foundry4/

Safety tech in the UK: skills & capabilities

Pamela Woods and Lucy Hart, Foundry4

May 2021

foundry4.com

Contents

Executive summary 3

About this research 8

Skills and capability model 11

The safety tech ecosystem 11

Required skills and capabilities 12

Skills and capability challenges 16

1. Safety tech is losing out on technology talent who would find its mission compelling 16

2. Safety tech needs to actively recruit for diversity while it builds its profile 21

3. Safety tech companies take the burden of putting data privacy, security and ethics first 26

4. Safety tech companies need support in how to sell their products and how to keep users at the centre of their development process 29

Conclusion and recommendations 34

Department for Digital, Culture, Media & Sport

ktn

Executive summary

Safety technology – or 'safety tech' – companies develop technology or solutions that help keep people safe online. They aim to protect users, including children and vulnerable people, from online harms ranging from cyberbullying and misinformation to child sexual exploitation and extremism.

In the UK, the nascent safety tech sector has around 100 providers, and is seeing rapid annual growth of around 35% in sector revenues. Foreign markets are particularly significant; more than half of safety tech companies have an export presence, and the UK holds around a quarter of the global market share[1].

This report looks at how the safety tech sector accesses the talent it needs – particularly the skills and capabilities for digital, data and technology roles – in order to capitalise on this impressive early-stage growth. Our findings are based on qualitative research carried out with 11 safety tech companies and underpinned by quantitative analysis of the UK's technology labour market.

As a sector that sits at the forefront of technological innovation, safety tech, in common with parallel sectors such as fintech or cyber security, depends heavily on the UK's skills and capabilities in machine learning research and software development. However, one way in which it differentiates itself is its compelling mission of keeping users safe online, which results in high retention rates and employees who help access hard-to-reach talent by championing their companies' causes.

Safety tech does face some challenges in achieving its objectives - namely, attracting suitably-skilled technical candidates; creating a diverse workforce to better ensure products address the needs of all users; prioritising data privacy and security; and centring the people it serves within product development. Yet we found that the industry is already taking steps to tackle each of these challenges.

Our recommendations seek to amplify the impact of those steps. They are designed to be tested and implemented collaboratively over the coming year by government and industry, and to create the scaffolding for the continued yet sustainable growth of this sector.

Challenge 1: Safety tech is losing out on technology talent who would find its mission compelling

Similarly to all technology sectors, safety tech looks for capable, experienced developers. Companies can find it hard to recruit people with the right mix of skills, capabilities and work experience, especially in deep technical roles such as machine learning researchers and developers.

Safety tech companies have, however, seen the benefits of hiring talent with commitment to the mission; this work can be challenging psychologically as well as intellectually, and requires an active sense of purpose.

When there is alignment between a candidate's individual values and the company's mission, safety tech companies experience successful, longer-term hires. The companies in our study see an average tenure of three to five years for employees, twice as high as the normal rate for startups.

1. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech

Companies reported that they recruit from local pools of candidates in cities (London, Leeds, Edinburgh) and wider regional UK areas (Greater London, Yorkshire). Although the workforce is often international, this is due to people residing in the UK rather than being recruited internationally. Remote working may change this, in particular for smaller companies seeking to hire specialist skills to aid their expansion but this is not expected to impact immediate recruitment of software developers.

The challenge is that software developers – even those who are looking for a role in 'tech for good' – do not seek out positions at safety tech companies. The nascent nature of the sector and the small brand names for most companies combine to create low visibility of safety tech and the challenging roles it can offer. Candidates will often be considering five or six opportunities at once, which means that salary and brand are strong factors in role selection. However our research showed that the attraction of a company's mission can enable small companies to compete against bigger corporations offering significant salaries and benefit packages, particularly when employees are looking for more satisfaction from the work they do which is an increasing trend seen across all age groups given the Covid-19 pandemic and recognised fragility of life. In all cases, safety tech companies spoke of the 'delight' engineering candidates expressed at interviews when they learned about the existence of the sector. It appears that candidates are prepared to overlook the disparity in salary and brand when they understand what safety tech companies do.

Recommendation

We recommend that government and industry work together to more actively promote the story of safety tech and its growth, as well as the stories of individuals within the sector, in order to raise awareness and position it as an exemplar for other tech sectors. Sector organisations may also benefit from more closely aligning themselves with 'tech for good' certifications such as B Corp status.

We also recommend carrying out research into the pathways and motivations of technical people such as software developers to join tech for good companies, as well as the channels and methods they use. This research will help the industry as a whole promote careers in safety tech, and give individual companies the insights they need to better market to and attract the required talent. With the focus on the UK skills market, further research should include people who have returned to their 'home' country (New Zealand, Iceland, Spain, Portugal, Eastern Europe) and what this means for UK companies and recruitment opportunities from these overseas 'hubs' longer term.

Challenge 2: Safety tech needs to recruit actively for diversity while it builds its profile

Much of safety tech is driven by machine learning, which has the potential to amplify existing biases. Alongside this, marginalised and minority groups suffer disproportionately from online harms such as hate crime. As online harms discriminate against and threaten individuals, it is important to ensure that countering those harms does not introduce other biases. This emphasises the critical need to ensure that the safety tech sector workforce itself is as diverse as possible, so that it can better reflect the needs of society and the users it serves.

Within the sector, there is a concerted effort to improve all aspects of diversity during the hiring process and beyond. Safety tech companies in our study have relatively representative gender balances, with some companies managing a 50:50 male female split. Unlike the wider technology sector, where 19% of workers are women, the safety tech companies only saw this level of imbalance in their technical teams, increasing in accordance with the deep technical skill set required. All the companies in our study have majority male technology teams.

Contrastingly, deeply technical teams tend to have greater neurodiversity. Although very few of the companies interviewed used this term, several recognised that technology workers were often more neurodiverse than the general population and their company had increased tolerance to accommodate the different needs of this group.

As safety tech companies actively work to increase diversity in their workforce, it remains difficult for small companies to access harder-to-reach candidates with the right technical skills. Micro firms, in particular, feel they are not able to get the traction needed among women technologists or ethnic and religious minority groups.

Recommendation

We recommend that safety tech companies, with the support of government where necessary, develop a sector-wide diversity action plan. This should set out the steps that industry will take to benchmark current performance, share good practices and deliver a more diverse workforce. These steps should include activity to more closely understand and align the safety tech sector with diversity initiatives taking place across the tech industry, such as the Tech Talent Charter.

Safety tech companies should also look at the routes through which they recruit, and ensure their promotional materials including their company websites speak to the needs of a diverse workforce.

Challenge 3: Safety tech companies take the burden of putting data privacy, security and ethics first

Safety tech companies handle highly sensitive, personal and often harmful data. This, as well as the work they do, makes them more likely to be the target of an attack, and more under pressure for data to remain secure, even in micro and small companies early in their journey.

Safety tech companies are successfully training their people on the nature of online harms, the role of data in how their technology keeps people safe online and how innovation must remain in step with the legal and ethical requirements around an individual's privacy. They take people from having little or no previous experience in safety tech to being productive within three to six months.

However, this is a training burden for a sector which is predominantly made up of micro and small companies.

Recommendation

We recommend development of a central set of resources that help to address areas of common need, raising capability levels across the sector. These should have two broad areas of focus.

First, there is the need to offer introductory training on the safety tech sector itself, covering its scope and overall aims and challenges. This will help employees understand the broad ethical and societal context in which they operate. This could be offered as a standalone course, or integrated within related learning environments, such as training courses for developers, AI, cyber security or gaming professionals.

Second, we recommend developing a separate set of resources focusing specifically on data privacy and data sharing issues. This should include dedicated guidance on data sharing principles (for example, those established under GDPR), and an element of centralised training on best practices.

Challenge 4: Safety tech companies need support in how to sell their products and how to keep users at the centre of their development process

Safety tech is evolving rapidly to stay abreast of developments in online harms. Commercialising this complex technology is particularly challenging in an environment where many businesses are not yet cognisant of their need for the solutions safety tech offers.

In smaller companies, people work across more than one area of the business and can rarely specialise, making it harder to recruit experienced people with the right commercial skills to sell these products. Companies in the early stages of their product development in particular need support translating how their product could meet the needs of users in the real world.

