UK FINANCE

EY
Building a better working world

Microsoft

USE OF NON-INCLUSIVE LANGUAGE IN TECHNOLOGY AND CYBERSECURITY AND WHY IT MATTERS

Report by UK Finance, EY and Microsoft

FOREWORD

by David Postings, Chief Executive, UK Finance

The language we use when we write and talk to one another is critical to effective communication. For many of us, our language is something that we have grown up with or that has become embedded in our vocabulary through repetition and culture. However, for some people that language is steeped in negativity that highlights and entrenches inequality, further compounding a system that often creates barriers based on race and ethnicity, gender, sexual orientation, and accessibility. It is incumbent on all of us to ensure that we remove those barriers, creating a society that is fairer and equal to all.

The recent focus on these issues within broader society is something that the sector takes extremely seriously, and I am proud we are actively tackling this together. However, one area that can often be overlooked is language – in particular language that is non-inclusive which can alienate a sub-sector of society and portray people in an unnecessarily negative light.

I am pleased to say that UK Finance members have collaborated with us on this report, highlighting the industry's commitment to driving change and ensuring the language they use is inclusive and promotes diversity in the workplace.

That is not to say that we cannot do more. This report intends to provide a perspective that I hope the whole sector can stand behind, that non-inclusive language is something that we should look to eliminate or replace. We have chosen the specific sub-sectors of technology and cybersecurity to examine this issue, as for many of our members the language they use in these areas is embedded within the processes or coding of legacy systems. We are delighted that Microsoft and EY have joined us in writing this report and are able to provide their own unique perspectives on this important issue.

This report does not set out to demonise or blame anyone for the language already in use. Instead, it is intended to educate and provide alternatives to enable firms to move away from instances of non-inclusive language. The report also addresses the benefits that these changes can lead to from a business perspective – firms that have a diverse and inclusive culture often outperform their peers. In those simple terms, it should be obvious that firms would want to promote inclusion and diversity and that this report can play a small, yet valuable part in that.

I would like to thank our members that contributed to this report and to Microsoft and EY. I hope you enjoy reading it and that it causes you to think and reflect on this issue.

ACKNOWLEDGEMENTS

Thank you to authors, contributors and members.

UK Finance

Ian Burgess
Director, Cyber and Third Party Risk

Oge Udensi
Principal, Cyber Security

Peer Review by City of London Corporation's Tackling Racism Taskforce

Caroline Addy

Andrien Meyers

Caroline and Andrien are the co-chairs of the City of London Corporation's Tackling Racism Taskforce.

EY and Microsoft

The EY and Microsoft alliance helps clients respond to the digital disruption challenge. It brings together deep EY business and industry insights with scalable, enterprise cloud platform and digital technologies from Microsoft to create innovative and proven solutions that help accelerate clients' digital transformation, minimise risk and create new business value faster.

Ernst & Young LLP

Kanika Seth
Partner, UK Financial Services Cybersecurity Lead, EMEIA TPRM lead and EY Women in Technology Board member

Nina Driscoll
Director, Banking & Capital Markets and Diversity & Inclusion Client connections lead

Sarah Ramsey
Business Consultant

Microsoft

Sarah Armstrong-Smith
Chief Security Advisor

Tim Jarman
Diversity & Inclusion Lead – UK, Ireland & Western Europe

Janet Jones
Head of Industry Strategy, Financial Services, Microsoft UK

Special thanks to:

EY

- **David Williams**, Partner, Ernst & Young LLP, Technology and EY Women in Technology Board member
- **Mduduzi Mswabuki**, Partner, Ernst & Young LLP, Assurance and UK Co- Chair for Diversity & Inclusion and Member of UK Board D&I Sub-Committee
- **Ololade Adesanya**, Director, Ernst & Young LLP, Financial Services and Race Steering Committee Chair

Microsoft

- **Monica Rush** – Senior Program Manager, Commerce & Eco-system
- **Roxanne Kenison**, Senior Content Designer, Microsoft 365
- **Stephanie Blucker**, Content Designer, Microsoft 365
- **GeriAnn Baptista**, Global D&I Strategy, Brand, & Executive Communications

EXECUTIVE SUMMARY

Recent events have placed a spotlight on the importance of diversity & inclusion (D&I) within society. Within the financial services industry, banks, insurers, wealth and asset management firms, trade bodies and regulators have made great strides to make diverse and inclusive cultures a reality. Yet there is more to do.

Following the Black Lives Matter (BLM) movement in 2020 the cybersecurity industry began to explore the issue for itself, raising significant debate with the launch of #VersusRacism, an initiative designed to tackle the problem of racism within the information security community, and central to this was addressing the use of language in the industry.

"When it comes to the Diversity & Inclusion agenda, meaningful change that moves the dial across an industry can only happen if there is large-scale, collective action. Removing non-inclusive language will be an ongoing process with no end date as society changes and evolves, but we are at a crossroads currently and there are a number of urgent language changes we should make now to start to create a more inclusive and professional environment. This is a sensitive and delicate topic, and will require leaders to listen to the groups affected, meaning there is a top down and bottom up element to success."

