although the hardest of all to pinpoint and quantify, is society. More opportunity means people are healthier and more productive. This means governments spend less on support. More people in work also means more tax revenue. Everyone wins.

2.3.3 The moral and ethical case

To put this simply, having an equity, inclusion and diversity policy is the right thing to do. People matter. Recognising that everyone is different and has different talents and needs and making them feel welcome in an organisation should be at the heart of any policy.

The moral case for ensuring there is inclusion and diversity in cyber security is clear. Studies such as those quoted in Harvard Business Review's article 'Why Diverse Teams Are Smarter', have shown that having significant levels of diversity provides better outcomes for security teams and better business outcomes. And the moral and ethical case for equality of opportunity is being driven forward by high-profile events and campaigns. Increasingly, people from all walks of life are not just recognising the need for equality but there is also an expectation that their working environments should be inclusive, diverse and that everyone should be allowed to thrive. It is important to note that this can be generational, with different age groups having very different expectations.

Getting it wrong can mean significant reputational cost to an organisation. Worse than cost, an organisation will fall behind the curve, fail to attract top talent and eventually fail to meet client demands.

2.3.3 The business case

There is an abundance of evidence showing that equity, inclusion and diversity provide commercial advantages, deliver better business performance, increased creativity and innovation, along with greater employee satisfaction and talent retention. By employing a diverse range of people, organisations benefit from experiencing diverse backgrounds with different experiences and perspectives. Bringing together different ideas will help an organisation be more effective. For example, the latest McKinsey & Company report — 'Diversity wins, how inclusion matters'[3] highlighted that companies with more than 30% of women on their executive teams were significantly more likely to outperform those with between 10% and 30% women. The report also found ethnically and culturally diverse companies were more likely to outperform their rivals.

Research carried out by Deloitte Australia (Deloitte) and the Victoria Equal Opportunity and Human Rights Commission for their report 'Waiter, is that inclusion in my soup? A new recipe to improve business performance'[4] found companies with greater diversity and inclusion show an 80% improvement in business performance over those with less. They are also 45% more likely to expand their market share and have 33% higher earnings.

For the cyber security industry, the skills shortage, on a practical level, heightens the need to engage with and attract as many people as possible representing the broadest range of diverse backgrounds. However, it is not just about sorting out the skills shortage. When it comes to cyber security the threat landscape is constantly changing and becoming increasingly sophisticated and the only way to get ahead of attackers is to have people who think differently. Only diverse teams can deliver true diversity of thought. A more diverse and inclusive security team is a more innovative and creative team.

Harvard Business Review research[5] also found that more diverse Venture Capital (VC) teams make better decisions. Currently in the USA, only 8% of VC investors are women. Fewer than 1% are black.

2.2.4 Top reasons for increasing equity, inclusion and diversity in cyber for any country

To find employees with the very best minds, skills and experience for cyber it is important to look at the whole of society

Equity, inclusion and diversity practices lead to all staff feeling valued and will improve retention rates

Numerous studies such as McKinsey[3], Deloitte[4] and Harvard Business Review[5] have found diverse companies financially outperform those who are not

More diverse security teams lead to more creative and innovative solutions when they are given the opportunity to do so

Increasingly, job seekers are looking for companies that demonstrate good practice in equity, inclusion and diversity

Improved reputation in the industry for any organisation, public or private sector

2.3 Why should equity, inclusion and diversity be considered in National Cyber Security Strategy?

In most nations, the cyber security industry is a significant employer. This means that the equity, inclusion and diversity of its workplaces will affect many people. Add to this the ever-growing demand for cyber security experts and well-publicised skills shortages and we realise that a more diverse range of talent into the industry is of national and global importance.

A nation needs to have a cyber security sector rich with different backgrounds and life experience to enable innovation and insight and stand a chance of meeting the challenge of growing threats. A more diverse workforce is essential for the sustainability of a nation's cyber security sector. By far the most effective way to reduce barriers is to include equity, inclusion and diversity in national policy and define a process to support it. There is, however, currently a lack of guidance on how to do this.

All the countries reviewed for this report with a National Cyber Security Strategy have statements about the need to increase the number of people in the cyber security industry. Most also talk about the need to improve the competence of those already working in the industry, as well as ensuring competence levels of those entering the industry, their continued development and measurement of their skills. However, few had any practical advice on either increasing the numbers or how higher competency could be achieved.

To increase cyber capability, it is clearly important to establish academic and professional training and development programmes and provide a flexible and tailored pathway to keep people engaged and excited. These are essential if a country is to move toward self-sufficiency in cyber security. However, it is also essential that these programmes are made available at a cost that communities can afford, to ensure there are fewer socio-economic restrictions. Outreach is essential — communities need to be made aware of opportunities. At national level, training and development programmes must be made inclusive and accessible to everyone regardless of their background, gender or disability to ensure as diverse as possible a workforce.

If a country is to grow its cyber security capability and invest in a new generation workforce, national policy is required to act as a focus for investment. Part of this policy needs to focus on the development of skills, and it is vital that countries include equity, inclusion and diversity in the workforce.

> "We need diversity of thought in the world to face the new challenges."
>
> **Tim Berners-Lee**

The last decade has seen a great deal of discussion over the shortage of skilled cyber security practitioners — and many efforts have been made to address this issue. It must come from a national level to difference and it must be written into policy. It has to be properly tracked to ensure we know what is working and what is not, and it must include diversity and inclusion.

3. What is equity, inclusion and diversity?

3.1 Defining equity, inclusion and diversity

Equity, inclusion and diversity should always go together. There is little point in a workplace having one without the other, however, they are distinct from one another, and it is important to make that distinction clear. When incorporating them into National Cyber Security Strategy and any national programmes, both need to be understood and considered to ensure they can be implemented properly.

Inclusion is ensuring everyone is valued, whatever their differences may be. It is about ensuring everyone can thrive in the environment, that they feel like they belong without having to change who they are to fit in with the organisation. It is about making everyone feel like they matter and enabling them to perform to the very best of their ability, whatever their background, gender, race or individual circumstances.

Diversity is about recognising difference. It describes the different personal, physical and social characteristics — for example gender, ethnicity, age, and education of an individual.

It is deliberate that in this report we are referring to inclusion first. In many policies and other documentation, inclusion comes second but without inclusion you simply cannot achieve lasting and meaningful diversity. It is recommended that in all policies inclusion is listed first as a reminder of its importance.

> "Diversity is being invited to the party; inclusion is being asked to dance."
>
> **Verna Myers, Diversity and Inclusion Expert**

As an example, if various unconscious biases are overcome, an organisation will manage to employ diverse people and build a diverse team. However, it is only through having truly embedded inclusive policies, processes that are carried out in an inclusive way in support of policies, and a culture of inclusivity that diverse team members will feel valued and able to contribute equally to the team. They will stay and the team and the company will thrive.

> "Diversity can be mandated and legislated, while inclusion stems from voluntary actions."
>
> **Winters, 2014**

3.1.1 Equality vs equity

Equality and equity may sound very similar, but they have very different meanings — and it is important to understand the difference.

The UK's **Equality and Human Rights Commission** defines **equality** as: "*Ensuring that every individual has an equal opportunity to make the most of their lives and talents.*" However, in practice this often means simply giving people the same access and the same opportunities. The problem with this is that not everyone has the same mental or physical abilities.

And crucially, not everyone is perceived in the same way by others.

Equity is about giving people what they need to make things as fair as possible. It is about levelling the playing field. It is not about making it easier for any one group than another, it is about making it the same.

So, the concept of equity might include, for example, providing the tools people need to do the job, making reasonable adjustments to the workplace and recognising unconscious bias in recruitment advertising language.

It is only through providing *equity* that *equality* can be achieved.

3.2 Key areas of diversity and characteristics

Areas of diversity are potentially limitless since diversity really means anyone who is different. However, it is important to attempt to define the term. It is only by defining some of the key areas that solutions to creating a more inclusive workplace can be considered. Some areas of diversity are covered by law, such as gender and race in most countries. Discrimination in the workplace is illegal. In fact, the overwhelming majority of countries with 155 of the 173 examined for a World Bank report, had gender-based anti-discrimination embedded in the law.[6]

Legal obligations differ from country to country, with South Africa having some of the broadest anti-discrimination laws. Section 9 of the South African Constitution states — *"all persons are equal before law and there can't be any discrimination on the grounds of race, gender, sex, pregnancy, marital status, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture, language and birth."*[7]

The picture isn't the same all around the world for things like sexual orientation, disability or social origin. Of course, embedding something in law is not the same thing as creating a nationwide or even company-wide culture of inclusivity, but it is a starting point.

If you search online for diversity in the workplace definitions no two are the same, and that is part of the problem when it comes to things like measurement of diversity programme success or understanding what best practice looks like. It is difficult to make like-for-like comparisons when there are not any globally or even nationally agreed lists and definitions.

For the purposes of this report, based on an analysis of existing lists, we recommend the following points as a minimum standard for a National Cyber Security Strategy to consider and potentially measure on its diversity list.