As the safety tech sector is fast-growing and eclectic, with its products and services addressing a vast array of online behaviours, it would benefit from further support to bridge the gap between product design and user needs.

Recommendation

We recommend that industry leads the development of a set of safety tech design principles which represent the practices and beliefs of the sector, its users and markets. These will act as guide-rails for safety tech companies to follow when developing products, building in safety by design and keeping the user at their centre. These principles can be shared openly so that they can be employed by adjacent sectors doing similar work, simultaneously raising the safety tech profile.

More should also be done to build a shared evidence base of user insight that can be used to inform the development of safety tech products and services. The safety tech industry may want to look to the emerging use of 'design patterns' in parallel sectors such as mental health and data privacy, as examples of ways in which this can be effectively put into practice.

These recommendations look not only to bring safety tech onto a level playing field with its sister sectors, but also to blaze a trail as an exemplar for the tech industry: a sector where roles are sought-after for their compelling mission; where the workforce is truly representative of the people it serves; and where privacy and security sit at its core.

About this research

Safety tech sector
In this report, we have used the definition of the UK online safety technology sector (referred hereafter as safety tech) as outlined in the 'Safer Technology, safer users: The UK as a world leader in safety tech' report (May 2020). Safety tech providers develop technology or solutions to facilitate safer online experiences, and protect users from harmful content, contact or conduct[2].

Research scope
Foundry4 has been commissioned by the Department for Digital, Culture, Media & Sport (DCMS) and Knowledge Transfer Network to conduct research into the safety tech sector's access to talent, in particular access to skills and capabilities needed for digital, data and technology roles.

Primary research

Methodology
We conducted primary research with 11 businesses operating within the safety tech sector through the following means:

1. **Survey:** we received 14 responses (responses came from more than one individual in some organisations) to questions about recruitment challenges and skills in most demand by the organisations.

2. **Roundtable:** we carried out a remote roundtable event on 12 March 2021 to discuss two questions with attendees:

   a. What skills do you and the people who work in your company (directly or through associate networks) need to develop to increase adoption, quality and maturity of your products?
   b. What are the biggest challenges you face to growing the skills and capabilities you need?

3. **In-depth interviews:** we ran 60-minute sessions with representatives from safety tech organisations investigating their skill needs, recruitment challenges and progress in making diverse hires.

In these conversations, we spoke with CEOs, COOs and Heads of HR, as well as those responsible for and working within policy and regulation, technology and engineering, product management and data analysis.

We also attended the expo 'Safety Tech 2021: Unleashing the Potential for a Safer Internet' on 24 March 2021 and used the recorded sessions for reference.

Participants
The 11 safety tech businesses we engaged with represented a range of sizes: four micro, four small, two medium and one large based on the number of employees they have in 2021 (using the Companies House categorisation[3]).

More broadly, the organisations identified as part of the UK safety tech sector are primarily micro (59%) and small (31%) businesses[4].

2. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech
3. https://www.gov.uk/government/publications/life-of-a-company-annual-requirements/life-of-a-company-part-1-accounts
4. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech

The businesses' specialisms represent different categories within the safety tech taxonomy[5].

	System-wide governance	Platform level	User protection	Age-orientated online safety
micro	2	2		
small	1	2	1	
medium		1	1	
large				1

The businesses were also at different stages of growth and evolution; two were incorporated in the first decade of the 2000s while the rest ranged between three and eight years old.

Secondary research

To complement our primary research, we carried out quantitative and qualitative desk-based research with the support of Perspective Economics.

Quantitative research

Perspective Economics carried out analysis of job data related to the safety tech sector. They analysed data from January 2018 to March 2021. This period was chosen to yield a sufficiently high sample of job postings while ensuring it reflected the current state of the industry.

Perspective Economics used two search approaches to identify potential safety tech job postings:

1. Matched job advertisements with the ~70 safety tech commercial employers in the UK
2. Undertook a keyword search including and excluding certain job titles, employers and industries in the market more generally

The analysis took advantage of the following data outputs:

- Number of safety tech-related job postings in the UK, including a time series analysis of the number of job postings each month
- Industry sectors of the employers seeking people in these roles
- Geographic locations across the UK for these job postings
- Advertised job titles (to analyse the job roles most in demand)
- Job descriptions (including analysis of the skills, experience, education, and qualifications requested)
- Salaries or salary ranges being offered in these job postings

5. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech

The use of this database offers the following advantages:

- **Real-time analysis:** the data is up to date and can provide insights into the labour market at that given moment in time; this is especially important given the fast evolution of the safety tech sector
- **Strong coverage:** more than 40,000 online data sources were scraped; online postings reflect ~85% of jobs posted in the labour market

However, there are also limitations:

- **Selection bias:** only free-to-use job sites were scraped which potentially leaves an (unknown) risk of bias if employers are using closed platforms to post jobs or other means of recruiting including networking, head-hunting and word-of-mouth
- **Interpretation of jobs:** the sector is still emerging and as such there is limited data regarding what constitutes a 'safety tech professional'; the multidisciplinary nature of the field means that often safety tech organisations require a wide range of professionals with technical, legal, ethical, and commercial skillsets; job titles can overlap with unrelated industries, such as Health & Safety in construction
- **Small sample size:** 934 job postings were identified in the January 2018 - Feb 2021 period (an average of 25 per month) for employers within the safety tech sector, which reflects the small size of the industry (~1700 people employed[6])

Qualitative research

Alongside this data, we also carried out qualitative analysis including the following resources:

- Safer technology, safer users: The UK as a world-leader in safety tech – Department for Digital, Culture, Media and Sport (2020)[7]
- Tech Nation reports on the state of the tech market in the UK
- Safety tech company websites
- Job sites such as Otta (https://otta.com/) and Hired (https://hired.co.uk/)
- Startup industry news such as Sifted (https://sifted.eu/)
- Academic courses and training sites such as FutureLearn (https://www.futurelearn.com/)

Acknowledgements

The authors would like to thank all the research participants who took part in the survey, the roundtable event and interviews. We would also like to thank Sam Donaldson, Director at Perspective Economics, who contributed quantitative data to support our understanding of the safety tech sector.

We would like to thank the Security and Online Harms Directorate at DCMS and the Knowledge Transfer Network for their support and guidance throughout the study.

6. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech
7. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech

Skills and capability model

The safety tech ecosystem

Our study focuses on skills and capabilities within the UK safety tech sector. As an emerging sector, the core activity involves developing technology to support the protection and safety of users on the internet. However, safety tech sits within a much larger ecosystem which is helpful to understand as it incorporates the relationship that brands and service companies have with their user communities.

The chain reaction, from technical algorithms to the consumer's experience, is powerful, and safety tech companies play a pivotal role in the end-to-end journey of keeping people safe online. The underlying reliance on data privacy, security and ethics flows across every element of the ecosystem.

We will address the different areas of safety tech skills and capabilities, and the value of understanding the user, in the skills and capability model and skills and capability challenges sections of this report.