Nina Driscoll, Director, UK Financial Services, Banking and Capital Markets, Technology Market Lead and EY's EMEIA Financial Services Client Service D&I Lead, EY

Language is one of the most important tools we have as individuals and when used well, it can create a common understanding and feeling of belonging. Conversely, when used negatively it can also create and reinforce barriers and feelings of alienation. The use of non-inclusive language is a sensitive, broad and complex topic and covers both the language used in social settings with friends and family and the language used within the workplace.

It has become clear that across **technology and cybersecurity** negative and often prejudiced connotations have slipped into everyday use of written and spoken language (including language used in system coding), body language and visual cues. This is an issue that has been highlighted by UK National Cyber Security Centre (NCSC) and the US National Institute for Standards and Technology (NIST) has spoken publicly about the need to remove insensitive and non-inclusive terms from our workplace language.

This report has been co-authored with UK Finance, EY and Microsoft to explore language that may have become institutionalised, specifically in technology and cybersecurity through legacy application systems and coding, as well as emerging and established terminology. Through dedicated research, industry insights and discussions with UK Finance members, the report delves deeper into these issues to understand the impact this has on society, the financial services industry and individuals. Within the report we consider terms that have become synonymous with race and ethnicity, gender, sexual orientation, accessibility, as well as the use of criminal and military terms specific to cybersecurity.

In a survey conducted by UK Finance, **over 50 per cent of participants said they believe there is currently an issue regarding non-inclusive language in technology and cybersecurity**, citing a **lack of awareness** of the issue as the top perceived barrier to enabling effective change. It is clear there is a huge opportunity for the industry to come together to deliver impactful change. But this is more than just doing the right thing, it is a strategic business and regulatory imperative to drive positive behaviour that enables organisations to attract and retain talent, and to be representative of the society they jointly serve.

When developing a successful strategy for sustainable change, four key focus areas have been identified:

1. **Technical changes** to existing and future products and services to identify and replace non-inclusive terms utilised in system architecture and designs.
2. **Driving the right culture** from the top down with engagement of a senior sponsor and a core team of champions from across the organisation to provide leadership.
3. **Engaging employees** in the conversation by encouraging open dialogue and providing training and education throughout the organisation, through mentors and allies.
4. **Continuous improvement** by scheduling regular policy reviews and considering the wider impact of non-inclusive language beyond technology and cybersecurity.

It is recognised that organisations are at different stages of their D&I journeys, therefore a 12-step guide has been provided to help organisations gauge where they are now, and where they aim to be, in order to help determine the next steps.

The UK financial services industry must come together to drive real and effective change. If successful, this has the potential for a far wider-reaching impact across society.

BACKGROUND

Diversity and inclusion in the workplace drive better business performance

In the current competitive and uncertain economic environment, organisations rightly place importance on the 'bottom line' and making sure they provide value to shareholders. Often, societal impacts can be seen to 'get in the way of this'. Research demonstrates that D&I is not just a social imperative, it is a key enabler of business growth.

Companies in the top-quartile for gender diversity on executive teams were

21% more likely to outperform on profitability

27% more likely to have superior value creation

MCKINSEY (2020)

The highest-performing companies on both profitability and diversity had more women in line (i.e. revenue-generating) roles than in staff roles on their executive teams.

Organisations where individuals experienced a high sense of 'belonging' had a

56% increase in job performance

50% Drop in turnover risk

75% Reduction in sick days

BETTER UP (2019)

FEWER THAN 1 IN 10 management roles in financial services are held by black, Asian or minority ethnic people

Only **80** directors of colour in the FTSE250,

5% of the total

The Parker Review

Most ethnically diverse companies, for example, **35%** are more likely to outperform the least diverse.

FCA: Why black inclusion matters to us

Now more than ever, organisations need to be cognisant of the role they play in building a better working environment for all. This is not just because it's the right thing to do, but also because the long-term systemic impact of ensuring the organisation is inclusive and diverse has clear successful growth outcomes in the long term.

Today's technology leaders have a tremendous opportunity to help carve out a new future with their customers and partners that is both good for society and the bottom line. Language used in technology and cyber is one area where we can actively drive change to ensure all individuals feel included and non-inclusive language is removed.

Financial services regulators continue to place greater focus on diversity

From a regulatory perspective, D&I is gaining greater focus from an organisational and consumer level – it is moving to the heart of regulation, with a joint approach to D&I being worked on by the Financial Conduct Authority (FCA) and the Prudential Regulatory Authority (PRA), as announced by Nikhil Rathi, CEO FCA, in his speech at the launch of the HM Treasury Women in Finance Charter Annual Review.

During his speech Rathi said "this lack of diversity at the top raises questions about organisations' ability to understand the different communities they serve, and their different needs. I would question if any organisations can adequately respond to the needs of these consumers if they do not have the diversity of background and experience required to overcome biases and blind spots."

As part of the FCA's work on wholesale banking culture, it introduced five conduct questions to help focus the minds of senior managers on conduct risk. Rathi outlined that he would like to include an additional question for all organisations – "is your management team diverse enough to provide adequate challenge and do you create the right environment in which people of all backgrounds can speak up?".