3.2.1 Age

This represents having a diverse range of ages. According to CIPD research, only a fifth of employers have a board level strategy to manage a more age diverse workforce[8]. This is a statistic that needs to improve.

Ageism is having a negative bias against a person or a group of people because of age. Typically, this would be younger or older adults, but it is important to recognise that it can happen to employees of any age depending on the specific culture of the organisation or even the country.

Despite ageism potentially occurring at any age, it is more likely to happen when people are older and there are many more negative aging-related language stereotypes — such as 'over the hill' and 'past it'. Depending on the makeup of the nation and the maturity of the cyber security industry there could be a wealth of older untapped talent with transferable skills or even already working in the cyber industry and to be upskilled.

Simple tips

- Improve recruitment and workplace practices to eliminate conscious and unconscious age bias in language
- Ensure employees are supported for health and wellbeing
- Offer flexible working
- Offer phased retirement options

3.2.2 Disability

National policies and laws on rights for disabled people in the workplace differ, as well as what disabilities they cover. However, many countries have signed up to the United Nations Convention on the Rights of Persons with Disabilities (CRPD). This states "Countries are to recognize that all persons are equal before the law, to prohibit discrimination on the basis of disability and guarantee equal legal protection (Article 5)."[9]

The Americans with Disabilities Act (ADA) of 1990[10], as an example, protects 'qualified individuals' with disabilities from unlawful discrimination in the workplace also ensuring they have equal access to training and career development. Under the act, it defines a disability as a physical or mental impairment that substantially limits one or more major life activities.

There is a good list of the different policies and laws for African countries here.

3.2.2.1 Visual impairment

According to the International Classification of Diseases 11 (2018) by the World Health Organisation[11] — vision impairment falls into two groups: distance and near presenting vision impairment.

According to the World Health Organisation, from the estimated 2.2 billion people globally with a near or distance vision impairment almost half of them could have been prevented, or are yet to be addressed.[12]

Rates of unaddressed near vision impairment are estimated more than 80% in western, eastern and central sub-Saharan Africa, and in high-income regions of North America, Australasia, Western Europe, and of Asia-Pacific they are lower than 10%.[12]

How well someone can live with their vision impairment, according to the World Health Organisation, depends on the availability of prevention and treatment interventions, access to assistive products and whether the person experiences problems with inaccessible buildings, transport and information.

Hearing loss worldwide: by the numbers

466 million
Number of people now experiencing hearing loss

$750 billion
Annual global cost of untreated hearing loss, in US dollars

900 million
Number of people estimated to have hearing loss by 2050

1.1 billion
Number of people between 12 and 35 years old at risk of hearing loss due to noise exposure

60%
Percentage of childhood hearing loss resulting from preventable causes

Simple tips

- Verbalise non-verbal communication — e.g., say yes or no instead of shaking the head
- Use descriptive words that can aid communication for things such as shapes and colours
- When entering or leaving the room, announce arrival or departure and include your name
- If someone has a service animal, do not interact with the animal without asking permission first
- Don't avoid words like see and look — people with visual impairments use these too

3.2.2.2 Hearing disability — types of hearing loss

Sensorineural hearing loss

According to Healthline, over 90% of all hearing loss in adults is sensorineural. This means damage to the auditory nerve or the structures of the inner ear and ranges from mild hearing loss to profound deafness, depending on the amount of damage. Being exposed to sounds louder than 85 decibels can harm the ear.

Nerve damage to the inner ear's structures — created by loud noises, genetics, or aging — are also causes. Occasionally illnesses such as measles can be the cause.

Conductive hearing loss

This is an issue with the ear canal, eardrum, or middle ear and its bones, meaning conduction of sound is interrupted from the external and middle ear to the inner ear.

Conductive hearing is different from sensorineural because the hearing loss is caused by sound blockages in the outer and middle ear.

A variety of issues cause conductive hearing loss, including:

- Ear infections
- Fluid in the middle ear
- A hole in the eardrum
- Benign tumours
- Earwax stuck in the ear canal
- Infections in the ear canal, sometimes called swimmer's ear
- An object stuck in the outer ear
- Incorrect formation of the outer or middle ear

Conductive hearing will usually affect loudness rather than clarity of sound, so symptoms include:

- Difficulty hearing speech
- Muffled conversations
- Strange odour from the ear
- Pain / pressure in one or both ears
- Ear discharge

Mixed hearing loss

Mixed hearing loss is a combination of conductive damage in the outer or middle ear and sensorineural damage in the inner ear. Anything that could cause either sensorineural hearing loss or conductive hearing loss could potentially cause mixed hearing loss.

How hearing loss impacts working life

- Challenges in communication
  Hearing loss causes challenges for people when they need to communicate with other people. This can create obstacles to getting a job and creating and maintaining professional relationships
- Difficulty learning
  Communication is essential for learning so hearing loss will create problems. Hearing loss can hamper academic achievement, and alter vocational choices
- Increased need for assistance
  Assistive devices for hearing loss include tools such as captioning, telephone amplifiers, and flashing and vibrating alarms
- Stress
  The stress related to hearing loss-related challenges can lead to other health issues
- Loss of balance
  Some types of hearing loss can lead to balance problems
- Social and emotional effects of hearing loss
  Have difficulty communicating with others can lead to feelings such as embarrassment, loneliness and frustration

Simple tips

- Always face the person and ensure they have an unobstructed view of your face and mouth. Remember that it doesn't matter whether they read lips or not, your body language will help with communication
- The different sign languages are proper languages (BSL, ASL, BANZSL etc) and each of them has its own grammar, vocabulary and style. This means that written communication may be more complicated with people who use signing as their primary language. So, when you are using written communication, it is important to keep sentences sort and simple
- Always speak at a normal volume when speaking to someone with hearing aids

3.2.2.3 Ambulatory disability

An ambulatory disability is any condition that impairs a person's ability to walk. Causes can include physical damage to, or loss of, a limb or multiple limbs, spinal cord injuries, neurological disorders and brain injuries.

Simple tips

- Always ensure workplace accessibility
- Always ask someone if they need help — never assume.
- Always respect personal space

3.2.2.4 Cognitive disability

A cognitive disability will lead to difficulty concentrating, remembering or making decisions.

There are many physical, mental and emotional conditions that can contribute to someone having a cognitive disability. They can be acquired at birth or early childhood; others may be acquired later in life due to brain damage or mental health conditions.

Simple tips

- It will help to build in extra time when planning meetings. Some people with cognitive disabilities may have more difficulty taking in, processing and responding to information
- Allow for breaks during extended meetings

3.2.3 Neurodiversity

According to the Neurodiversity Association, neurodiversity is an umbrella term covering a number of neurodevelopmental conditions.

The business case for diversity was outlined earlier in this report. For the cyber security industry to flourish, address its significant skills gap and be truly inclusive, it cannot afford to exclude the neurodivergent. To do so risks missing out on much needed talent. When we talk about the business case for diversity in the cyber security industry to stay ahead of the attacker, one of the most important things is the importance of 'diversity of thought'. The industry needs people with different perspectives, backgrounds and experiences in a room. However, despite this, being perceived as 'different' has created a systemic barrier to employment for those who are neurodivergent.

A lack of awareness and understanding means that all too often the neurotypical recruitment processes, management practices and workspaces make things challenging for people who are neurodivergent. However, for what can be small and inexpensive adjustments, there are big wins to be made. Employers surveyed by the US Job Accommodation Network found that as many as 59% of common adjustments cost nothing for the employer[13]. Technology, in particular assistive tech in the form of apps such as speech-to-text software, is facilitating both the inclusion and performance optimisation of neurodivergent people such as non-verbal autistic and dyslexic people.

Dyslexia

- Creative thinking: Dyslexics often think in images, making their brains great at visual processing
- Seeing the big picture: Those with dyslexia have the ability to connect ideas, spot patterns and see trends where others may not
- Thinking outside the box: Dyslexics can be great at problem solving, sometimes taking a different approach to an issue that may have been missed

Autism

- Concentration: Autistic people are brilliant at concentrating on what they are doing
- Creative ideas: People with autistic traits excel in producing creative ideas
- Productivity: People with autism can be extremely productive when given a chance to reach their full potential

Asperger's Syndrome

- **Intelligence**: People with Asperger's Syndrome may be of average or above average intelligence
- **Routine**: To try and make the world less confusing, people with Asperger's may have set ways of doing things
- **Knowledge**: Some are exceptionally knowledgeable in their chosen field of interest. This can be developed

Dyspraxia

- **Empathy**: Those with dyspraxia — difficulty in performing coordinated movements — can be clever and creative and have a have a strong sense of empathy for others
- **Motivation**: Once those with dyspraxia get started with a task, they are determined to succeed with it
- **Innovation**: Those with dyspraxia generally have very complex minds that excel at innovation

Attention Deficit Hyperactivity Disorder (ADHD)

- **Hyperfocus**: Those with ADHD have extreme drive to channel attention and energy into work
- **Resilience**: People with ADHD often push past setbacks, adapting well to new strategies
- **Persistence**: They will set their sights on something and do it

Simple tips

- One-size does not fit all — whether interviewing or ensuring the workplace is inclusive — ask if there is anything that would help
- Adjust the interview process and style to ensure autistic candidates are able to portray their skills properly. For example, provide interview questions in advance
- In the workplace always give clear, concise instructions, this is particularly helpful for autistic staff, but really good for everyone
- Provide the option for a well-structured working environment for those helped by having fixed times and structure
- Consider a mentoring programme for neurodivergent individuals in the workplace / academia
- Provide verbal as well as written instructions
- Signpost the key points to read in a document for people with dyslexia
- Provide additional time for completing forms / written tests
- Offer screen reading software / speech to text software
- Provide a quiet space
- Have regular feedback sessions to track progress and enable adjustments
- Educate other employees

3.2.4 Gender

Gender diversity concerns the fair representation of people of different genders. It will typically refer to the measurement of the ratio of men and women. However, it also includes people of non-binary genders and transgender people.