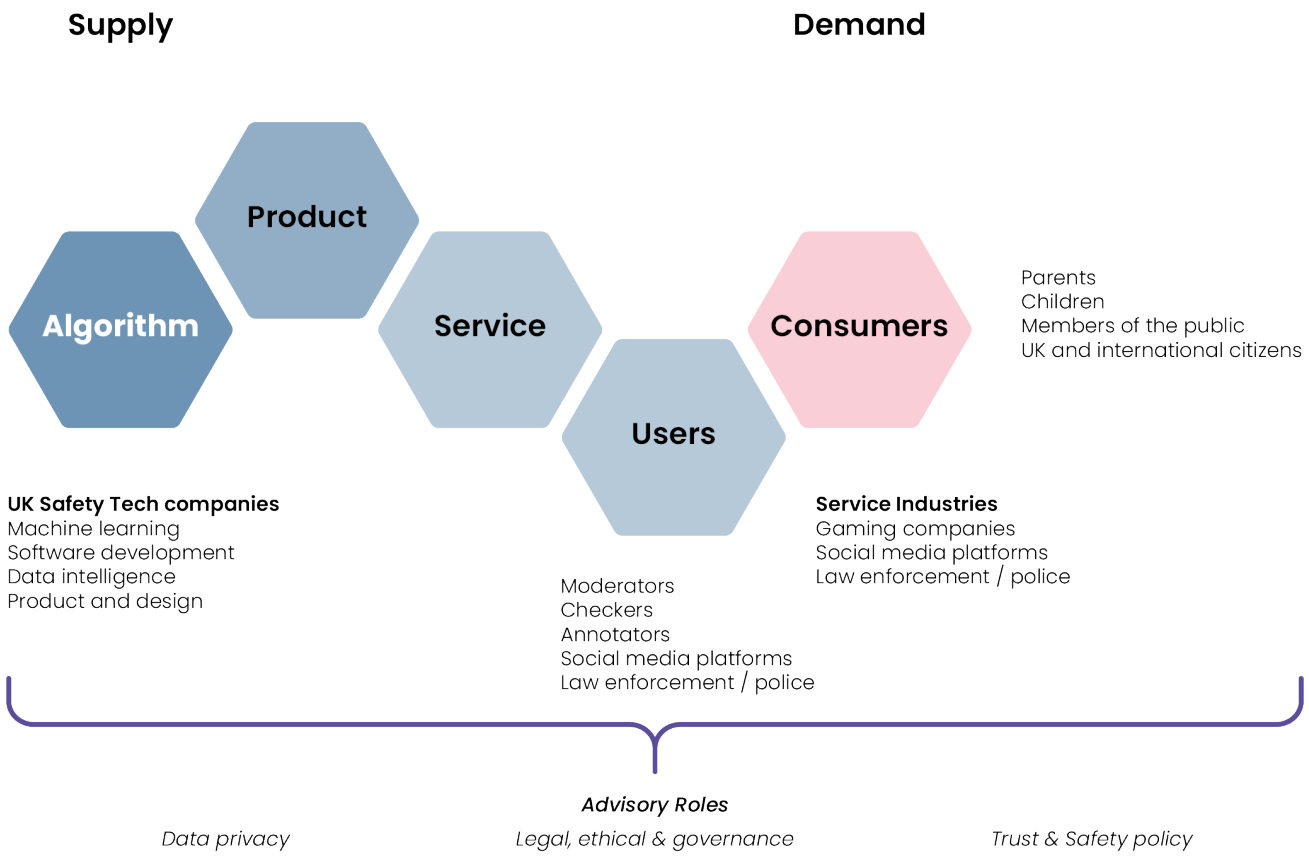


Figure 1. The safety tech ecosystem including technology, services and users

Required skills and capabilities

Alongside the operational capabilities shared with other sectors, such as finance and human resources, safety tech companies are structured around the following functions:

Technical capabilities

- Machine learning and artificial intelligence
- Software development and engineering
- Data intelligence and analysis
- Product and design

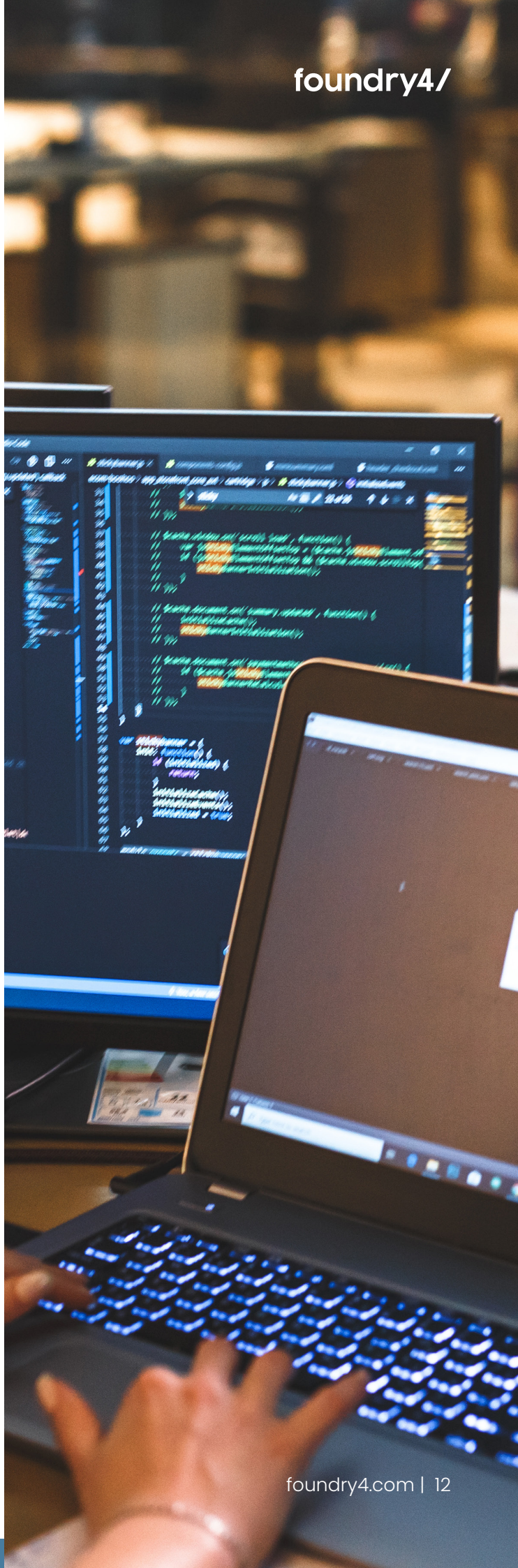
Non-technical capabilities

- Moderation, checking and annotation
- Legal and ethical governance

In micro and small businesses, individuals in the organisation fulfil a number of these capabilities, whereas in larger organisations, the roles become increasingly discrete.

We assessed the commonalities between existing technology-focused roles in safety tech companies and those they are currently recruiting:

- Capability groupings
- Associated job titles
- Skills required for each capability
- Qualifications required for each capability
- Capability characteristics that appear unique to safety tech



This table illustrates our findings for technical capabilities:

	Machine learning and artificial intelligence	Software development and engineering	Data intelligence and analysis	Product and design
Job titles commonly listed	ML researcher, ML developer or engineer, research scientist, data scientist	Software developer or engineer (frontend, backend, full stack, QA, DevOps, platform, language), solution architect	Analyst (data, specific harm, human intelligence, general), researcher, data scientist	Product manager, project manager, designer (UX, UI, product), cyber psychologist, forensic adviser
Knowledge commonly required	Data privacy compliance, information security, data ethics	Data privacy compliance, information security, data ethics	Data privacy compliance, information security, data ethics	Data privacy compliance, information security, data ethics
Skills commonly required	Python Advanced mathematics Advanced physics Advanced statistics Data science Deep learning Specific data types (eg facial, live stream) TensorFlow and PyTorch (machine learning libraries) Data visualisation	Python Java C, Embedded C, C++ .Net C# Go React, Vue and Angular (JavaScript frameworks) Node.js Swift and Xcode (iOS) Kotlin (Android) Cryptography	Excel OSINT Quantitative data analysis Numeracy Arabic, French Online harm-specific intelligence, eg mis/dis information Social media understanding Advertising tools Report writing	Product & project management Product marketing Data analysis Design (UX, UI) User research and testing Knowledge of user group, eg law enforcement Knowledge of behaviours, eg extremism Design thinking Age appropriate design
Qualifications commonly required	Bachelor's degree in Computer Sciences Masters, PhD in AI/ML	Bachelor's degree in Computer Sciences	Bachelor's degree	Bachelor's degree