Becoming more diverse is not only about who you hire. Creating an environment of equality, respect and inclusivity ensures that employees utilise their differences and work together to bring the positive impact of diversity to life.

Yet language can also be the barrier to building a diverse and inclusive team. In order to ensure a positive and diverse environment, language must be treated as a key element of an organisation's D&I strategy. This is why driving change in the language used in technology and cybersecurity brings us one step closer to having a fully inclusive culture where all individuals feel they belong.

Research has suggested that greater gender diversity improves risk management culture and decreases the frequency of European banks' misconduct fines, providing an estimated savings of US$7.84m per year. The lack of diversity at the top of organisations poses a challenge on the ability to understand the different communities and needs of their employees and customers.

Organisations that fail to reflect the society they serve run the risk of not being able to adequately support diverse communities – making diversity a regulatory issue.

Language in technology and cybersecurity

Why does language matter?

It is arguably the speed of evolution and accessibility of technology to so many people that has brought the conversation on language and inclusivity to the forefront. If we want more people to embrace 'tech for good' as a pillar of modern society, then we must systematically identify and remove barriers to adoption, barriers in accessibility, and barriers to attracting talent to organisations. One such barrier is the language that is used by organisations in technology and cybersecurity.

The cybersecurity industry utilises a language that is unique, often difficult for people to understand, and occasionally sensationalist.

Cybersecurity is often portrayed as a niche specialism, physically and logically closed off from the rest of the organisation due to the confidential nature of the work. This can often be intimidating for non-security people, as the language and visual cues tend to portray cybersecurity negatively as it often goes together with cybercrime, fraud and data breaches, i.e., a place where bad things happen. The use of militarised terms such as 'kill-chain', 'detonation chamber' and 'wargames' does little to improve the situation

Indeed, the head of security awareness at a high street bank highlighted how employees are often 'turned off' by cybersecurity due to people being portrayed as 'the weakest link' or labelled as 'repeat-offenders'. In the past, negative language has often been used to attempt to convince people that they should care about cybersecurity, but instead it leaves them alienated and confused. In fact, people are typically more motivated by positive language and by re-engaging them in this way this can lead to improved engagement and outcomes. Therefore, we need to consider not just the terms we use, but how we use language to enable positive change.

Impact on individuals

In considering the impact that non-inclusive and negative language can have on tech and cybersecurity as a business function, it is also necessary to consider the impact it has on individuals, particularly those from diverse backgrounds.

Research has indicated that the most effective D&I strategy is one that focuses on creating an inclusive work environment. In 2017 the Kapor Center for Social Impact ran a national study examining why people in tech voluntarily left their jobs. They found that underrepresented minorities were twice as likely to leave their job because of unfair treatment, rather than a better job. Unfair treatment included: unjust management practices, stereotyping, sexual harassment, bullying and hostility.

Having non-inclusive terms, such as those highlighted in the Microsoft case study, baked into application systems or technical terminology and promoting this as acceptable in the corporate culture can leave certain segments of the workforce feeling isolated or uncomfortable and undermines the wider D&I efforts being made by each organisation.

While any industry has its own technical terms, language can also be a barrier to recruitment for many. The intersection between technology and financial services has also created a digital skills gap, that continues to extrapolate, with the lack of availability and diversity in tech and cybersecurity roles. This should be a concern as the financial services sector looks to become more inclusive, rather than exclusive.

The (ISC)2 Cybersecurity Workforce Study 2020, highlights that the majority of cybersecurity professionals either work in technology (20 per cent), or financial services (ten per cent), and 'for organisations that want to maintain their momentum, it's important that they keep their long-term, senior-level cybersecurity professionals satisfied and eager to share their deep institutional memory. They also need to continue to recruit a new stream of younger professionals interested in learning from their peers and offering diverse new perspectives on maintaining the highest level of cybersecurity'.

There is a need to make the industry more open, appealing and accepting to a broader, more diverse audience. A simple change that can be made is to make cybersecurity less intimidating, and language plays a big part in that. Until biases in our language, even if used unintentionally, are proactively addressed, they will continue to propagate in system and service design as well as in algorithms used for new technology.

This sentiment is echoed by Fox Ahmed, Global Head of Cybersecurity and Technology Regulatory Risk at BNP Paribas, who highlighted that their organisation had made great strides in terms of following more diverse recruitment practices, however there are issues that need to be addressed across the industry in terms of attracting diverse talent at different stages of their careers, from those fresh out of academia, to those considering a pivot into cybersecurity mid-way through their career, and 'different types of initiatives are required, to create a fully inclusive environment, that removes barriers'.

A CASE STUDY FROM MICROSOFT

How Microsoft is updating sensitive language

Microsoft has consistently transformed the way that people live, work, play, and connect through technology. With a corporate mission **'to empower every person and every organisation on the planet to achieve more'**, Microsoft is committed to designing products and services that are both inclusive and accessible to all that use them.