In the cyber security industry globally, figures vary a lot, but there are around 15 — 25% women working in the industry in various roles.

> Research by the UK's Department for Digital, Culture, Media & Sport (DCMS) for its Cyber security Skills in the UK Labour Market 2020 report[14] suggested that less than 15% of cyber roles are filled by women. This is disappointing since it followed a number of initiatives globally and shows little improvement on previous figures.

The (ISC)² Cyber security Workforce Study, 2021[1] found that globally, the industry remains predominantly male and Caucasian at 76% in North America and the UK. It actually reveals a lower percentage of women in the sector in 2021, 20% compared to 25% in 2019. However, it also suggests that this may be because more professionals holding formal cyber security roles, who are more frequently men, participated, and that a more reliable estimate of women in the cyber security workforce remains at 25%. It is difficult to know accurately if this is the case because the study does include IT professionals who are also responsible for cyber security along with dedicated formal cyber security professionals. However, the fact it also identifies that more men hold the formal cyber security roles is also important.

The slower pace of change is not unique to the cyber industry. A 2019 World Bank report 'women, business and the law 2019: a decade of reform'[15] found that in 131 economies there have been 274 reforms of laws and regulations. Some 35 economies had implemented new laws on workplace sexual harassment, protecting nearly two billion more women. However, the typical country was still only providing women with three-quarters the rights of men in the measured areas. Only Belgium, Denmark, France, Latvia, Luxembourg and Sweden had achieved equal rights. Countries in the Middle East and Sub-Saharan Africa had average scores of 47.37% of the rights of men. Encouragingly, the report highlighted positive trends in South Asia, East Asia and Sub-Saharan Africa as the three most-improved regions for the decade, so it is likely that there have been further improvements over the last two years.

Simple tips

- Remove any gender biases — conscious or unconscious — whether writing job descriptions, training materials or policy documents
- Implement equal compensation practices
- Sell cyber security as a long-term career choice with personal development
- List essential and non-essential requirements more clearly in job specs. Women are far less likely than men to apply for jobs that lack detailed job specs

3.2.5 Sexual orientation

This simply refers to a person's sexual attraction towards either the same sex, the opposite sex or to both sexes. While it applies to all people, gay, lesbian and bisexual people are most at risk of prejudice and discrimination.

In a survey carried out by the UK's Institute of Engineering, 29% of lesbian and bisexual people would not consider a career in STEM for fear of discrimination.[16]

Simple tips

- Educate recruiters to focus on skills and experience needed to do the job and only ask for personal information relevant to the role
- An up-to-date Equal Opportunities Policy is essential, and must be clear on how people are supported if they have an issue and any processes they need to follow
- Recommend managers are trained on issues regarding sexual orientation and are up to date on the organisation's policies and national legislation

3.2.6 Race and ethnicity

Race and ethnicity are both commonly used, often interchangeably. However, although there is some overlap, they do have different meanings.

Race is the group or groups that a person identifies with as having similar physical traits. Race defines people who have a shared ancestry. However, it is important to recognise that it is commonly agreed in the scientific community that race is a social, not a biological, construct. There is no gene common to all white people or all black people. "Assumptions about genetic differences between people of different races have had obvious social and historical repercussions, and they still threaten to fuel racist beliefs." — Scientific American: Race Is a Social Construct, Scientists Argue.[17]

Ethnicity is broader than race. It is the group of people a person identifies with according to their national, tribal, religious, linguistic, or cultural origin or background — for example African-Caribbean, Indian or Irish. Essentially it is something acquired, based on where people were brought up and shared cultural and familial bonds and experiences.

A study called 'Tech leavers' by the Kapor Center for Social Impact[18] found that almost 25% of underrepresented minorities and women of colour working in tech had experienced stereotyping. It also found that 40% of Black, Hispanic and Native American men had left a job due to unfairness and racism.

Simple tips

- Write a policy that specifically addresses racism in the workplace
- Train employees on how to avoid discrimination and racism and encourage more to step forward as allies
- Foster an environment of open communication so employees are more likely to report racism, even if they see it happening to someone else
- Ensure all reports are followed up immediately
- Make sure all key decision-making teams include people from diverse backgrounds, to their visibility

3.2.7 Religion or belief

In many countries a person's religion or belief may be protected against discrimination under law. This may also cover people being discriminated against for lack of religion or beliefs — for example atheists.

What is religion?

A person can be discriminated against for belonging to an organised religion, for example:

- Islam
- Christianity
- Judaism
- Sikhism
- Buddhism
- Hinduism

Religion also includes smaller religions or sects such as Scientology or Paganism.

People can belong to a specific denomination or sect within a religion and discrimination can occur:

- Sunnis or Shi'as within Islam
- Orthodox or Reform Judaism
- Protestants, Methodists or Jehovah's Witnesses within Christianity

What is religious belief?

Religious belief is the belief in the religion's central articles of faith. For example, within Christianity this is that Jesus is the Son of God. This can also include elements of beliefs that are not actually shared by everyone who practices that religion.

Some examples of religious beliefs.

- A Christian should wear a cross
- A woman within Islam should cover their head
- The belief in creationism

What is a philosophical belief?

A philosophical belief is a non-religious belief such as humanism and atheism. It is always something an individual strongly believes so is a fundamental part of their life. Man-made climate change has been defined as a philosophical belief, however political beliefs have not.

The belief must be acceptable so cannot conflict with the fundamental rights of others. For example, if someone's belief was racial superiority for a particular racial group or in the rights or one gender over another, this would not be acceptable.

Simple tips

- Employers should ensure they are aware of the meaning of religion or belief
- Assess employee requests relating to religious or philosophical beliefs on an individual basis
- Always carefully consider any requests for flexible working because of religion or belief
- Consider providing a quiet room for prayer and meditation
- Be sensitive to cultural and religious needs when organising events or training
- Be sensitive to religious beliefs when writing policies, job adverts, training and other documentation
- Clearly set out unacceptable behaviour relating to religion or belief in policy

3.2.8 Socio-economic background

Socio-economic background is the combination of an individual's income, occupation and social background that will play an important part in an individual's chance of future success. As well as the perseverance and ability of the individual, the amount of opportunity there is for social mobility will depend on which country the person lives in and sometimes even which area within that country.

Simple tips

- Encourage businesses to work with charities on joint initiatives for getting people into work
- Provide subsidised or free training and scholarships
- Engage with schools in disadvantaged communities to deliver cyber learning materials, workshops and webinars

4. National Cyber Security Strategy

4.1 What is a National Cyber Security Strategy?

A national cyber security strategy exists to improve the overall ability of a nation to protect itself from cyber threats. A national cyber security strategy aims to provide a framework for prevention, preparation, response and recovery to cyber threat. Having one is a key indicator of a country's cyber security maturity and readiness. Implementation will help reduce the scale and impact of cyber attacks.

4.2 Building equity, inclusion and diversity into National Cyber Security Strategy

Experts from over 20 organisations shared their experience, knowledge, and expertise to produce the 'Guide to developing a National Cyber Security Strategy'.[19] The organisations involved included: Council of Europe (CoE), Commonwealth Secretariat (ComSec), Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU). Axon Partners Group (Axon), the Cyber Readiness Institute (CRI), the Global Forum on Cyber Expertise (GFCE), and the Organization of American States (OAS).

The World Economic Forum (WEF) contributed to the Guide as observers. It was released in December 2021 and is the most comprehensive guidance for building a national cyber security strategy available.

The guide's objective is to aid and stimulate strategic thinking and help national leaders and policymakers worldwide to establish and implement national cyber security strategies. In December 2021, the ITU estimated that more than 127 countries had cyber security strategies in place, and many of them used the Guide as a reference.

Focus area 5 in the Guide — Capability and capacity building and awareness raising — refers extensively to skills development. However, in terms of diversity, it is only gender that is specifically mentioned and only refers to encouraging more women into security. Of course, this is an extremely important area, and any national cyber security policy should include provisions for closing the gender gap both because it is the right thing to do and to help with the skills shortage.

An inclusive and diverse cyber security workforce will help improve a country's economic and social position. The importance of equity, inclusion and diversity reaches far beyond economic benefits, into societal fairness and equity. Therefore, building it into all areas where the national cyber security policy looks at skills development will not only help address the skills gap, but help build a better, stronger and more resilient sector.