Machine learning and artificial intelligence

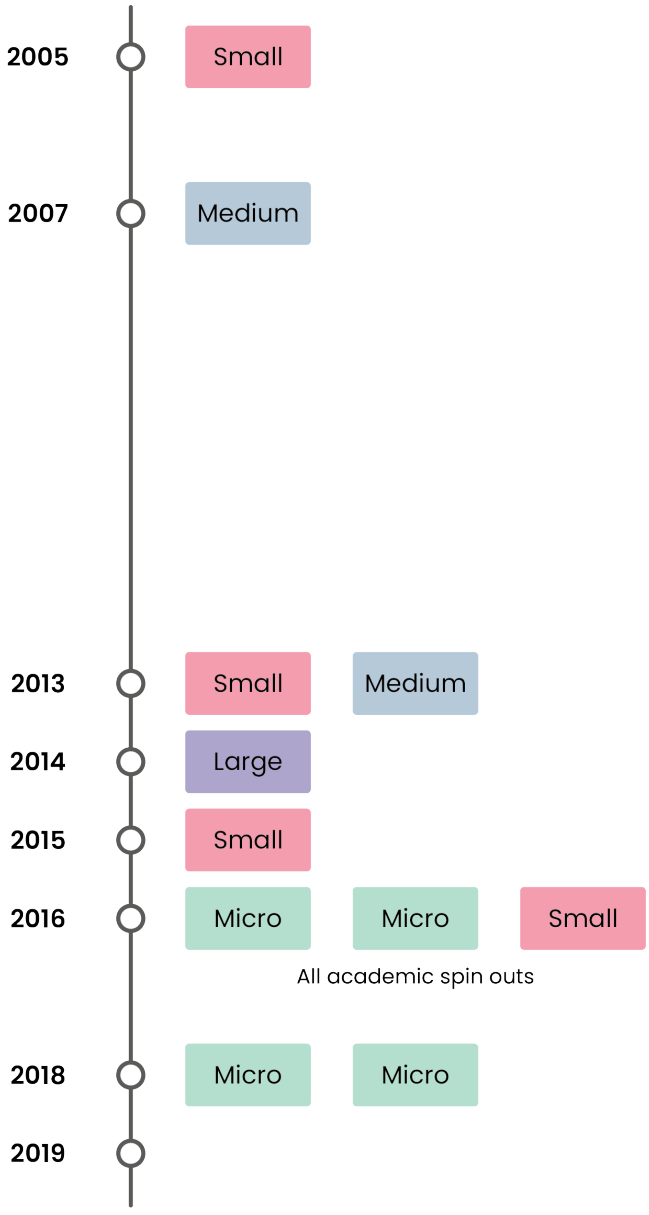
Safety tech companies' reliance on deep technical knowledge to design and build their AI tools causes them to lean heavily on researchers and engineers who have obtained PhDs and/or are "very good at maths, advanced physics and data science", particularly when companies are in the micro stage of growth. In medium and large companies, machine learning research and development is often split off into a separate 'R&D' department.

Employees in these technical roles tended to come from other organisations with a strong engineering focus – eg oil and gas, gaming and computer science academia – or directly from PhD courses. Many machine learning researchers and developers in safety tech specialise in natural language processing and computer vision, including facial recognition in image, video and livestream.

Between 2017 and 2019, the demand for AI skills in the UK is reported to have increased by 111%[8]. This correlates with the explosion in safety tech companies across those years, averaging at six new companies per year. The incorporation of companies in our study clusters around the several years prior to this period with all of them experiencing growth through a time where they are required to compete for the same specialist skills as other sectors.

Software development and engineering

All companies in the study needed software developers/ engineers. The terms software developer and software engineer were used somewhat interchangeably, although it was suggested that 'engineer' implied a greater understanding of how the underlying technology worked, where 'developer' was more commonly associated with coding activity only.



Company size based on no. of employees in 2021

Figure 2. The incorporation dates of the safety tech companies in this study

8. https://technation.io/jobs-and-skills-report/#tech-roles

However the term encompassed roles as diverse as solution architect, frontend developer and QA test engineer, with the majority of safety tech companies expecting their technical staff to be able to move comfortably between front and back end development and solution architecture in order to respond nimbly to product pivots. As small companies, employees were expected to wear many hats and therefore full stack developers were often sought by preference.

The coding languages frequently requested in safety tech, such as Java, Python and C, are commonly looked for by other tech sectors including fintech, health tech, banking and gaming[9].

The 2020 Tech Nation report shows that software developer was the most in-demand role across the UK, and particularly in city hotspots such as London, Glasgow, Edinburgh, Belfast and Cambridge[10]. Given the overlap with the safety tech hotspots (London, Edinburgh, Leeds, Cambridge[11]), it is clear that the emerging safety tech sector is competing in the same talent pool as most other technology companies. These hotspots can also provide opportunities, such as a ready supply of talent and a startup community.

Data intelligence and analysis

Alongside the development of technology, most safety tech companies have an intelligence and analysis capability. These people are responsible for gathering and analysing data. This data can be related to: online harms, such as dis/misinformation or extremist content; risks to brand reputation; matter that goes against companies' terms of use; and/or the performance of technology in countering these issues. People in this capability are required to be strong in quantitative analysis and communication.

Intelligence and analysis work commonly had a project-based nature, and consequently many safety tech companies swelled their numbers using contractors or consultants for specific projects. This tended to be for capability, as well as capacity, for:

- Foreign languages, especially Arabic
- Country/market context
- Subject matter expertise in online harms

Product and design

Safety tech companies were unlikely to have distinct product- and design-focused roles unless they were medium or large. Only one company we spoke with had a product-focused organisation in which engineers sat within product teams; in all other companies the product and design capability was either distinct or sat within software engineering.

Developing a product capability was seen as part of the scale-up journey; companies that were looking to grow from small to medium commonly mentioned plans to hire a product manager, while those looking to grow from micro to small spoke of outsourcing design capability.

9. https://technation.io/jobs-and-skills-report/#tech-roles
10. https://technation.io/jobs-and-skills-report/#tech-roles
11. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech

Skills and capability challenges

All of the safety tech companies in our research are looking to grow in the coming year, and so are expecting an increase in their need for additional capacity and capability. Hiring more staff for technical capabilities presents them with challenges as they feel the UK market is highly competitive; that technology skills are highly sought after but relatively low in supply.

Companies reported that they recruit from local pools of candidates in cities (London, Leeds, Edinburgh) and wider regional areas (Greater London, Yorkshire) in the UK. Although the workforce is often international, this is due to people residing in the UK rather than being recruited internationally. Remote working is recognised as an enabler for smaller companies to hire specialist skill sets from overseas and aid their company expansion plans. However most companies continue to see the UK as the main source of their technical workforce, enabling better face to face collaboration and removing personnel security issues when working on government projects.

Safety tech companies believe it is no more difficult for them to recruit technical people than for any other technology sector in their location. However they feel that, in contrast to other sectors, their mission is particularly compelling: to keep people, including children, safe online.

From our research, we have identified four challenge areas for skills and capabilities as the safety tech sector grows and evolves in the coming years. These are set out in the following sections.

1. Safety tech is losing out on technology talent who would find its mission compelling

In survey responses and in-depth interviews, all companies in our study reported that it was difficult to attract people who were suitably skilled in technology to their organisation. The recruitment experience of safety tech companies relates to:

- Salary and benefits
- Mission and visibility
- Recruitment and retention

Salary and benefits

Safety tech companies report that the challenge is both in finding candidates that have the deep technical knowledge required for safety tech work and in competing with bigger, well known brands seeking a similar type of person. Micro and small companies struggle to pay a salary comparable to the competition, which can be more than double what safety tech companies offer for rare machine learning skills.

Indeed, the analysis of safety tech job vacancies data suggests that over the last three years, average advertised salaries for technical safety tech roles have been in the region of £40,000-£45,000 per annum. In comparison, exploration of average salaries paid for roles with AI or ML skills in 2020[12] in the wider industry suggests average advertised salaries of £57,000.

12. Perspective Economics analysis of online job vacancies data

This only covers advertised salaries; often job postings mark the salary simply as 'competitive' subject to experience. While companies would prefer to hire mid- and senior-level candidates, the mix of lower salaries and a skill set in high demand means that they are more likely to have to recruit junior people initially. This is a challenge particularly for micro and small safety tech firms.

> *Where we lose out is that we can't compete with fintech. Banks slap a load of money on the table. Because they're struggling for staff they can overpay graduates, taking the bet they can retain them.*
>
> *Small, system-wide governance*

The lack of awareness of the safety tech sector means that the majority of potential candidates do not start out looking specifically for safety tech companies. They have choices about who they work for as demand for their technical skill set continues to grow.