Financial services is a focus industry for Microsoft, helping the sector to streamline core systems and reduce cost and risk, in order to achieve differentiation and spur sustainable growth. The focus is on providing services that facilitate a trusted cloud with pervasive intelligence. Microsoft's engagement with regulators and the financial industry helps improve transparency and customer assurance in adoption of innovative technology.

An early effort to remove sensitive language from Microsoft documentation and code began after the fatal shooting of Michael Brown in 2014, when initial updates to guidelines, documentation and code were made. This commitment to change was emphasised further with the acquisition of GitHub in 2018, utilised by over 65 million developers, in promoting leading practice for software code.

Why and how

A common reference to a primary/secondary relationship in software is master/slave (ex. primary server/slave client). This language does not align with Microsoft's mission. The need and principle driving these updates was clear, yet the high volume of articles on docs.microsoft.com, the site for Microsoft's technical documentation, required a methodical approach. The steps taken to update insensitive language are highlighted below:

Step 1: Identify stakeholders
The documentation team sought help across the company to consider the context of how these terms are utilised. This required input from engineering, marketing, legal, editorial, localisation and diversity and inclusion teams. They also consulted industry partners for more complete alignment. These are initial guidelines that will be revisited over time:

- **master**: Microsoft is not changing all references to master in documentation since it has many meanings. We're changing explicit references to slave (ex. *master in/slave out* for hardware signal names) and implicit references (ex. *primary server* that implies a *slave client*)
- **slave**: We're changing to *secondary* or other appropriate term. For references to slave in non-Microsoft code that we can't change we add a note before the code to provide additional context: "This article contains references to the term *slave*, a term that Microsoft no longer uses. When the term is removed from the software, we'll remove it from this article".
- **whitelist**: We're changing to *allow list*
- **blacklist**: We're changing to *block list*

Step 2: Create a process that is clear and actionable:

- The document team created scripts to scan for terms and variants in articles during the publishing process. Updates are both automated and manual.
- Writers may request exceptions for *whitelist* and *blacklist* in non-Microsoft code which they can't change.

Long term

The stakeholders and processes are in place for a long-term commitment to assess additional sensitive language updates. Microsoft is partnering with other companies including IBM, Intel and VMWare to use the technology industry's influence as a driving force to deliver systematic change proactively and positively. This enablement will also speed up the adoption of change across companies.

Identified non-inclusive terms in context

Contributions from industry and the research conducted for this report identified terms in D&I Pillars which may be considered non-inclusive.

It is recognised that language is contextual and evolves over time and utilising these words in the technology vocabulary does not make them inherently "bad", nor are the suggested replacements inherently "good". In themselves the words "black" and "white", simply represent colour, but when used to infer that one colour is more positive, or negative than the other, or when used to represent opposites, the context and meaning of the words change, as does the likelihood of it causing offense or distress.

Written and spoken words can also be misinterpreted, or have different meanings when expressed in different languages and cultures; and for the purpose of this report, the English definition of terms has been utilised, since this is typically the main business language commonly used in a technology and cyber context.

Being mindful of how a word itself has become corrupted through misuse in context is a good first step in objectively identifying a broad suite of potential terms that may require replacing. This view also ensures that technology practitioners are not goaded into feeling that they have set out to be deliberately egregious.

As language evolves, its use evolves, and it is important to reflect on its current contextual use to promote diverse and inclusive working practices and culture and be mindful about the effect that language may have on people. Terms now deemed unacceptable were previously acceptable, and it is conceivable that as cultural norms and social values continue to evolve, that other terms may become unacceptable over time. Some suggestions related to common terms and suggested alternatives have been included in the appendices, and it can often be helpful to highlight that such terms have already been widely adopted across the industry.

Recently National Institute of Standards and Technology (NIST) released guidance encouraging their authors to consider the context of terms when writing NIST Technical Series publications. Within the guidelines they asked authors to avoid terms that use black to mean something bad and white to mean something good, terms that perpetuate negative stereotypes and unequal power relationships and terms that assign gender to inanimate objects. As well as this, they encouraged the use of plain and people-first language, to not identify gender unless necessary for comprehension, to ask individuals for their names, prefixes and personal pronouns and to pay attention to the order in which groups of people are presented. These are valuable considerations when questioning when to use terminology.

In addition to terminology, there are also examples of visual cues and graphics used alongside that may be considered non-inclusive. These visuals reinforce negative stereotypes, such as the portrayal of a 'dark figure in a hooded jacket' to represent a cybercriminal and propagates the use of inappropriate language. This is particularly relevant as touch technology increasingly relies on icons or facial recognition datasets for search tools and other applications.

Language affects how people see the issues they are trying to solve and can impact the decision-making. As the language builds assumptions, these then need to be broken down and challenged when trying to manage technology and cybersecurity differently. Bias in language and visual cues have also been identified as key ethical considerations in the training phases of machine learning and facial recognition, to establish pattern recognition, and false positives. The potential for reinforced biases is an important factor to consider when designing and building technologies, in order to acknowledge and remove any potential 'poisoning' of algorithms.