Equity, inclusion and diversity have to be seen as a national opportunity. They must be written into national policy to eventually become embedded as part of every security organisation and security team's culture. So, when national cyber security policies talk about skills and the need to build more native capacity and capability, it can't just be designed for one group of people, for example, women or more university graduates. It has to be for more people from all walks of life — that is diversity. It must attract anyone with the aptitude and the desire to work in security and remove the barriers, both real and perceived, that are stopping them from applying or studying to enter the industry.

4.3 Examples of equity, inclusion and diversity in National Cyber Security Strategy

Despite the clear benefits for including equity, inclusion and diversity in National Cyber Security Strategy, there are very few examples where they are mentioned — and fewer still go into detail.

4.3.1 The UK National Cyber Security Strategy

The UK's National Cyber Security Strategy, both the 2016 (1.1) edition and the more recent December 2021 (1.2) edition ensure the UK has diversity within the cyber security workforce as a dominant theme.

The 2021 strategy states that the government is: "*taking steps to increase the diversity of the cyber workforce — recognising that being able to harness and nurture the skills and talents of the whole population is critical for our national security.*" It also clearly states that "*Central to the UK's ambitions will be developing a sustained and diverse supply of highly-skilled people into the cyber workforce, capable of securing the core elements of the digital economy, as well as innovating and developing new approaches*" stressing the importance of diverse skills to the UK's cyber security industry.

The policy also outlines various initiatives, such as the government's flagship CyberFirst programme, and the CyberFirst Girls Competition, designed to interest more school aged girls into cyber security. The Cyber Choices Programme, run by the National Crime Agency, increases access to education and career opportunities for at-risk young people.

There is a lack of concrete targets or measurements of what success might look like. The focus is on encouraging more women into cyber and on neurodiversity and autism in particular.

4.3.2 National Cyber Security Policy 2021, Pakistan

Pakistan's National Cyber Security Policy recognises the importance of skills development both in terms of new entrants, taking about new cyber security academic degrees and people upskilling. It recognises the need for up to date, relevant, professional skills to improve cyber security resilience. It highlights the skills demand and supply gap in the digital workforce as a significant challenge, as well as the absence of a mechanism for delivering more of these skills and resources being a threat to the country's cyber security.

Several suggestions address these issues. However, at no point is inclusion and / or diversity mentioned. There are areas of the policy where it would be simple to weave in, for example, section 3.9 Capacity Building — *'Formulate and implement customized human resource development programmes to fulfil the Cyber Security needs of both public and private sectors'* could easily be expanded to say *'Formulate and implement customized human resource development programmes that are fully inclusive and diverse, to fulfil the Cyber Security needs of both public and private sectors.'*

4.3.3 National Cyber Security Policy and Strategy 2021, Nigeria

Section 8.2 of the National Cyber security Policy and Strategy 2021, Nigeria — 'Robust Cyber Security Workforce' covers the need to develop local talent and states it is the government's role to create pathways for this. The focus is mainly on cyber security education, skills acquisition and professional development. A key policy is the establishment of a National Cyber Security Training Institute which would cover certification, career tracks and courses. The policy talks about working with various stakeholders from industry, academia, advocacy groups, societies and associations to develop this training, which has the benefit of being very collaborative and sounds very inclusive. However, the document doesn't explicitly mention inclusivity or diversity as an element of the strategy.

4.3.4 USA

The 2018 White House National Cyber Security policy makes no specific mention of equity, inclusion and diversity. However, it does cover skills and the importance of training and education. There is a line in the strategy that suggests diversity for government recruitment "*This includes expanding Federal recruitment, training, re-skilling people from a broad range of backgrounds.*" In terms of skills development the NICE framework[20] is referenced in the strategy. While this important framework is helpful in terms of mapping skills and what is needed to increase the size and capability of the U.S.' cyber security workforce, it does not address equity, inclusion and diversity.

4.3.5 EU's Cyber Security Strategy for the Digital Decade

The EU's Cyber Security Strategy for the Digital Decade published in 2020, provides information on how the EU will protect its people, businesses and institutions from cyber threats. It also aims to encourage more international cooperation.

The strategy recognises the need for skills development, particularly in certain areas such as SOC, finance and energy. It provides various suggestions to help increase cyber security and cyber defence skills at EU level, for example the European Union Agency for Cybersecurity (ENISA), the European Defence Agency (EDA), and the European Security and Defence College (ESDC) seeking synergies between their respective activities.

In section 1.8 '*A Cyber-skilled EU workforce*' which addresses the importance of upskilling the workforce and developing and attracting the best cyber security talent, it states that "*specific attention must be paid to developing, attracting and retaining more diverse talent*".

Specific reference is made to encouraging more women into STEM careers and ICT jobs, as well as upskilling and reskilling in digital skills. However, inclusion is not mentioned, and no other diverse group is mentioned.

4.3.6 Canada's National Cyber Security Strategy

Canada's National Cyber Security Strategy (1.7) makes it clear that demand for qualified cyber security professionals outstrips supply. Solutions include encouraging more students into STEM degrees and more people from non-STEM degrees into cyber careers. It also suggests that working together across governments, academia and the private sector is necessary to address the cyber skills gap.

Although this is all likely to help encourage more diverse people into cyber security, there is no mention of equity, inclusion and diversity in the strategy.

4.3.7 Australia's National Cyber Security Policy 2020

In the public consultation for Australia's National Cyber Security Policy 2020 carried out in 2019, a key piece of feedback was that Australia needs more trusted and skilled cyber security professionals. Clearly, growing a skilled cyber security workforce is a key part of the strategy. It includes a Cyber Security National Workforce Growth Program that aims to help Australian businesses and academia grow the cyber skilled workforce of the future. A number of specific initiatives are outlined with funding figures given.

Although the Cyber Security National Workforce Growth Program does reference growing cyber education, skills, training, mentoring and coaching programmes and having specialised programmes for women to increase representation in the sector, other areas of diversity are not referenced, nor is inclusion.

4.3.8 The Singapore Cyber Security Strategy 2021

The Singapore Cyber Security Strategy 2021 has created a highly skilled workforce at its heart. There is a section specifically about attracting diverse talent. The areas it focusses on are young people, women, and mid-career professionals. There is a lot of emphasis on the importance of upskilling. While inclusion is not mentioned, the document's language is very inclusive. For example, it talks about improving access to training and networking opportunities for cyber security professionals. And also: "*To build stronger communities of practice and foster trust within the profession, the Government will work closely with industry associations to further recognise the achievements and contributions of our cyber security community.*"

A key initiative is the Youth Cyber Exploration Programme that introduces pre-tertiary students to the fundamentals of cyber security. The strategy also references that in partnership with industry and the local cyber security community, the Cyber Security Agency of Singapore (CSA) launched an "SG Cyber Women" initiative. Successful diversity programmes have been organised as part of SG Cyber Women, such as Capture The-Flag for Girls competition, Ladies in Cyber mentorship programme and technical workshops.

4.3.9 National Information Security Strategy Saudi Arabia

A key element of the Saudi Arabia National Information Security Strategy is to grow the number of people working in information security. Areas it focuses on include security education and training, on-the-job experience and evaluating each individual's skills and capability to aid growth. It is encouraging that the strategy talks about special programmes to "*identify work-ready women who are capable in IT and IS and who, with focused training, can meet some of the Kingdom's immediate IS needs*." In addition, it discusses the employment of young people who have no formal education but possess strong computer skills and can be vetted. Mentoring programmes are also mentioned. While equity, inclusion and diversity are not mentioned, the strategy clearly recognises its importance in plugging the skills gap and staying ahead of threats.

4.3.10 The Cyber Security Strategy for Sierra Leone 2017-2022

The Cyber Security Strategy for Sierra Leone 2017-2022 has an extensive focus on skills and the importance of finding short and long-term solutions to growing the pool of talented, qualified cyber security professionals. It pledges that the government will not just act immediately and for the length of the strategy, but beyond, to fill the demand for cyber security roles through more education and training. It lists ways it may achieve this, for example, via apprenticeships.

In terms of equity, inclusion and diversity it refers to the importance of attracting a diverse range of people and in particular, more women, into the industry. There are no diversity programmes mentioned, but it does demonstrate the need to look at the whole of society to plug the skills gap.

4.4. Other examples of national equity, inclusion and diversity good practice

The examples of equity, inclusion and diversity in national cyber security strategies are sparse, so here we have also investigated and included national-level examples of equity, inclusion and diversity to help inform good practice.

4.4.1 Stonewall Diversity Champions (UK)

Positive reinforcement in action

In the LGBTQ+ rights charity **Diversity Champions** good practice programme is responsible for providing highly bespoke support and advice for more than 600 employees. Members of the programme receive recommendations based upon their Workplace Equality Index score to help them improve their workplaces for lesbian, gay, bisexual and trans staff each year.

Stonewall's annual UK Workplace Equality Index[21] is a free diagnostic and benchmarking tool open to all employers to help them identify practical steps they can take to meet their legal obligations. If required, workplaces can use it to carry out an anonymous survey of lesbian, gay, bisexual and trans staff to measure satisfaction and experiences in the workplace.