> *Nothing is unique to safety tech – that's part of the problem. The skills that would be utilised by a safety tech company are in demand in other sectors – when you think about AI, that's in huge demand in health tech, life sciences etc.*
>
> *Small, system-wide governance*

Despite the difficulties, safety tech companies claim they can get a pool of people for a role, but struggle to find candidates who meet the mixed criteria they hold for technical skills, work experience and alignment in attitude with their values and mission. It seems the challenge increases as their technical requirement increases, meaning machine learning researcher and backend development roles are the hardest to fill.

One micro company explained why finding the combination of skills and experience is almost impossible and therefore they rely on graduates who they need to train:

> *In all cases, we managed to find great graduates. We haven't managed to find junior, mid, or senior level in the area. When they get too senior, they're not interested in getting their hands dirty, which is required when working in startups. We didn't get too many applications or got good applications from people who were past the point of wanting to code every day. Some were ridiculously expensive – there are other markets out there that pay maybe twice as much for the same job (eg fintech).*
>
> *Micro, system wide governance*

Where they can't compete on salary, SME companies are able to offer other benefits. Flexible, friendlier working conditions with attractive offices and perks as simple as free tea, coffee and fruit were cited as generally attractive to the under-35 workforce. Share options were also named as an incentive for people joining smaller, fast growing companies.

There are two additional advantages that safety tech companies have over other sectors: a worthwhile purpose and hard, interesting problems to solve. It is difficult to quantify the impact they have on recruitment but it is certainly recognised that once applicants are aware of what safety tech companies do, they become excited about the role and committed to the cause.

> *Through the interview process we talk a lot about safety tech and our role in the industry. I find that works well to get that excitement built with candidates. We're huge evangelists.*
>
> *Medium, platform level*

> *I hear people say "I'm fed up working for these great big banks, they just rob people". Candidates going through recruitment agencies are talking to 5-6 companies at one time. The decisions they make are around vision & values; purpose; salary.*
>
> *Small, system-wide governance*

> *What mission we're on; that's one of the defining questions we ask. That's usually when we get the best candidates - when they completely understand it. They are here to protect kids online.*
>
> *Small, user protection*

However safety tech companies are realising they need to keep salaries in review in order to remain competitive. Unlocking the next round of funding can give them the confidence to align with a rising market rate for specialist skills.

> *We went back and looked at our salary scales. Before we were slightly under market, and then I think we slipped back a bit. For me, it was a slight realisation of "if we want this ability we're going to have to pay for it"*
>
> *Small, system-wide governance*

Mission and visibility

One of the small safety tech companies is noticing that "Covid has recalibrated people's thinking", with a company's mission and values having more significance to all age groups rather than just among the under 35s. Candidates are assessing the impact they can make on the world through the work they do during the seemingly short length of their career.

Alignment with a company's values makes for a better, longer-term employee:

> *What we're looking for is people who are aligned to our vision and values. If they're not, that can give difficulties later on (that become HR ones).*
>
> *Small, system-wide governance*

> *When I ask what attracted candidates to [our company], it's working in a business that aligns with your own values. Everyone knows the work they're doing is delivering value in the mission and objectives of the business.*
>
> *Medium, platform level*

> *When we get people here and they see what we're doing, they're really passionate about it.*
>
> *Small, user protection*

The combination of candidates wanting purposeful work and the existence of safety tech companies should create a recruitment sweet spot and for one medium company, it does:

> *We can compete - our mission is very strong and resonates with a lot of software engineers. We want people to come in and solve problems straight away so we take on mid-level engineers, not grads straight out of uni.*
>
> *Medium, user protection*

However for most, lack of awareness of the sector and knowledge of the brands within it is a barrier to matching candidates and companies:

> *One thing I think we suffer from is a lack of knowledge of the sector and certainly our brand. We are drowned out by the likes of Sky Betting & Gaming in our local markets. Everyone in tech knows of health tech, fintech, etc, but online safety tech comes as a surprise to the candidates we reach out to.*
>
> *Medium, platform level*

> *Part of the picture is who you are, what you do, and how well known you are.*
>
> *Small, system-wide governance*

It is possible that the benefits remote working offers companies to throw the recruitment net wider in the UK, and even internationally, will reduce the difficulty of finding appropriate candidates, although it may exacerbate the brand challenge for them to be recognised outside their local area.

There is work that safety tech companies can do to compete with bigger brands and take raising their own visibility into their own hands. Publishing research, increasing national coverage of their products and services and being active on social media platforms and TED Talks are helping one company punch above their weight in knowledge of their brand.

> *The shine has come off Google and Facebook. The mission is much more important to [candidates] than working for a brand… Of course we lose out to them, but it's not as much of a slam dunk.*

Medium, user protection

Recruitment and retention

In the study, companies preferred to recruit through free and easy means such as posting job adverts on their website, finding people on LinkedIn and word of mouth. One large company and a small company are fortunate to get a regular stream of speculative applicants which often results in hires.

Direct and targeted head hunting also proves successful for experienced hires into specific roles but less successful to gather a pool of potential software developers. Developers tend not to promote themselves actively on professional networking sites such as LinkedIn given the continuous demand for their skills and therefore, despite the costs, recruitment agencies are used by over half of the companies we spoke to, including all the medium and large organisations.

> *We tried to avoid paying fees for as long as possible. But the space is so hard; we had to try.*

Micro, system-wide governance

> *Tech hiring has been one of our challenges – our biggest agency spend is in this.*

Medium, platform level

Companies report mixed results from recruiters. On average, they feel that recruitment agencies do not understand their business well enough to promote it to a candidate, but do know how to generate a pool of suitably qualified candidates.

> *Recruiters just farm the field. They're not knowledgeable about what we do but they know where to go look. The CVs we get, we would probably discount ~90% of them. Maybe 10% are good enough to take to interview.*

Micro, system-wide governance

The cost of recruitment is high – recruitment agency fees, the time and effort by employees to sift, test and interview candidates – and the smaller the company, the more keenly these costs are felt.

On the plus side, safety tech companies enjoy high retention of their staff. The average employee tenure is three to five years, which is high for SMEs and startups.

For context, the average safety tech firm is about six years old, so they are seeing a high level of commitment from their core staff. Safety tech companies also commented on a "surprisingly high return rate" where younger people have gone to bigger companies but returned within the year.

> *We have really high retention rates. I can think of fewer than ten people who have left in the last five years. And people come back! We hire people at entry level, they spend some years with us, then want to try something else, and they come back so quickly.*

Small, platform level

2. Safety tech needs to actively recruit for diversity while it builds its profile

Much of the safety tech sector is at an early stage of maturity[13], with the industry association OSTIA formed in early 2020[14]. As such, the profile of the sector is evolving, both externally and internally. This has a knock-on effect on both recruitment and sales, where awareness of businesses is related to awareness of the sector in general.

Three factors are important to consider in the active development of the profile of this new sector:

- Public awareness
- Workforce diversity
- Championing voices

Public awareness

The term 'safety tech' is not yet fully known within the industry, and is relatively unrecognised outside the leadership of the relevant businesses. This perhaps also reflects the general lack of consumer awareness of activity taking place to keep people safe online.

> *People don't think that it's a thing; I don't think they appreciate how much work goes on to keep them safe on the internet.*
>
> *Medium, platform level*

> *There are not that many people who know much about this. The only thing synonymous with safety tech is parental control for the general population.*
>
> *Micro, platform level*

People working within the industry identify with a range of technology sectors and subsectors, depending on their specialism, including:

- Security technology
- Fraud prevention
- Digital identity and biometrics
- Countering online harms, including mis/disinformation, extremism and child exploitation
- Reputation management
- Social media and community management

Searches for safety tech-related roles beyond the sector demonstrate the diverse areas that overlap in this space; results yield employers from broadcasters to police forces to large social media companies, with a broad range of job titles and descriptions. This impacts the visibility of safety tech roles to prospective employees in a competitive market.

Workforce diversity

Diversity of the workforce was top of mind for many safety tech companies. Companies interviewed commonly mentioned the following types of diversity:

- Gender
- Ethnicity and race
- Nationality
- Education and life experience
- Neurodiversity

13. https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech
14. https://ostia.org.uk

Religious and cultural background, class and disability were also mentioned.