UK Finance members a driving force in tackling this topic

To further explore the use of non-inclusive language, a survey was conducted with UK Finance members to gauge their experiences and issues identified.

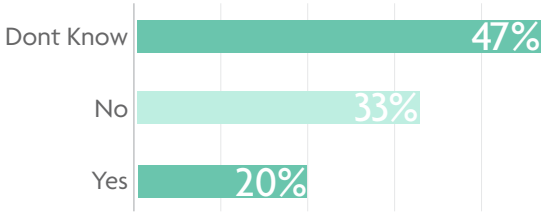
Do you agree that there is currently an issue regarding non-inclusive language being used in technology and cybersecurity within financial services?

More than 50 per cent of participants indicated that they believed there is currently an issue regarding non-inclusive language in technology and cybersecurity within financial services. A further 27 per cent had no opinion on the matter, which may be indicative of more education being required on the topic, to arm organisations with the tools they need to aid discussion, form an opinion and create a plan.

Hem Pant, Head of Information Security, BNYM International, stated: "It is imperative that all UK Finance member organisations work together, if only a few companies change their use of language then the majority will still be using insensitive and non-inclusive terms."

To the best of your knowledge, is the use of inclusive language being built into emerging and new technologies in your organisation, such as artificial intelligence, machine learning and chatbots?

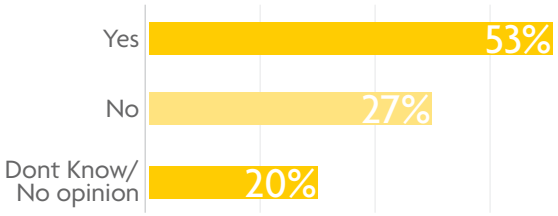
47 per cent of participants said they did not know whether actions were being taken to remove the use of non-inclusive language, which may be indicative of a lack of strategy and direction.



Organisations who reported positive action had awareness campaigns and messaging from the company to employees. This indicates that even if an organisation has a policy, further improvement on employee communication and awareness is needed.

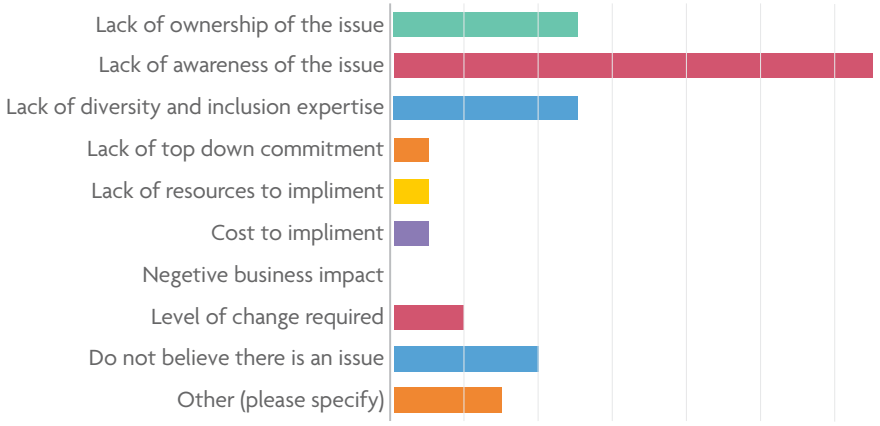
Is use of inclusive language and visual identifiers adequately built-in to the development of graphical images such as advertising and training materials at your organisation?

While 60 per cent indicated that they do not actively monitor the use of non-inclusive language, 53 per cent said that they believe that the use of inclusive language and visual identifiers are adequately built into the development of graphical images.



Organisations appear to be aware of the effect of language to some degree and have taken active steps to ensure their brand image is inclusive. It is important for organisations to not only work towards an inclusive brand but to also embed this into every part of their organisation.

What do you perceive are the top three barriers to changing non-inclusive language (in a technology and cybersecurity context) at your organisation?



The highest perceived barrier was lack of awareness of the issue. Joint second were lack of ownership and lack of diversity and inclusion expertise.

Franky Biles, from Lloyds Banking Group Security Education and Awareness, noted that 'most colleagues are aware of inclusive language and try to drive it. But change takes time, and it takes courage to repeatedly challenge seemingly small words in a professional environment'.

Furthermore, Hem Pant at BNYM International highlighted that 'Firstly, people need to be educated and made aware of the topic and issue, they can then start to identify non-inclusive terms and alternatives. People need to be offered alternative language and terms, as otherwise they won't change'.

This is echoed by Fox Ahmed, Global Head of Cybersecurity and Technology Regulatory Risk, at BNP Paribas, who said 'there's a key piece here around understanding and education. Part of that is not understanding the history, or how the context of the terms has changed. Equally, it can be a light bulb moment, for people to better understand themselves in terms of their own privileges, and the impact this may have'.

This was a sentiment echoed by the technology risk director at a global investment bank who said: 'A barrier to changing non-inclusive language is the lack of industry guidance/cohesion around a common set of terminology. Given the collaborative nature of engineering/cybersecurity, it is important to coalesce around a single framework or set of terms so that it becomes part of the culture of engineering across all types of organisations.'

