TESSIAN

#THE FUTURE IS CYBER

Opportunity in Cybersecurity Report 2020

There are over 4 million unfilled positions in cybersecurity with a workforce that is twice as likely to be male.

The question is: Why?

CONTINUE READING →

Table of Contents

Introduction

Despite higher-than-average salaries, the opportunity to solve real-world problems, and unlimited growth potential, there's a skills shortage in cybersecurity. In fact, the cybersecurity workforce needs to grow by 145%[1] to meet the current global demand.

That's over **four million** unfilled jobs[1].

But, there isn't just a skills gap. There's also a gender gap, with women making up less than a quarter of the workforce. While – yes – there's been significant progress in reducing the gender gap thanks to initiatives from individuals, organizations, and even governments, there's still a lot of work to do.

The first step in solving the problem? Defining it.

To get a clearer picture of the skills and gender gap in the industry, we conducted quantitative and qualitative research. We worked with the Centre for Economics and Business Research to analyze the economic impact of encouraging more women into the cybersecurity industry, we surveyed female cybersecurity professionals in the US and the UK, and we interviewed over a dozen practitioners, from some of the world's biggest organizations, about their own experiences.

With these economic and social insights, we reveal what's preventing people from joining and, more importantly, what would encourage more women to take advantage of the tremendous opportunities that are available.

After all, **#TheFutureIsCyber**

[1] (ISC)2 – Strategies for Building and Growing Strong Cybersecurity Teams

ECONOMIC IMPACT

An economic impact worth billions

Today more than ever, cybersecurity plays a pivotal role in supporting not just organizations and government bodies, but the economy.

In fact, the industry contributes $107.7 billion in the US and £28.7 billion in the UK, and that's in spite of four million job vacancies.

> “Need is the mother of invention. Highlighting the number of open positions and highlighting the fact that there are women with these skills in and outside of the industry is the first step.
>
> The fact is, **you're cutting out 50% of the population when you don't create an environment for women** where they feel they can excel and actually progress their careers.”

KPMG

Carolann Shields

Former CISO at KPMG

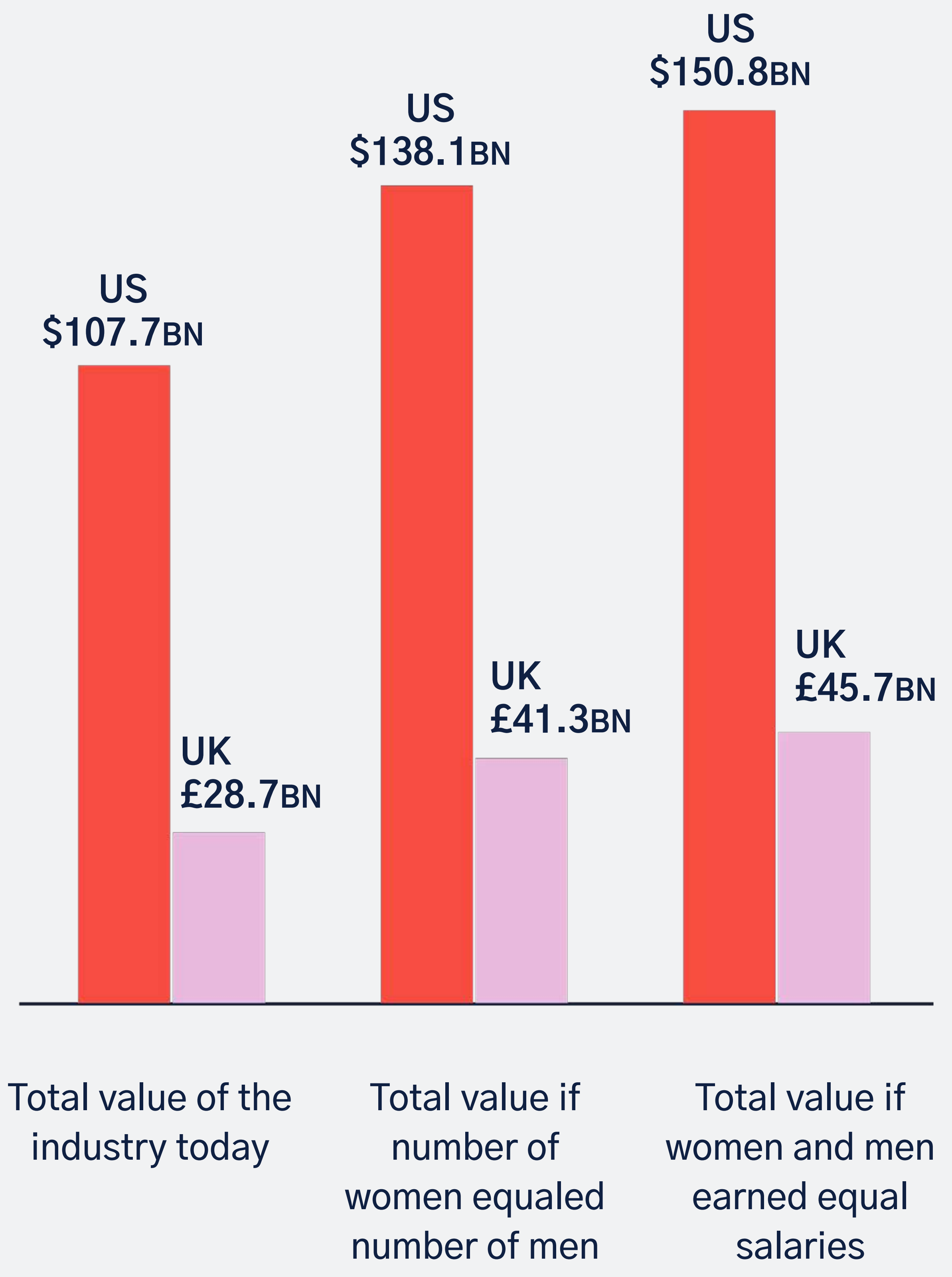
So, what would happen if we minimized both the skills gap and the gender gap, and the number of women working in cybersecurity rose to equal that of men? Our research reveals that we'd see an economic boost of $30.4 billion in the US and of £12.6 billion the UK, bringing the total contribution of the cybersecurity industry up to $138.1 billion and £41.3 billion in each respective country.