The index provides tangible year-on-year measurement, allowing organisations to see where they are in relation to other organisations. Stonewall has a list of best performing organisations rather than shaming ones which perform badly in inclusion and diversity terms. This ensures organisations are incentivised to achieve more diversity and inclusion, and a good score is something positive to aspire to.[22] Companies are more likely to be incentivised to participate in any equity, inclusion and diversity programme because the benefit to the company is clear, rather than being constantly beaten with a stick. Change can be gradual, and companies must be acknowledged for wanting to do the right thing and even allowing measurements to be taken.

The UK's House of Commons takes part and publicly announced its results in the commons by the Speaker of the House in 2017 when it reached the top 100 employers list.[23]

4.4.2 The Making Space Initiative (USA)

Stakeholder collaboration in action

The aim of the Making Space Initiative is to increase representation and encourage a diversity of experts on all cyber-policy related panels. It launched in October 2020 with more than 20 think tanks, universities, foundations, corporate partners and individuals collaborating. Collaboration is an essential theme needed for any equity, inclusion and diversity strategy or programme rolled out from the initiative. Those who sign the Making Space Pledge[24] are dedicated to hosting or supporting panels that represent diversity in the cyber security industry.

4.4.3 DCMS Cyber Skills Immediate Impact Fund — UK

Government funding

The UK government set up the DCMS Cyber Skills Immediate Impact Fund with the aim of very quickly increasing the diversity and numbers of those working in the cyber security sector, particularly in relation to women and neurodiverse candidates. There have been two rounds of funding, one in 2018 and one in 2019. In total it has funded seven projects with grants ranging from £20,000 to £70,000.

In 2020, a research report, 'Evaluation of the Cyber Skills Immediate Impact Fund Pilot', concluded the fund should continue its funding recommendations, which are also useful for best practice in other equity, inclusion and diversity programmes.

Recommendations for improvement:

- Future initiatives should consider supporting the continued professional development of entry-level cyber professionals, as well as providing training for new entrants
- DCMS should advertise future funding opportunities further in advance and with a wider group of providers to encourage more diverse proposals
- Set realistic timeframes and targets — providers indicate that the lead in time required for some projects was longer than expected, and this needs to be factored in
- More should be done to reinforce the idea that the people participating in these projects are leaders in diversity
- Participants should be encouraged to gain participant consent to gather data so that the success of the programme can be better communicated
- Communication between participants in the programme to share insights through some form of alumni group

4.4.4 Blacks In Cybersecurity — Global

The power of community

Blacks in Cybersecurity started as an event series and meet up group in 2018. The official mission of Blacks In Cyber is: 'to encourage the participation of the Black community in Cybersecurity'. The group achieves this by offering a range of activities, from online forums, conferences and meet ups to seminars and group outings.

It has an international reach and provides schools with information about cyber careers, along with training for people who want to change careers into cyber. Its focus is very much on community, using networking and people's own personal connections to spread the word.

4.4.5 CyberDay4Girls — Global

Women can be technical

CyberDay4Girls is an internationally-available virtual programme provided by US technology firm IBM that aims to promote awareness of cyber security as a career option to among pre-teen and teenage girls.

The initiative provides core lessons, (now online) including 'Internet of Me', 'Securing the Internet of Things', 'Intro to Blockchain' and 'Intro to Cryptography', with supporting activities to reinforce learning. Girls learn how to protect their online identities, are introduced to the Internet of Things, and engage in activities such as basic threat modelling. They also have the opportunity to hear from experts about working in the security industry.

Key points

- It has great engagement from more than 1,500 IBM staff, who volunteer their time to deliver the content — this helps improve company culture
- The girls learn from women working in cyber security who help them realise they have genuine technical career choices

4.4.6 NeuroCyber

Industry collaboration

NeuroCyber is a network of industry volunteers led by a Board who all have connections to neurodivergent people. The aim is to improve career outcomes for neurodivergent colleagues, to enrich the sector and positively impact the cyber skills gap.

Its objectives are:

- Educating the cyber sector on the competitive advantage and value of a properly supported neurodiverse workforce
- Creating a network of organisations that are positive about a neurodiverse workforce and signposting neurodiverse talent
- Continually improving working environments and productivity through positive conversations, research and case studies

It does this through:

- Events — Conference speakers, cyber industry trade events, bespoke events connecting job seekers with hiring organisations
- Information hub — Everything you need to know but were too afraid to ask, all in one place
- Inclusion tips — Identifying and sharing fact-based advice to the cyber sector

4.4.7 CyberHeroines — Africa

Equality

CyberHeroines aims to change perceptions about women in cyber to enhance Africa's growth and sustainability. CyberHeroines seeks to create an environment of inclusivity, purpose, commitment and excellence that will encourage more women to embrace cyber security and STEM careers, build confidence in their abilities and enable them to excel in academia and at work.

It provides:

- An equal opportunity for women to embrace and excel in cyber security;
- A safe place where women can fall but not stay down
- A place where women's wins are celebrated

5. Recommendations for building equity, inclusion and diversity into a NCSS

It is recommended that equity, inclusion and diversity should be woven into all the areas covered by Focus Area 5 — Capability and capacity building and awareness raising — in the ITU's Guide to Developing a National Cyber Security Strategy.[17]

In practice, this means ensuring that wherever skills development is addressed, equity, inclusion and diversity is also considered.

5.1 First steps

The Guide to Developing a National Cyber Security Strategy[19] stresses that in looking at cyber security capacity and capability building, all ecosystems are unique — so there is no single solution.

Nowhere is this more important to remember than when looking at equity, inclusion and diversity. There are many different societal, cultural and legal frameworks that government departments need to understand and work within.

5.1.1 Make a single entity responsible

It is important that responsibility within government for equity, inclusion and diversity in cyber security is clearly defined, ideally within a single entity responsible for skills development. Ideally, it should be the same entity that is responsible for skills. That way it can establish, grow and maintain essential relationships with industry, academia and other community stakeholders. For example, in the UK the **UK Cyber Security Council** has been established with this remit.

5.1.2 Identify and engage

It is essential to identify all stakeholders and engage with them from the beginning. This is particularly true where the NCSS either no mention of equity, inclusion and diversity or very little. There is a danger that it will end up only being added in after all the other elements have been carefully researched. This simply will not work. It must be treated as an essential element from the start and in careful consultation with all stakeholders. This is the only way to get it right. Buy-in must be gained from the start to stand a chance of making it part of culture in places where it may not already be.

5.1.3 Measure and assess

It is essential to assess what stage the government and the cyber security industry is at in terms of equity, inclusion and diversity. It's equally important to identify areas that need improvement at a national level, as well as any that are doing well and where lessons can be learned. It is also vital at this stage to start communicating the benefits to all stakeholders and demonstrating them. All stakeholders need to be consulted on how to make improvements and where possible, collect figures from them.

Consultation with stakeholders at this stage may include:

- survey questions structured to provide data
- online presentations with Q&A session
- in person presentations
- meetings with key stakeholders
- a general call for feedback on equity, inclusion and diversity

It is important to include groups relevant to various areas of diversity in this activity. For example, many countries have active Women in Security Groups[1]. Where there are no security-specific groups, look for those that address employment issues for that group, for example in the **Autism National Committee (AutCom)** or the **Disability Databank** in Nigeria.

A list of these stakeholders should be researched, and once engagement has started, it must be nurtured and continued. Genuine public, private and third sector partnership is essential, so it must be more than lip service.

It is essential that the results of any consultation work is both referenced and reflected in the strategy.

5.1.4 Establish priorities and set realistic, measurable, targets

An NCSS needs to establish priorities for a country to achieve the long-term goal of increasing cyber resilience. Equity, inclusion and diversity need to be part of this — and in many cases a priority.

Part of setting clear objectives includes setting realistic targets. How targets are set will greatly depend on availability of national diversity metric figures and specific industry figures. For some nations, gathering better diversity data may be seen as a priority. For others, targets may be set — such as a 10% increase in neurodiverse people in the next five years. The key is to make them measurable, realistic, accurate and representative of the nation and its ecosystem.

As mentioned previously, while gender diversity is likely to be a global issue, the extent will differ, and metrics are necessary to provide regional context. For example, those societies that have been more homogeneous than others but which may have recently seen a growing number of refugees. The inclusion of migrants in the workplace may be something to look at to help address the cyber security skills gap.

When establishing priorities and setting targets, governments simply cannot ignore significant historical, political, or geographic barriers or opportunities. These will impact how individuals from all social categories and groups will be represented in the cyber security industry.

5.2 Mind your language

It may seem simple, but it would be counterproductive when building equity, inclusion and diversity into the NCSS *not* to ensure the language throughout the strategy, (not just elements that directly address skill development), is inclusive. It is important to have the finished document checked thoroughly to ensure nothing can be perceived in the wrong way.

5.3 Academia

It is important to have a clear picture of the country's current position when it comes to the skills shortages and the pipeline for skills development through academic institutions. Questions should be asked such as — is there a bigger problem in a particular skills area? Are there some areas of diversity that the cyber industry is failing to recruit in more than others?