It's clear from the research and discussions that UK Finance members believe there is a challenge around the use of non-inclusive language. Organisations are asking for a common set of terminology and alternative terms that people can get behind to drive the change needed, through industry guidelines and active discussions to elevate the topic to the right levels.

Driving positive change

Cybercriminals are continually changing and modernising their tools and methods. They recognise the evolution of cybersecurity as an opportunity of scale. By allowing more people to easily understand the fundamentals of security and take an active role in shaping its culture, better defences can be built. Therefore, language plays a vital role in narrowing the gap.

To truly influence and shape the industry's culture, organisations are required to examine how and what is communicated, and how to make cybersecurity easier to understand. It's perhaps one of the reasons why addressing language and biases in technology and cybersecurity can drive positive action that can be emulated across all aspects of the business.

What change has been driven across organisations to date?

Just like Microsoft, there has been a recent surge in organisations removing racially non-inclusive terms from their code and technology.

In May 2020, the National Cyber Security Centre (NCSC) said it would stop using the terms 'whitelist' and 'blacklist', instead using 'allow list' and deny list' in response to a customer request, citing that 'every little helps' when it comes to being more inclusive for all.

Apple announced an initiative to remove non-inclusive language in its developer ecosystem, after the Worldwide Developers conference in June 2020. In the Apple style guide, it also included alternatives to 'master/slave' and 'whitelist/blacklist', as well as encouraging readers to learn about Black leaders who have shaped the world.

UK Finance members have also brought in policies against certain terms. Emily Turner, Head of Education & Engagement within the Resilience & Security Office at Lloyds Banking Group, noted that 'the process was easy, changing policy wasn't a problem and we sent out an email informing people. The biggest hurdle was people using the terms out of habit'.

Changing technology and cybersecurity language can be driven by the respective communities and initiatives, but to be truly successful it needs to be considered in the context of a wider corporate and social responsibility strategy.

Firstly, leadership needs to understand the challenge – the impact it has on employees, the ability to attract diverse top talent and what needs to change. Reinforcement and consistency of messaging is key in driving sustainable change that becomes part of the embedded culture.

The Operational Resilience lead at a regional building society agrees: "The concerns need to be recognised by all, and organisations and employees need to not be afraid to challenge and take individual responsibility."

The change in language can start with quick wins such as the policy around language and making changes to coding language in emerging technology, which can be used both as a driver for larger changes in language used in the organisation and a way to start the conversation.

This was echoed by the senior operational risk manager at a private bank, who highlighted the need for 'communication to engage, guide and encourage the use of standardised language, through training and education'.

Shaping the conversation

Changing and replacing technical terms is only part of the equation, and it's clear from research and UK Finance member feedback that challenges persist with employee engagement, changing stereotypes and the negative connotations associated with language and imagery that are perhaps harder to navigate and change.

A strong culture of inclusion is key to ensuring that people are constantly using an inclusive lens not only when making decisions, but also when using language in discourse and in other situations such as documenting and writing code.

Lawrence McEwan, Head of Enterprise Security at Nationwide Building Society, commented that: "Language is one of the most important levers of modern civilisation, it often guides our thinking and behaviour. As the technology and cybersecurity sector evolves, it is imperative that we decode some of the terms with negative and prejudiced connotations in our language and replace those terms with progressive inclusive terms."

Any culture-change programme needs to be rooted in ensuring that people are shown how inclusive behaviours and concepts can be practically applied to their day-to-day work and provided with the resources and guidance to help them to do so. Organisations must recognise that this isn't something that will happen overnight and is an ongoing learning journey, enabling each person to progress at the pace that best suits their personal learning. This level of culture change will not be achieved simply by unconscious bias training alone, though that is a start. It requires investment in a fully-fledged and long-term programme of learning, regular nudges, resources and genuine commitment from both an organisation and individuals.

The focus should be on learning, not shaming, and recognising that everyone can fall prey to demonstrating non-inclusive behaviour. This aligns with seeing moments of failure as opportunities for open discussion and learning.

To illustrate this point, Paul Vincent, IT Cyber Security Director at Lloyds Banking Group, demonstrated how the bank created the '3 Principles of Respect' to help guide the conversation in a less threatening way:

3 PRINCIPLES OF RESPECT

Think before you speak. Think about how your 'words count'. How will they be perceived by those you are speaking to or those observing. Avoid phrases that link black with negative situations (e.g. Blacklists, Blackout, Black Sheep, Black Swan). Replace words such as 'Master' and 'Slave' with Primary and Secondary. Lead by example but be cautious about creating rules for others. Be curious about common phrases and share what you learn with others in the spirit of understanding.

Do not be quick to assume malice. If someone says something you feel offended by, do not be quick to assume they intended it to be hurtful. Feel empowered to call out offensive terms/phrases, but do so in a kind, considerate and empathic way. Confide in a manager you have a good relationship with if you do not feel you can speak to the person yourself.