It was recognised that a diverse workforce would diversify approaches to problem solving and contribute to the commercial success of the business. Furthermore, safety tech companies recognise their unique need to build up a diverse workforce. There is an undeniable connection between designing products to protect and influence a diverse range of people online and the diversity of their own technical teams.

> *If I have 10 people with the same background & skills, I'm going to get the same answer 10 times.*
>
> *Small, system-wide governance*

> *I think diversity will add more to our product teams to have a more balanced gender within those; we'll get different results.*
>
> *Medium, user protection*

> *I think bringing in a diversity of knowledge in whatever form that comes from is a really valuable thing.*
>
> *Micro, system-wide governance*

> *Disability. We have to look at how our products help people with auditory, motor, visual etc disabilities; we need to be aware of those challenges in our products, so we want them working with us.*
>
> *Large, age-orientated online safety*

One small company worked to offer placements to students transitioning onto a degree course having completed college-level education later in life, believing it reflected their personal drive. A micro company CEO commented on how employees' cultural upbringing affected the degree to which they were comfortable with experimentation. Several of those interviewed mentioned positive experiences of working in diverse teams.

Gender

The primary type of diversity raised was gender. Most companies claimed to have a relatively representative balance across their organisation as a whole. For example, one small company had a 50:50 men:women split, while a medium company stated that 48% of their hires in the last year were women.

However, it was recognised that this balance tipped as the roles became more technical. Universally, companies had majority male technology teams, to the extent that several of the companies interviewed had exclusively male technology teams.

It was generally felt that this imbalance represented the imbalance within the sector as a whole, starting with the gender split seen for Computer Science graduates and continuing for experienced candidates.

> *It's not easy to fix. On the technical side we're not getting anyone coming through.*

Micro, system-wide governance

> *I think it's the biggest challenge facing all recruiters in this field; 20-25% coming out of these [computer science] degrees.*

Medium, user protection

> *The problem I have is that our hiring is representative of candidates… Certain groups are underrepresented in the whole, and we've tried everything we can think of to improve it but I'm not seeing candidates from other groups.*

Small, system-wide governance

> *It goes all the way back to GCSEs and A Levels. I think the system of so few A Levels has an impact – it affects choices for ongoing years.*

Large, age-orientated online safety

> *If we end up with a dev team that's 70% male I won't feel that's a failure; we'll reflect the wider industry.*

Small, platform level

This belief appears to be true; according to a Tech Nation report, 19% of workers and 23% of directors in technology are women[15].

Religious & cultural background

It was recognised that certain religious and cultural groups were also underrepresented, and that this may be impacted by the industry's reputation. For example, one small company described the historically unjust targeting of Muslims in counter-extremism campaigns.

> *We are known for our work in counter-extremism; people in Muslim communities are wary of how that work is being done.*

Small, platform level

Ethnicity, race and nationality

It was commonly recognised that the racial and ethnic diversity of each company's workforce was influenced by the language requirements for their work, particularly in data analysis.

> *We have good ethnic diversity – in our human intelligence teams we have Arabic speakers, Thai people, Burmese.*

Medium, platform level

> *When it's a language speaker for an analyst role, we get a wider mix of ethnicities.*

Small, platform level

15. https://technation.io/insights/diversity-and-inclusion-in-uk-tech-companies/

It was also common to observe a greater range of nationalities in machine learning roles, where safety tech companies were working directly with people currently undertaking PhDs. Elsewhere in the business, there appeared to be less racial diversity, and this intersected with class and gender.

> *For our general analyst and manager applicants, we get more white and middle class applicants than would be reflective of the wider working population in London.*
>
> *Small, platform level*

> *It's mainly white guys in engineering.*
>
> *Medium, user protection*

> *Our diversity is terrible. It's a bunch of white guys and one woman.*
>
> *Small, system-wide governance*

There was some complexity around hiring introduced by the perceived need for sovereignty, particularly when fulfilling contracts for the UK public sector including central government, crime agencies and law enforcement bodies.

> *The need to stay sovereign doesn't help. For example, if I'm employing a Chinese person, the Chinese government could coerce them, so I can't use a Chinese PhD student for government contracts.*
>
> *Micro, system-wide governance*

Neurodiversity

Very few of the companies interviewed mentioned neurodiversity before being asked, and the term was not recognised by some interviewees. However, several companies felt that technology workers were often more neurodiverse than the general population.

> *It's definitely an asset. Most people in our business can be put in that category… Being in the area of computer science, we attract a lot of autistic, bipolar, dyslexic etc and we learn a much better tolerance for it.*
>
> *Micro, system wide governance*

Actions taken

Safety tech organisations were generally active in their efforts to diversify their workforce. Small and medium companies were able to cite multiple examples of actions they had taken, in particular to increase gender diversity.

> *I'm not setting a target but I will be doing the work – articulating that we care, looking for specific platforms like women in tech. I hope the end impact is that we encourage more people of colour and women into the industry in the first place.*
>
> *Small, platform level*

> *This is the most diverse company for race, language and origin I've ever worked in.*
>
> *Small, user protection*

Micro companies, by default, are able to make fewer hires and take fewer active steps to diversify their workforce. Where micro companies were diverse, it appears to be more by luck than by design.

> *Not having all male machine learners on the team would be great, but it's not easy to fix… We're not actively trying to find diverse people.*
>
> *Micro, system-wide governance*

> *All of my current lot have been through word of mouth. We've never hired anyone from LinkedIn.*
>
> *Micro, platform level*

Examples of actions taken by safety tech companies include:

- Posting on job boards targeted to marginalised groups
- Using external reviewers to assess job descriptions for gendered language
- Volunteering with coding bootcamps targeted to specific groups, such as disadvantaged young people or women
- Offering reasonable adjustments to interviewees
- Standardising structured interview questions
- Ensuring all candidates were interviewed by a diverse panel
- Connecting or partnering with networking groups for specific groups, such as 'Women in Identity'
- Carrying out unconscious bias training for all employees
- Improving the digital accessibility of their website
- Offering internships or work placements

Some of those interviewed also commented on the difficulty of tracking diversity within their workforce.

> *Neurodiversity – we do consider it. It's challenging because we tried to look at it by asking candidates. We're not allowed to ask because it might discriminate. We wanted to help in the interview – to optimise our processes.*
>
> *Medium, user protection*

> *There's a need to improve your diversity while not necessarily being able to record it. We want to be a more diverse organisation, but asking for gender data can be difficult.*
>
> *Medium, platform level*

Championing voices

There are a number of individuals and companies who are building the profile of safety tech for their own organisation and the sector as a whole.

Championing the UK safety tech sector is being done in different ways by the companies we spoke with:

- Publishing research that can be referenced in articles in national newspapers or online
- Developing the company brand through its website
- Becoming actively involved in industry groups (OSTIA, Safety Tech Innovation Network)

- Speaking on UK and international public platforms eg Innovation Network events, TED Talks
- Growing a social media following through actively participating in discussions around online harms
- Offering internships and placements
- Partnering with not-for-profit or social enterprise organisations that promote the involvement of certain groups in technology, eg CoderDojo

A welcome by-product is that companies experience an increase in speculative applications as a result. It also generates a stronger network among companies in the sector, enabling younger startups to link up with more experienced ones for help navigating 'all things entrepreneurial'.

3. Safety tech companies take the burden of putting data privacy, security and ethics first

Despite nine companies in our study being five or more years old, none expect candidates to have prior experience of or knowledge of safety tech. Safety tech awareness is not helped by the lack of use of this term on job boards and job searches, where categorisation like health tech, fintech and age tech are more common terms.

> *I don't think we're expecting people to come from that background in terms of their experience.*
>
> *Medium, user protection*

> *New people don't know anything about this industry.*
>
> *Micro, platform level*

Companies in our study expect to upskill candidates in the areas of data privacy, safety and ethics. Additionally, safety tech companies need to manage their data securely. By the nature of the work they do, they are likely to be under more scrutiny and subject to the threat of activist and cyber attacks.