As part of this, it is valuable to understand a country's situation when it comes to inclusion and diversity in the eduction system. This means having accurate figures for both students and staff and, ideally 'state of the nation' reports from a good cross section of both.

As an example, South Africa's universities have women from all races as Dean, but there are only nine Deans who are women in science, technology, engineering, and mathematics (STEM) in total across 26 public universities[27]. It is highly likely that having a lack of women in these leadership roles will be detrimental to women's skills development. This is something that should looked at for improvement.

At a school level, the Guide to Developing a National Cyber Security Strategy[19] says an NCSS should recommend that security is on the agenda. However, the curriculum — technical and non-technical — must also be totally inclusive to encourage a wide range of diverse individuals to study cyber security and consider it as a career. When it comes to gender, it is essential to remove gender bias in language and avoid conscious or unconscious bias. There cannot be assumptions about certain roles suiting one gender over another.

The NCSS must stress that whether, (as recommended by the Guide to Developing a National Cyber Security Strategy)[19] developing dedicated cyber security curricula for primary or secondary schools, integrating cyber security into a computer science degree or developing a dedicated cyber security degree or apprenticeships, equity, inclusion and diversity must be built in. The curricula are crucial for creating interest in cyber security careers so the way they are written is important.

5.3.1 Recruitment programmes

Depending on the country's needs, academic equity, inclusion and diversity-focused recruitment programmes included in the NCSS could be:

- Scholarships for lower socio-economic groups / women
- Grants for apprenticeships
- Funding for coding clubs or dedicated classes / courses to help address the gender balance
- Funding for cyber courses at all levels, adapted for neurodiversity
- Visibility of more diverse role models from industry

5.4 Training

The Guide to Developing a National Cyber Security Strategy[19] recommends that the NCSS should encourage training and skills development schemes for both experts and non-experts in the public and private sectors.

Based on identified needs of the government, these could consider how equity, inclusion and diversity impacts:

- Executive and operational training
- Formal internships and traineeships
- National and international certification of security professionals
- Initiatives focused on cyber risk management
- Practical exercises among government entities and other stakeholders, including drills and simulations

Specific training for regulators and legislators

It is important all areas of diversity are considered (gender neutral language and accessibility for everyone are always essential) to ensure no one is excluded from training. However, special focus can be given to areas identified as key to the NCSS.

5.4.1 Recruitment programmes

Any training campaign in the NCSS needs to encourage more diverse people who wish to develop a long-term cyber security career path. However, the specific campaign will depend on the needs of the ecosystem.

- Free or subsidized government, third-sector or industry-led training and certification programmes for diverse groups (e.g. **TechVets** programme for Veterans, or **Sans Cyber Diversity Academy**)

5.5 Industry

5.5.1 Improving recruitment

All initiatives to grow diverse talent are for nothing if there are no organisations ready to employ them. Government needs to work closely with industry to ensure engagement with all initiatives. Advice and support should be made available for issues like removing gender bias in recruitment advertising and adapting the interview process for neurodivergent candidates. Effort should be made to grow awareness of the importance of equity, inclusion and diversity and employer benefits. In many countries, the government will be able to work with, and use existing support material from, diversity charities and groups.

5.5.2 Improving retention

There is little point attracting lots of new people to the cyber industry if they hate it and leave. This is where making it inclusive is essential and where the NCSS must engage industry and embrace changing workplace culture. A Tech Leavers Study from the Kapor Center for Social Impact[18] found that by improving workplace culture, retention can be significantly improved. Some 57% of those surveyed in the study would have stayed if their company had taken steps to make company culture fairer and more inclusive.

5.5.3 Best practice for industry recruitment and retention programmes

Top down

As a starting point, any organisation, whether public or private sector, should have a management / board level leadership equity, inclusion and diversity programme. The whole organisation needs to share the culture of recruiting and retaining and being completely inclusive for all people, whoever they are.

Language matters

Always avoid language that discriminates against other genders. In practice this means using pronouns that are not specific to one gender or another. For example, rather than saying “He needs to have the following experience” or “she is required to be able to” refer to the candidate or use they / them. Gender Decoder[27] is a great tool for picking up on unconscious uses of gendered language. This tool was inspired by a research paper written in 2011, called “Evidence That Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality.”

The researchers showed job adverts with gender-coded language to men and women and recorded how appealing the jobs seemed and to what extent participants felt they ‘belonged’ in that occupation. It is important to note that no non-binary people were included in this research, and the research didn’t touch on non-binary-coded words.

Women felt that job ads with masculine-coded language were less appealing and that they belonged less. For men, feminine-coded adverts were only slightly less appealing and there was no effect on how they felt they belonged.

Diverse means diverse

Equality doesn't mean treating everyone the same. To recruit and retain diverse teams, everyone cannot be treated as a homogeneous group. But as well as that each individual in a diversity group (e.g., race, gender, religion, etc.) will have different motivation for joining a company and potentially for leaving. Everyone must be treated as an individual.

Positive role models

Encouraging industry engagement in mentoring programmes is important. The ability to see positive role models in the workplace is one of the most effective ways to encourage more diverse people into cyber security education or a particular organisation and retaining them.

An inclusive culture

Create programmes that work to create an industry culture where all voices are equally heard and given equal respect. Make it an industry where people aspire to work — because it has a reputation for being friendly, diverse and inclusive to work in.

5.6 Upskilling and reskilling

Upskilling is providing training to improve a person's performance of add to their skills in their current role. So, this won't add to the numbers in the sector, but it can improve capability and is useful where organisations have skills gap.

Reskilling provides training that will help an individual move into a new role or make a significant change to their current role. Programmes that consider reskilling can potentially bring more diverse people into the industry.

Brief tips:

- Provide subsidies to businesses who want to provide cyber security training to upskill diverse employees or a subset that have been identified in the NCSS as a key target
- Provide subsidies to businesses who want to provide cyber security training to *reskill* diverse employees or a subset that have been identified in the NCSS as a key target
- Encourage closer collaboration between training providers, diversity groups and industry for upskilling and reskilling initiatives
- Provide support and advice for veterans, police and other career changers with transferable skills, including free training and mentoring
- Provide training subsidies, support and advice to diverse individuals who want to reskill

5.7 Certifications

A key part of any National Cyber Security Strategy is improving the standard of skilled cyber professionals as well as the quantity of them. One way to do this is via certifications. Both Enisa's NCSS Best Practice Guide[28] and the **Guide to Developing a National Cyber security Strategy**[19] recognise the importance of both national and internationally recognised certification for security professionals. The drive to get more people certified should also include diversity targets.

5.8 Issues with equity, inclusion and diversity metrics

Metrics are essential. The government department responsible for cyber security will relay nationally gathered metrics on diversity and inclusion.

5.8.1 Data problems

Measurement of diversity at a national level is essential. And once any equity, inclusion and diversity programmes outlined in the NCSS have been implemented, repeating that measurement to establish whether there has been any change is crucial.

However, in most countries the level of workforce diversity data is poor. In the UK for example, employers are only obliged to report on diversity demographics in regards to gender (in Northern Ireland, additionally religion). In the USA the picture is better, and employers need to monitor the racial or ethnic and gender composition of their workforce by specific job categories. In many countries, gender and age can be collected by employers legally without permission — but they do need permission to collect other data.

5.8.2 Disclosure difficulties

There may be difficulties gathering some forms of personal data (this is any data that can identify them or help identify them) because people simply do not want to disclose personal information. But government or employers can ask. They need to be clear about why they need the data, why they are asking and of course, reassure people that they will protect it.

Many people prefer not to disclose personal data when related to potentially sensitive information such as disability, sexual orientation or gender identity. So, although increasing disclosure to get better quality data is important to improve inclusivity and diversity, it is a challenge.

> Having good corporate culture and implementing visible non-discrimination policies will encourage disclosure. However, it cannot eliminate the fear that disclosure may cause problems in their career.