Be quick to apologise. Full stop. It doesn't matter about who was in the right or wrong, be quick to apologise if you have upset someone by something that was said. Make sure you are sincere and learn from the experience. We all say things that are taken the wrong way or blurted out in a clumsy manner...it's how we deal with it afterwards that defines us.

This level of culture-change requires investment in a fully-fledged and long-term programme of learning, senior sponsorship, regular nudges, and genuine commitment from individuals to 'walk the talk'. As the head of security awareness at a high street nank highlighted, 'it's OK to admit that it may be hard, but it's important to offer some tips and guidance, and to create a safe forum where people can ask questions without feeling attacked or guilty'.

Hem Pant of BNYM International, added that 'we can make an internal commitment to change the words we use and be courageous enough to call out the use of such language. Language links our shared cultures and values and must evolve alongside these constructs whether passively or actively'.

STEPS TO SUCCESS

Changing technology and cybersecurity language in organisations can be driven by the respective communities but it will need to be part of the wider D&I strategy. In many situations, education is the first step in instigating change – it is key for leadership to understand the challenge, the impact it is having on the organisation's employees and future ability to attract diverse top talent and what needs to change. Reinforcement of messaging is key to driving sustainable change.

It is recognised that financial services organisations will be at different stages of their journey and hence this 12-step guide may be helpful in determining what to do and when:

Set regular review dates to examine progress, further embed the changes and ensure that the culture is adapting to embrace the change needed. Within this it will be important to gauge if further education and awareness is needed to support the right level of change.

STEP 1: **Review current language used in technology and cyber**

STEP 2: **Identify non inclusive language**

STEP 3: **Secure technology and cyber leadership support**

STEP 4: **Engage central D&I or HR team**

STEP 5: **Agree a set of alternative words to replace the non-inclusive language**

STEP 6: **Business Leadership sponsor**

STEP 7: **Consider cultural alignment**

STEP 8 **Engage employees to help shape response**

STEP 9: **Approval of alternative words**

STEP 10: **Communication strategy**

STEP 11: **Instigate changes, update policy documents**

STEP 12: **Assign maintenance responsibility**

CALL TO ACTION AND KEY TAKEAWAYS

Remember many organisations have already started on their journey to actively change non-inclusive language. It is not necessary to start from scratch, but rather to build from the foundations already set by some of the leading technology companies and industry bodies. It is imperative that all UK Finance members work together – if only a few organisations change their use of language then the majority will still be using insensitive and non-inclusive terms.

The below table highlights areas to considered when building a strategy and plan for effective change, which focuses on four key areas:

1. Technical changes to systems and products
2. Driving the right culture from the top
3. Engaging employees in the conversation
4. Continuous improvement and policy review

1. Technical changes to systems and products

- Pilot programs to identify and replace hard coded terms.
- Determine alternative options or create tools in developing new/emerging technology to QA such language prior to release
- Include a non-inclusive language review point from day one in new projects
- Understand potential biases applied in AI/ ML algorithms, and how this can be counteracted.

2. Driving the right culture from the top

- Engagement of senior sponsor to drive the tone from the top.
- Support from overall business leadership to stand behind changes
- Build a core team of champions within Technology, D&I team, Talent and policy.
- Drive inclusive culture through mentorship, sponsorship and allyship initiatives.

3. Engaging employees in the conversation

- Encourage open dialogue / seek opinions and viewpoints
- Publish communications on positive changes
- Perform educational sessions for technology and cybersecurity target groups (strategists, product owners, developers, coders, CTOs and users)
- Empower people to utilise available tools / products to identify non-inclusive language

4. Continuous improvement, and policy review

- Review current language used in technology and cyber and agree alternative terms
- Schedule future review of policies
- Consider wider impact of non-inclusive language beyond technology and cybersecurity as a secondary focus area
- Review current technology recruitment advertisements against non-inclusive language – and agree ongoing protocols.

APPENDIX – ALTERNATIVE TERMS

These tables represent examples of non-inclusive language utilised in technology and cybersecurity that have been identified as part of the research for this report. The list is not intended to be exhaustive but provides examples of terms that may be perceived as offensive by certain groups of people.

Suggested alternatives to the terms have been provided, some of which have already been widely adopted across the industry. When assessing the use of the words, and alternatives, organisations need to consider the contextual meaning, how these may be used within their own organisation and whether there may be cultural variances that may also need to be considered.

Organisations with an international presence should consider how the use of words may be perceived or translated when used in different cultures or translated to/from English as terms may have different meanings or connotation.

Conversely, there may be words utilised in other countries, or cultures that may also be deemed offensive. It is therefore important that variances in terms and their meaning be assessed for relevance and appropriateness.

Race and ethnicity

The terms highlighted below may infer a level of racial bias or discrimination.