In order to help the safety tech sector distinguish itself and thrive, we looked further at:

- Training in data privacy law
- Safety and ethics
- Costs and restrictions

Training in data privacy law

Data privacy was one of the most significant onboarding topics that companies in our study tackled with new joiners. The way everyone in the company thought about data privacy and its role in keeping people safe online needed to be 'baked in' to the company's way of working, among technical and non-technical staff:

> *Privacy compliance – it is specific learning which impacts devs and the features they build. Support and Product people went on external courses to learn about it and it trickled down to others.*
>
> *Small, user protection*

> *Understanding privacy and security principles – basically everyone needs that knowledge. How are we set up on Amazon? Where does the data sit? Who has access to it? What happens when it's deleted? Can we look at it? How are we collecting images from the internet to train our models; is that OK?*
>
> *Micro, system-wide governance*

> *[In onboarding, we run] a crash course on all things relating to kids, digital privacy regulations and best practice; everyone needs to be able to talk fluently about this.*
>
> *Medium, user protection*

It is clear that although this knowledge can be taught, it is not something that people gain from experience working elsewhere: the expectation was that "you have to train them with everything else related to online safety". Equally, a one-off course in this topic is not sufficient. Regardless of a safety tech company's size or maturity, each organisation felt they needed to run fast to keep up with data privacy law changes. Several companies talked about refresher courses which were run annually to keep privacy knowledge current.

> *There is privacy and information security training for all staff and refresher training every year.*
>
> *Large, age-orientated online safety*

Safety and ethics

Every person we spoke with, from founders to software developers, talked about the importance of data privacy in this sector but also understanding safety and ethics. It seems that ethics is increasingly part of the mindset of those coming out of university machine learning courses.

> *It's not just about improving the accuracy of our [AI] system but also monitoring bias. Most people have that in their psyche now, when they come to us.*
>
> *Micro, system-wide governance*

However, how it is 'taught' and how it influences a company's behaviour remains subjective and can be debated by the employees.

> *Data ethics is part of our job a lot. I don't necessarily class it as a skill. It is a constant recurring question for the organisation and that feeds into project-specific examples. It's often debated. There's formal training on that when you join.*
>
> *Small, platform level*

It seems that "the questions you ask is the skill you're learning" in this area. It is driven more from a person's perspective or approach. Undeniably that perspective can be moulded by the company, its leadership and the degree to which it encourages its people to continually ask questions and debate.

To support this and disseminate thinking across the organisation, one small, platform-level company implemented an ethics committee. The committee members were also part of project teams and represented all levels of seniority - analysts, managers and directors - in the company. This approach embedded ethics deeply within all the company's functions and enabled the thorny questions to be 'talked about all the time' rather than giving a stamp of approval at a particular stage of a project. Another, larger company had an established ethical framework to inform decision making from product design to collaboration opportunities.

Ethics didn't just influence the design and development of products and services, it also played a role in a company's decisions to do business with other organisations or countries. Safety tech companies looked carefully at briefs before accepting the work, conscious that their powerful technology could be used to drive an outcome that would not align to their values.

However safety tech companies – especially micro ones – could feel isolated in making decisions based on acceptable risk. There is no appropriate safety tech body to go to for advice.

> *We had a brief last week from a [prospective client]… What else might they use [our technology] for? Who do I go to to ask whether that's an OK thing? What's the risk level?*
>
> *Micro, system-wide governance*

Costs and restrictions

To keep on the right side of data privacy law and stay aligned with the company's safety mission, safety tech companies spoke about the prohibitive costs around getting legal help and advice.

> *It's a really challenging area to get your head around - UK data protection law, GDPR… It's technically doable but you need the legals to understand how much work needs to happen. I think there's something about more support for startups who can't afford the £80,000 for a data protection officer. How do I get a pool benefit there? You could go to an agency or legal firm but very quickly you're into £400-£500 per hour.*
>
> *Large, age-orientated online safety*

One small company had chosen to buy in privacy and security expertise in the form of audits of its data management and processes by an external firm every several years.

Privacy, safety and ethics can also restrict a company's ability to be nimble and innovate. It's essential to have quick, clear responses to know what must be done when designing and iterating something new:

> *The softer side of the technical development stack will become as important as the harder side. The more you put security privacy stuff in, the slower you can be on the agility side. When's the right time? The right understanding and cultural awareness of these things is important.*
>
> *Micro, system-wide governance*

4. Safety tech companies need support in how to sell their products and how to keep users at the centre of their development process

The safety tech sector is positioned within a wide ecosystem of organisations, products and services that exist, at least in part, to keep people safe online. Different safety tech companies in our study sit at different proximities to the consumer and are therefore selling to, and used by, different user groups.

In order to grow the sector while protecting users, we must consider:

- Marketing and selling safety tech
- Serving safety tech users

Marketing and selling safety tech

Safety tech companies can be categorised as business-to-business (B2B) or business-to-consumer (B2C) businesses depending on the audiences that they are selling their technology to.

B2B

Almost half[16] of UK safety tech companies could be classified as B2B businesses and seven companies in our study fall into this category.

B2B companies create technology products to sell to other businesses. In many cases, this technology is then integrated into the other businesses' software. The 'businesses' that B2B safety tech firms sell to might include:

- Private sector: social media companies, content platforms, broadcasters, gaming platforms, brands in all verticals
- Public sector: law enforcement, government agencies

The users are therefore likely to be software developers, moderators and analysts.

Some safety tech companies are also considering selling services, particularly moderation, alongside their products.

> *We have thought about whether we would offer our moderation service to other companies. The combination of tech and humans scales pretty well.*
>
> *Medium, user protection*

16. 34 out of 70 UK companies categorised as B2B including markets such as Law Enforcement, Gaming developers, social media providers and government, taken from the SafetyTech - Dataset (May 2020), Perspective Economics

B2C

There is a growing minority of safety tech companies whose products are used directly by consumers. This is more common in age-orientated online safety, where companies develop child-safe environments or protect them from age-inappropriate content, and in user protection, where consumers are protected or supported at the endpoint itself. Three companies in our study (small, medium and large) provide consumer-facing products of this kind.

Some safety tech businesses use a hybrid model, with a product available directly to consumers and another to businesses (eg a software development kit, or 'SDK'). These companies are also more likely to have a 'human moderation' capability, where people are used to validate and/or act upon the findings of the technology product.

The users of these products are consumers, and particularly children and their parents/carers.

Challenges

In our study, some businesses found it challenging to commercialise their products for businesses and/or consumers. The smaller the business, the harder it can be to have all the skills needed to bring a product to market. Working with small numbers of people means that employees are rarely able to work purely within one area of the business.

Commercial skills in particular are hard for small companies to recruit. It was common for the companies in our study to seek experienced hires, including for technical roles, in order to get that broader skill set to support the growth of the business better.

> *Commercial skills can be a challenge in a smaller business. Everyone gets to do a lot of things. It's a learning experience, but also hard; there are gaps in your knowledge whereas some of the mature online safety tech companies have people in discrete roles.*
>
> *Small, system-wide governance*

Even companies steeped in the machine learning research stage of product development highlighted how they struggled to find people with the skills to understand how the technical product could meet needs in the real world.

> *That's the skill set – to not only focus on the research but to help bridge that gap between what's out there [in the market] and what you've made.*
>
> *Micro, platform level*

Most businesses we spoke to in this position hired in the skills from outside.

> *If we have gaps then we tend to have advisors.*
>
> *Small, system-wide governance*

> *We have advisors, contractors, consultants that help with sales, business development and so forth.*
>
> *Micro, system wide governance*

B2B safety tech companies also raised other challenges they experience when selling to businesses:

- Brands not yet aware of their need for safety tech
- Social media companies using multiple suppliers of safety tech so it could be hard to understand their processes and needs
- Entering a new market or vertical-required domain knowledge

One micro company specified that the sales approach for safety tech was different than that used for selling other products.

> *You're not selling a machine with online safety tech… We have to take an unusual sales approach as there's a different element here; there's the fear, or risk factor to include.*
>
> *Micro, system wide governance*

Serving safety tech users

The involvement of users in the development and design of safety tech products varies across the companies in our research, affected by company size and target customer.

Researching with users

Consistently carrying out primary research with end users to influence product development was only mentioned in companies with a strong B2C focus.

> *We take the company vision, using research and feedback from research practices (like with our user advisory board) to drive product and feature development. For example, how do we create some sort of feature or logic that communicates a child's level of risk to parent or child? What advice and guidance do we take them to? We work with a product manager and product designer.*
>
> *Small, user protection*

In other companies, the feedback from users was gathered informally or at a distinct point in the product development process when development had capacity to take it on board.