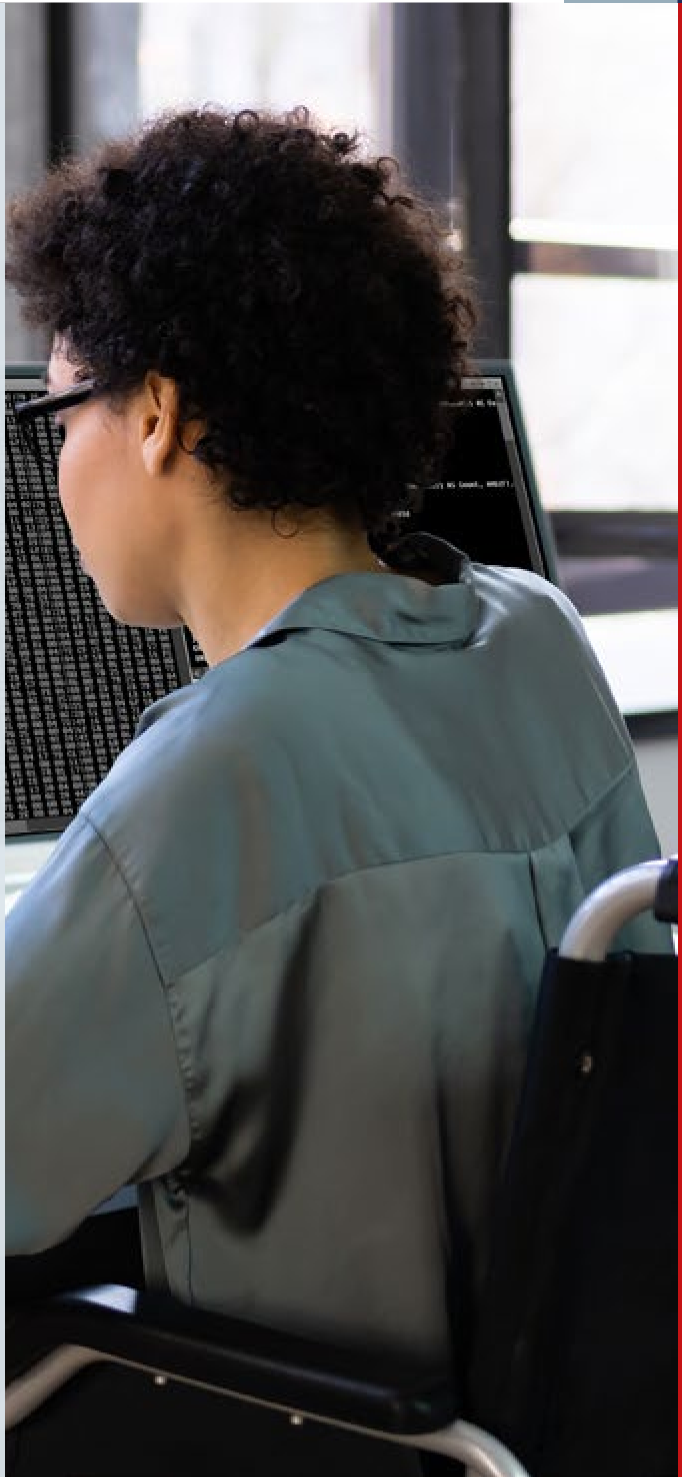
One study found fear that disclosure of disability would stall career progression and there was concern about not being hired.

Seeing role models — people who have disclosed disability, had reasonable adjustments to their work environment made and enjoyed thriving careers — are essential to promoting disclosure. In addition, effective communication of why it is required and its importance to the industry will be helpful.

5.9 Changing perceptions

Even the most carefully put together equity, inclusion and diversity programmes may not help if people's perceptions don't change. If they don't, for example, think that men are more technical. In 2009, women made up 11% of the STEM workforce in Australia. In 2019, after the Australian Government spent more than AU $268 million on initiatives to get women into STEM, the figure stood at 13% — a mere 2% more. The issue is clearly not about providing women with access to cyber security careers — it is a deeper societal issue.

The best way to change embedded perceptions is by promoting role models — and the viability of diverse people working in a variety of cyber security roles. Specific programmes like **Blacks in Cyber Security** do this very well. Other programmes include **Australia's Women Speak Cyber** encourages more women to speak at events nationwide, **NeuroCyber** which offers neurodivergent speakers for events, or CREST's drive to promote diverse careers videos on its **YouTube channel**.



6. National cyber security equity, inclusion and diversity programme good practice

Although full details of actual programmes to improve equity, inclusion and diversity are not scoped out in National Cyber Security Strategy, this section provides some guidance into good practice for putting together a programme.

Equity, inclusion and diversity require more than national strategy or even policy that legislates. Numerous cultural biases — which influence cyber workforce diversity — are challenging to change. Only through the best programmes that embrace the whole industry can we challenge — and hope to break down — these biases. For example, for equity, inclusion and diversity programmes to work, they must have both diverse and non-diverse leaders working together to create the right culture — one that embraces diversity of thought and deploys best practice. The message is that an inclusive and diverse cyber security workforce and workplace is better for everyone.

6.1 Program initiation

The first step is to put together a detailed project initiation document (PID). Contents may vary, but for good practice they should include:

6.1.1 Why is the programme being undertaken?

This should contain detail on the background of the equity, inclusion and diversity project. It needs to address why the project is being undertaken and its relevance and the wider context in relation to the NCSS. There needs to be a focus on the benefits it is expected to deliver and how that fits with the NCSS.

6.1.2 What is the programme expected to deliver?

The PID needs to be specific about what is in scope and what is not. Use project flow charts and diagrams to visually illustrate the boundaries. Make sure the document is absolutely clear on what constitutes success for the programme and how that is going to be measured.

6.1.3 Who is responsible for the programme?

Identify the people who will be taking part in the programme's planning and implementation and make sure each has a clearly defined role. There needs to be a project manager as well as team leaders. All stakeholders in the project must be documented along with their interests.

6.1.4 How will the programme be delivered?

Things to consider:

- What methodology to use — for example waterfall or agile?
- How to communicate with stakeholders
- Will there be a pilot programme?
- How to track risks and issues
- How to track changes to changes to scope
- Draft timeline of milestones for project delivery
- Top ten risks, issues and constraints
- Cost estimate

Ensure the PID is put together in collaboration with members of the programme team, and written in pain language.

6.2 Co-ordination and collaboration teams

Co-operation, collaboration and co-ordination

The importance of these three things cannot be underestimated.

The effectiveness of many excellent national initiatives has been limited by the lack of a joined-up ecosystem. The right mix of skills, background and views in the team is essential. It is remarkable how many equity, inclusion and diversity programmes do not have diverse teams. Engagement with groups that focus on the specific area of diversity the programme is addressing is essential. For example, there are many active groups working to encourage more women into cyber security around the globe. To not take advantage of their knowledge on a relevant programme would be a mistake (See Appendix 2).

As an example, training neurodiverse cyber-staff is a great thing to do, but if there are no organisations ready to employ them, the impact is diluted. Or if a training programme trains more women in a skill where staff shortages are not an issue, while ignoring areas where there are staff shortage problems. The big picture is important, but so is making real, tangible and measurable differences.

Although elements can be set and informed by the NCSS it is beneficial for countries to have a single entity that is responsible for cyber skills and diversity, it is also essential that for each programme that a handpicked team is put together with the perfect mix of skilled people from across the stakeholder groups. The team can be chosen from a draft list of skills and tasks.

6.3 The programme design

6.3.1 Focus on gender

It is often thought that to attract more women into cyber security, programmes need to stress that you do not need to be too technical. It is important to publicise the wide range of roles in cyber, but not only to women.

This approach assumes men are more likely to be technical than women. It is wrong to set out to have security teams that have non-technical women and technical men. Women can most certainly understand complex technical issues. But having proven technical aptitude doesn't mean you cannot also bring the softer social skills. And, of course, men can also bring those capabilities to a team.

6.3.2 Focus on neurodiversity

Having a programme that aims to increase the number of neurodivergent people as part of a strategy should not be a one-size-fits-all initiative. It is important not to generalise about people. Not all autistic people have issues with communicating and while cyber security may often be a job that is well suited to them, that doesn't mean everyone autistic is automatically suited to a technical job. Dyslexia and dyscalculia problems range greatly from mild to severe.

While some countries are recognising the benefits of employing neurodivergent people in cyber security roles, in others there is still a great deal of education required. Any programme will need to focus on educating employers about the benefits of employing neurodivergent staff — especially how easy making any required adjustments is.

6.3.3 Focus on race and ethnicity

It is essential to have open dialogue about where improvements are needed and the importance of setting and reaching targets. It is only through honesty that a true cultural shift can be made from reluctant quota filling to a realisation that everyone benefits. While it is well intentioned, the outdated idea that we should simply not see race, ignore the systemic problems and inequities many still face. It has to be talked about and reflected in any resulting programme design.

6.3.4 Focus on socio-economic

Improving socio-economic diversity in the workplace is just as important as all other inclusion and diversity initiatives. It is important to look at programmes that not only encourage people from all backgrounds into cyber security but also help and support those that are unable to afford the required training or qualifications.

6.3.5 Focus on unconscious bias

So why are businesses struggling to improve their diversity and inclusion when it's clear it could only strengthen their teams and improve their finances? The term unconscious bias was first used by Greenwald and Banaji (30) in 1995. Their research highlighted that implicit biases — including experiences, social background, and environment had and impact on behaviour and decision-making unknowingly. This means that unconscious bias can not be easily identified because it will vary from person to person.

> "Sometimes it is the people no one imagines anything of who do the things that no one can imagine"
>
> **Alan Turing**

6.4 Publicising the programme

There is no point getting everything right if no one knows about it. Make sure the programme's availability is widely known and the timelines are right. For example, if the programme provides the ability to apply for government funding and asks for equity, inclusion and diversity pitches that require significant input, allow enough time to put together realistic plans. The UK's CIIF review identified this as an area that required improvement, both in terms of the timeline and how widely aware people were.

This is where stakeholders in established programmes are important. Use their social media networks. Hold webinars, presentations, town hall meetings. Put out press releases, speak to journalists, write articles, blog, record podcasts and videos. Use role models wherever possible.