White-list / Black-list	
Use in technology	Whitelist is often used to describe something that is "good" or "allowed" while blacklist is used to describe something that is "bad" and should be blocked or "denied". Typically used to infer an approved list of programs, software, or system files that may be allowed access from a computer, or device.
Suggested replacements	Allow List / Deny List Approved List / Block List

Master / Slave	
Use in technology	Master/ Slave when used together is typically uses to infer some form of dominance, or hierarchy, such as database or server architecture, or backup regime.
Suggested replacements	Primary / Secondary Active / Standby Primary / Subordinate

White hat / Black hat	
Use in technology	'White Hat' is typically used to refer to an unauthorised user who accesses a system without harmful intent, whilst 'Black Hat' is typically used to infer an unauthorised user that accesses a system with harmful intent. In this context, white is used to describe something that is 'good', whilst 'black' is something that is bad.
Suggested replacements	Non-Malicious / Malicious Ethical / Unethical Authorised / Non-authorised

Black Market	
Use in technology	'Black Market' is typically used to infer an illegal, underground or shadow market, that operates outside normal rules and regulations, and where the trade of goods or services may be prohibited by law.
Suggested replacements	Illegal market Unsanctioned

Gender and orientation

The terms highlighted below may infer a level of gender bias or discrimination.

Grandfather	
Use in technology	'Grandfather-Father-Son' is typically used to infer a level of age or hierarchy in infrastructure or backups, where 'Grandfather' is an older generation of technology, or backup, whereas 'Son' is a newer generation or copy. Typically infers that 'Grandfather' takes longer to restore, whilst 'Son' is quicker to restore.
Suggested replacements	Legacy Primary / Secondary / Tertiary Full / Incremental

Penetration testing	
Use in technology	'Penetration' testing is typically used to infer an authorised security test to simulate a cyberattack, to see how far an attacker could infiltrate into the network, or systems without being detected, and to identify weaknesses in controls
Suggested replacements	Ethical Hacking Red / Blue Testing Security Assessment / Test

Man-in-the-middle	
Use in technology	'Man-in-the-middle' is typically used to infer a type of cyberattack that aims to intercept network communications between two parties; to observe, steal or re-route communications.
Suggested replacements	Intercept-attack Network interception

Male to Female	
Use in technology	Connectors are assigned as 'Male' or 'Female' when there is one or more protrusions from the 'Male' connector which fits into corresponding indentations in the 'Female' connector.
Suggested replacements	Male Alternative: Plug, Pin, Prong Female Alternative: Receptacle Socket, Slot, Jack

Accessibility

The terms highlighted below may infer a level of disability bias or discrimination.

Sanity Check	
Use in technology	'Sanity check' is typically used to infer a test of software or a formula to identify false or unexpected results, mistakes, or whether the results are 'rational'
Suggested replacements	Functional test Confidence check Sense check Spot check

Dummy	
Use in technology	'Dummy' is typically used to infer a lack of knowledge, or understanding in a subject, and therefore technical or difficult terms need to be explained at a lower level. Dummy can also be utilised in the context of coding, to describe a non-functional part of a programme.
Suggested replacements	Beginner

Military and criminal

The terms highlighted below may infer a level of criminal bias or discrimination.

Repeat Offenders	
Use in technology	'Repeat offender' is typically used to infer that someone in the organisation has violated a security policy multiple times, either accidentally or maliciously.
Suggested replacements	History of violations Accidental insider Malicious insider Threat actor When used in conjunction with phishing: Repeat clickers

Kill chain	
Use in technology	The 'Cyber Kill Chain' is typically used to explain the different phases of an active cyberattack and the mitigation required to defend and recover from an attack.
Suggested replacements	Attack chain Attack lifecycle

Wargames	
Use in technology	A 'wargame' is typically used to simulate a cyberattack in near real-time conditions, to practice the incident response strategy and plan, by all parties involved
Suggested replacements	Cybersecurity exercise / simulation

BIBLIOGRAPHY

1. #VersusRacism
2. UK National Cyber Security Centre (NCSC) – Terminology is not black and white
3. US National Institute for Standards and Technology (NIST) – NIST Technical Series Publications Author Instructions
4. McKinsey (2020) – Diversity Wins
5. Better Up (2019) – The value of belonging at work
6. Randstad (2018) - Salary survey paying attention
7. Gov.uk - The Parker Review
8. FCA – Why diversity and inclusion are regulatory issues
9. FCA: Why black inclusion matters to us
10. Centre for Banking Research, Cass Business School University of London – Gender Diversity and Bank Misconduct
11. Diversity in Tech – How to Achieve Diversity in Tech
12. Git Hub – How diversity, inclusion and belonging looks in the tech industry
13. Kapor Center for Social Impact – The 2017 tech leavers study
14. (ISC)2 - Cybersecurity Workforce Study 2020
15. Wikipedia - GitHub
16. docs.microsoft.com
17. Apple Insider – Apple to remove, replace non-inclusive language in code base
18. Help.apple - Apple Style guide
19. Microsoft Support – Microsoft Editor checks grammar and more in documents, mail and the web
20. Microsoft - Accessibility guide
21. Microsoft - inventory list accessibility guide
22. Microsoft Editor
23. Microsoft – Improve accessibility with the Accessibility Checker
24. Microsoft - Microsoft Writing Style Guide Released
25. Microsoft – Bias-free communication
26. Microsoft - Inclusive Design
27. Microsoft Inclusion Journey | Microsoft.com