> *We now need to do an overhaul of the UX. We bring in UX specialisms on a temporary basis as we don't have enough work for a full-time UX person. We're being more militant about saying no but getting a lot of requests [from customers].*
>
> *Micro, system-wide governance*

Furthermore, people in companies with a B2B focus, who had personal knowledge of a sector particularly from an earlier phase of their career, would act as proxy users to inform product development.

Medium and large companies were more likely to have discrete roles for user-related capabilities such as product managers and user experience designers. They were structured into product teams, rather than divided between engineering and product.

Micro and small safety tech companies had limited access to user research, product management and design capability. When those skills are required, they often engage contractors for the work or assign it to people from other functions, such as members of the sales or development teams.

Unseen technology, unseen moderators

B2B safety tech companies were less likely to engage in primary research either with consumers or with business users such as moderators or analysts. Even in companies where the developers and users of the tools were part of the same workforce, it was recognised that there was a gap to bridge.

> *I'm sure [the tech team] will talk to us. Like any tech company, there's the tech team with the tools, and then the people that use them. We need to bridge that gap.*
>
> *Small, platform level*

The products developed by these companies are unlikely to be 'seen' by consumers – indeed their invisibility can be a selling point and a sign of their effectiveness. This may to some extent explain the seeming lack of direct connection between safety tech B2B companies and their users.

Similarly, the accompanying services, and particularly moderation, are mostly unseen by the consumer. The moderation capability screens content on behalf of companies – social media channels, content platforms or any other organisations with user-generated content – to protect brand reputation as well as user safety. It is considered integral to the success of the safety tech sector and online safety for consumers.

> *The automation is only going to get you so far. You will also need to invest time in tools non-tech people can use to make the final decision or manage 5% error. Automation speeds up productivity by a huge amount; you have to go through 10% rather than 80% of the content, but you still have to go through it!*
>
> *Micro, system-wide governance*

> *Our human moderators are all remote (~20 part time) and review anything flagged up by the system. They can intervene as community managers… It's on two levels: personal information being shared, and also safety. They're our employees, not outsourced, and trained by us in our way of doing moderation…*
>
> *Medium, user protection*

Moderation as a capability sat at the edge of our study which concentrated on technology-focused skills. However, it was noted that the moderation user group was not often discussed. Even when companies have moderation capabilities, it is common for them to sit to the side of the core company, too; outsourced to or based in countries where labour is cheaper. For example, one large company uses a team in India for its manual checks.

People working in moderation often have backgrounds in customer support or service. They are mostly non-technical roles that involve making judgements and decisions about user-generated content based on guidance. Moderation often involves a high level of exposure to online harms, in order to avoid these harms being experienced by the end-user. This exposure has been identified as putting people working in this capability at risk of poor mental health and wellbeing and susceptible to negative effects on their relationships[17].

There is a growing awareness of the responsibility of companies – social media channels in particular – to support the psychological wellbeing of the people fulfilling the moderation capability and move away from the idea of content moderation as the "dirty work of social media"[18]. For example, the 'Child Safety Online: A practical guide for Providers of Social Media and Interactive Services' report states that good practice would be to support moderators and specialist teams with "one-on-one welfare reviews, desensitisation training, regular psychological assessments and access to 24/7 support services"[19].

The safety technology used by moderators plays a key role in the level of harm they experience and their resilience to that harm. Naheed Sheikh, cofounder of The Workplace Wellness Project – which specialises in working with Trust and Safety teams to reduce the harm to those who "handle difficult or disturbing content in order to keep others safe online"[20] – has found that the nature and proximity of the relationship between the people developing automated safety tech tools and their moderator users is a key factor in the resilience and wellbeing of moderators[21].

It is likely that interest in the moderation capability will increase in coming years as the B2C market – and its associated likelihood of providing moderation services – grows, and as B2B companies continue to export internationally to countries where the 'Trust and Safety' market is more mature, such as the United States.

17. https://jolt.law.harvard.edu/digest/the-human-cost-of-online-content-moderation
18. https://ir.lib.uwo.ca/cgi/viewcontent.cgi?article=1012&context=commpub
19. https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services
20. https://theworkplacewellnessproject.com/
21. https://cogx.live/event/resilience-and-wellness-investing-in-technology-solutions-to-content-moderation-online/

Conclusion and recommendations

Throughout this research, we have sought to understand how the UK safety tech sector accesses talent and the challenges it faces around skills and capabilities.

Safety tech is a dynamic, fast growing sector with a worthwhile mission to keep people safe online. The core obstacles it faces to achieve that mission – attracting suitably-skilled technical candidates; creating a diverse workforce to better ensure products address the needs of all users; prioritising data privacy and security; and centring the people it serves within product development – are in most part shared by the technology sector as a whole.

But for the safety tech sector the need to attract a skilled, passionate, diverse workforce is even more pressing because of the value safety tech products deliver to individuals and society as a whole.

We have identified primary recommendations against each of these challenge areas which focus on actions that can be taken in the coming year by government and industry working collaboratively.

Challenge 1: Safety tech is losing out on technology talent who would find its mission compelling

Recommendation

We recommend that government and industry work together to more actively promote the story of safety tech and its growth, as well as the stories of individuals within the sector, in order to raise awareness and position it as an exemplar for other tech sectors. Sector organisations may also benefit from more closely aligning themselves with 'tech for good' certifications such as B Corp status.

We also recommend carrying out research into the pathways and motivations of technical people such as software developers to join tech for good companies, as well as the channels and methods they use. This research will help the industry as a whole promote careers in safety tech, and give individual companies the insights they need to better market to and attract the required talent. With the focus on the UK skills market, further research should include people who have returned to their 'home' country (New Zealand, Iceland, Spain, Portugal, Eastern Europe) and what this means for UK companies and recruitment opportunities from these overseas 'hubs' longer term.

Challenge 2: Safety tech needs to recruit actively for diversity while it builds its profile

Recommendation

We recommend that safety tech companies, with the support of government where necessary, develop a sector-wide diversity action plan. This should set out the steps that industry will take to benchmark current performance, share good practices and deliver a more diverse workforce. These steps should include activity to more closely understand and align the safety tech sector with diversity initiatives taking place across the tech industry, such as the Tech Talent Charter.

Safety tech companies should also look at the routes through which they recruit, and ensure their promotional materials including their company websites speak to the needs of a diverse workforce.

Challenge 3: Safety tech companies take the burden of putting data privacy, security and ethics first

Recommendation

We recommend development of a central set of resources that help to address areas of common need, raising capability levels across the sector. These should have two broad areas of focus.

First, there is the need to offer introductory training on the safety tech sector itself, covering its scope and overall aims and challenges. This will help employees understand the broad ethical and societal context in which they operate. This could be offered as a standalone course, or integrated within related learning environments, such as training courses for developers, AI, cyber security or gaming professionals.

Second, we recommend developing a separate set of resources focusing specifically on data privacy and data sharing issues. This should include dedicated guidance on data sharing principles (for example, those established under GDPR), and an element of centralised training on best practices.

Challenge 4: Safety tech companies need support in how to sell their products and how to keep users at the centre of their development process

Recommendation

We recommend that industry leads the development of a set of safety tech design principles which represent the practices and beliefs of the sector, its users and markets. These will act as guide-rails for safety tech companies to follow when developing products, building in safety by design and keeping the user at their centre. These principles can be shared openly so that they can be employed by adjacent sectors doing similar work, simultaneously raising the safety tech profile.

More should also be done to build a shared evidence base of user insight that can be used to inform the development of safety tech products and services. The safety tech industry may want to look to the emerging use of 'design patterns' in parallel sectors such as mental health and data privacy, as examples of ways in which this can be effectively put into practice.

The safety tech industry is in a strong position to act on these recommendations given the conversations that have begun to take place; the government will need to capitalise on this collaboration in order to successfully test and implement any interventions.

foundry4/

Foundry4 Consulting Ltd
7 Savoy Court, London
WC2R 0EX
Twitter @Foundry4_UK
Email hello@foundry4.com