6.5 Implementation

Every nation has cultural social biases that influence the roll out of cyber security industry equity, inclusion and diversity programmes. Simply mandating higher proportions of diverse workers in cyber security will not solve the issues. For example, many workplace cultures incorrectly assume all technical leaders are male, while women are better at softer skills like communicating and being more supportive.

A critical success factor when implementing any equity, inclusion and diversity programme is to go beyond asking people to comply with the law or do the right thing, but ensure there is a strong focus on all the benefits. This means talking about the benefits to the security business, wider benefits to the cyber security industry and, of course, wider implications to society. It is only by instilling the right mindset at leadership level that systemic culture change will happen and any national cyber security programme needs the support of the cyber security community.

6.6 Measuring success

There are two main ways to measure the success of an inclusion and diversity programme. How success is measured depends on availability of diversity data at the programme's outset, and the ability to measure any improvements.

The two ways of best measuring success are:

- Cross-sectional comparisons with a designated set of peers (from other nations)
- Over time comparisons within the single entity whether that is a university, region within a nation or an entire country

Both have their place and can even be used in combination with one another. However, the second measurement is the most important in improving diversity and inclusion-related programmes, because while benchmarking between nations can be a useful barometer, the differences between nations means that may not be an entirely accurate or representative picture.

6.7 Maintenance and long-term development

Data drives culture change

Next to the visibility of role models, having accurate data will change hearts and minds and lead to the ability to maintain the programme and its long-term success. Giving people evidence on equity, inclusion and diversity pre — and post-programme implementation is key to success. This is what will make it relevant to stakeholders in the cyber security ecosystem. Facts and figures hold the power to persuade them that equity, inclusion and diversity will help solve the challenges that the cyber security industry faces and that they all have a part to play. So, academic staff designing curriculum will help, recruiters get involved in mentorship, trainers will look at how they can adapt their courses for dyslexic people, and so on. Everyone will become more deeply involved, and it will no longer be perceived as a problem, but as an opportunity.

The more granular, and localised the data the better it is that government and stakeholders can achieve long-lasting systemic change. It will also enable the programme to be continuously adapted to the changing needs of the cyber security ecosystem. It is only through accurate and continuously updated data that the programme will stay relevant, people will stay engaged and it stands a chance of making a difference. Any inclusion and diversity programme should help bring more diverse people into the cyber security arena, making cyber security more inclusive, and ultimately making nations more cyber-resilient.

References

1. **(ISC)2 Cyber security Workforce Study, 2021**
https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

2. **World Economic Forum, The Global Risks Report 2022**
17th Edition https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

3. **McKinsey, Diversity wins: How inclusion matters**
https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-wins-how-inclusion-matters

4. **Deloitte Australia (Deloitte) and the Victorian Equal Opportunity and Human Rights Commission, 'Waiter, is that inclusion in my soup?'**
https://www2.deloitte.com/content/dam/Deloitte/au/Documents/human-capital/deloitte-au-hc-diversity-inclusion-soup-0513.pdf

5. **Harvard Business Review, The Other Diversity Dividend**
https://hbr.org/2018/07/the-other-diversity-dividend

6. **World Bank Blogs, Six facts on gender laws and the public sector**
https://blogs.worldbank.org/governance/six-facts-gender-laws-and-public-sector

7. **Constitution of the Republic of South Africa**
https://www.gov.za/documents/constitution/chapter-2-bill-rights

8. **CIPD, Managing an age-diverse workforce**
https://www.cipd.co.uk/Images/managing-an-age-diverse-workforce_2014_tcm18-10838.PDF

9. **Convention on the Rights of Persons with Disabilities (CRPD)**
https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html

10. **AMERICANS WITH DISABILITIES ACT OF 1990, AS AMENDED**
https://www.ada.gov/pubs/ada.htm

11. **World Health Organisation, International Classification of Diseases**
https://www.who.int/standards/classifications/classification-of-diseases

12. **World Health Organisation, Blindness and vision impairment**
https://www.who.int/news-room/fact-sheets/detail/blindness-and-visual-impairment

13. **Digiomica, Thinking differently — the benefits of neurodiversity**
https://diginomica.com/thinking-differently-benefits-neurodiversity

14. **Digital, Culture, Media & Sport (DCMS), Cyber security Skills in the UK Labour Market 2020 report**
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/959164/Cyber_security_skills_report_in_the_UK_labour_market_2020_V2.pdf

15. **World Bank, WOMEN, BUSINESS AND THE LAW 2019: A DECADE OF REFORM**
https://openknowledge.worldbank.org/bitstream/handle/10986/31327/WBL2019.pdf

16. **The IET, We are celebrating Pride Month!**
https://www.theiet.org/membership/member-news/member-news-2019/iet-member-news-q2-2019/we-are-celebrating-pride-month/

17. **Scientific American, Race Is a Social Construct, Scientists Argue**
https://www.scientificamerican.com/article/race-is-a-social-construct-scientists-argue/

18. **The Kapor Center for Social Impact, Tech Leavers Study**
http://www.kaporcenter.org/wp-content/uploads/2017/04/KAPOR_Tech-Leavers-17-0427.pdf

19. **Guide to Developing a National Cyber Security Strategy**
https://www.ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf

20. **The NICE Framework**
https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework

21. **Stonewall's annual UK Workplace Equality Index**
https://www.stonewall.org.uk/creating-inclusive-workplaces/workplace-equality-indices/uk-workplace-equality-index

22. **Stonewall, Top 100 Employers**
https://www.stonewall.org.uk/our-work/campaigns/top-100-employers-2019

23. UK House of Commons, Speaker's Statement on Stonewall Workplace Equality Index
https://youtu.be/T83wae4AtdM

24. The "Making Space" Pledge
https://www.makingspacepledge.org/the-pledge/

25. Department for Digital, Culture, Media and Sport (DCMS), Evaluation of the Cyber Skills Immediate Impact Fund Pilot
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1009064/Evaluation_of_Cyber_Skills_Immediate_Impact_Fund_Pilot.pdf

26. BWASA WOMEN IN LEADERSHIP CENSUS 2017
https://bwasa.co.za/wp-content/uploads/2018/04/2017-BWASA-CENSUS-report.pdf

27. Gender Decoder
http://gender-decoder.katmatfield.com/

28. ENISA, NCSS Good Practice Guide
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

29. Garnett Interactive, The Value of Diversity in Cyber Security
https://www.garnettinteractive.co.uk/the-value-of-diversity-in-cyber-security/

30. Greenwald, A & Banaji, M (1995). Implicit social cognition: Attitudes, self-esteem and stereotypes. Psychological Review 1995, Vol 102, No. 1, 4-27. American Psychological Association Inc.
http://www.people.fas.harvard.edu/~banaji/research/publications/articles/1995_Greenwald_PR.pdf

Appendix 1. Examples of National Cyber Security Policy

1.1 The UK National Cyber Security Strategy 2016-2021
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

1.2 The UK National Cyber Security Strategy 2022-2025
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

1.3 National Cyber Security Policy Pakistan 2021
https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf

1.4 National Cyber security Policy and Strategy 2021, Nigeria
https://technologytimes.ng/wp-content/uploads/2021/02/NATIONAL-CYBERSECURITY-POLICY-AND-STRATEGY-2021_E-COPY_.pdf

1.5 Nation Cyber Security Strategy of the United States of America, 2018
https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

1.6 EU's Cyber security Strategy for the Digital Decade
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

1.7 Canada's National Cyber Security Strategy
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

1.8 Australia's Cyber security Strategy 2020
https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

1.9 The Singapore Cyber Security Strategy 2021
https://www.csa.gov.sg/-/media/Csa/Documents/Publications/The-Singapore-Cybersecurity-Strategy-2021.pdf

1.10 Saudi Arabia National Information Security Strategy
https://www.itu.int/en/ITU-D/Cyber security/Documents/National_Strategies_Repository/SaudiArabia_NISS_Draft_7_EN.pdf

1.11 Cyber Security Strategy for Sierra Leone 2017-2022
https://www.itu.int/en/ITU-D/Cyber security/Documents/National_Strategies_Repository/00090_03_Sierra%20Leone%20national-cyber-security-strategy-2017-final-draft.pdf

Appendix 2. Examples of Women in Security Groups

Women in Security France
https://www.wiisfrance.org/

Women in Security Forum
https://www.securityindustry.org/professional-development/women-in-security-forum/

Australian Women in Security Network
https://www.awsn.org.au/

Le CEFCYS (CErcle des Femmes de la CYberSécurité)
https://cefcys.fr/

Women4Cyber
https://women4cyber.eu/

She Secures (Africa)
https://shesecures.org/

WOMCY, Latam Women in Cyber security
https://womcy.org/

Women in Cyber security Middle East
https://www.womenincybersecurity.me/

Women In International Security (WIIS)
https://wiisglobal.org/

Women in Cyber security
https://www.wicys.org/

African Women in Cyber Defense
https://cyberheroines.com/

Warning

This Guide has been produced with care and to the best of our ability.
However, CREST accepts no responsibility for any problems or incidents arising from its use.

CREST

For further information contact CREST at:

www.crest-approved.org