And, if women earned as much as their male counterparts – which 28% of female cybersecurity professionals say would encourage more women into the available roles – we'd see billions more pour in.

In the US, women earn 17% less than men do and in the UK, the disparity is even greater, with a gender pay gap of 19%. That means that while men working in the US are earning a median salary of $86,375, women are earning just $71,835.

Equalize these salaries, and the US will see a further $12.7 billion boost to its economic footprint, while the UK will see another £4.4 billion.

The economic impact of the cybersecurity industry



If the number of women working in cybersecurity rose to equal that of men, the economic footprint of the industry would increase by...

$30.4BN ↗ in the US

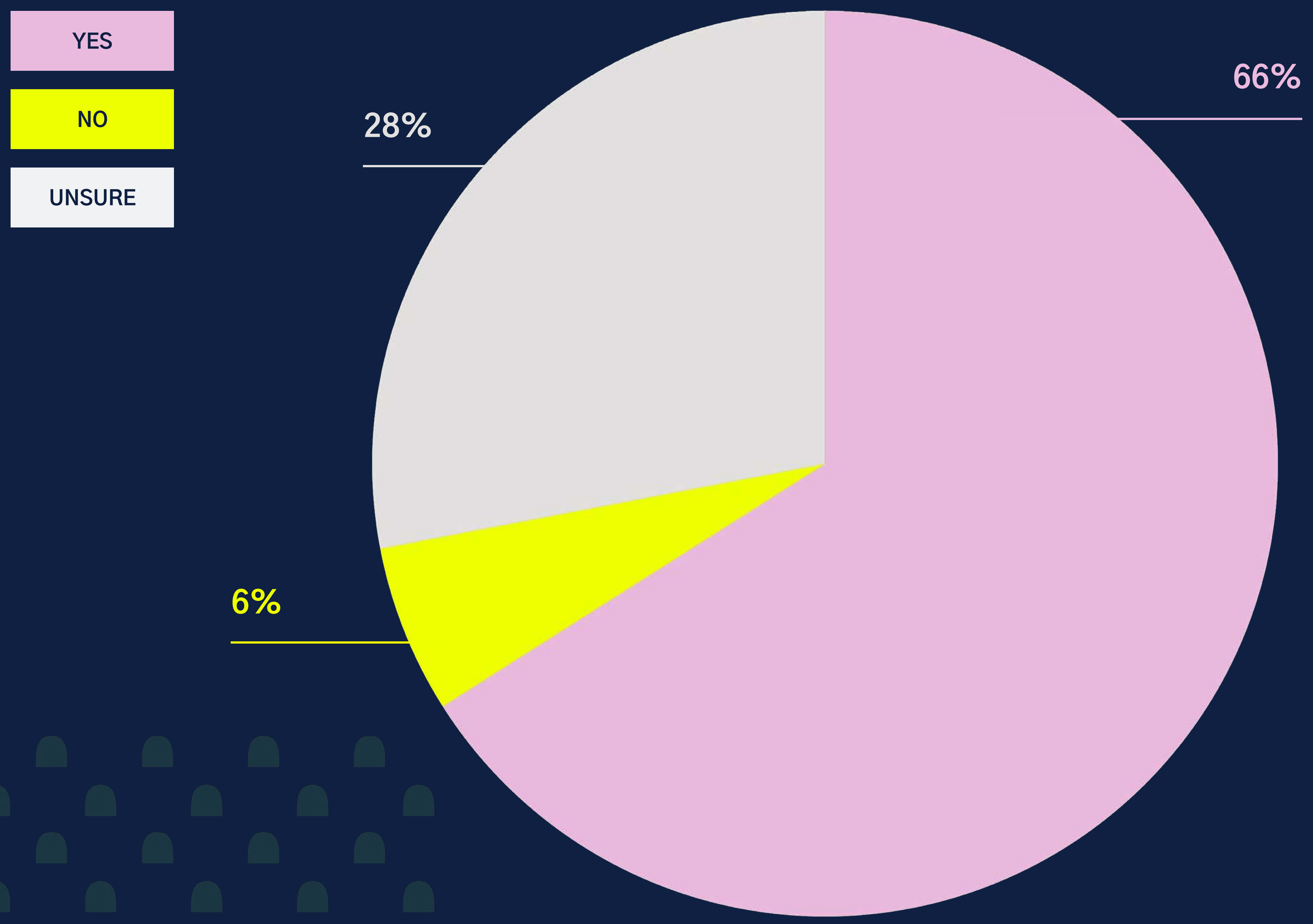
£12.6BN ↗ in the UK

If women earned as much as men, this number would increase by an additional...

$12.7BN ↗ in the US

£4.4BN ↗ in the UK

Does the cybersecurity industry have a gender bias problem?



GENDER BIAS

Yes, there's a gender bias problem in cybersecurity, but it's not the biggest challenge women face.

It's impossible to sugarcoat; there is a gender bias problem in cybersecurity.

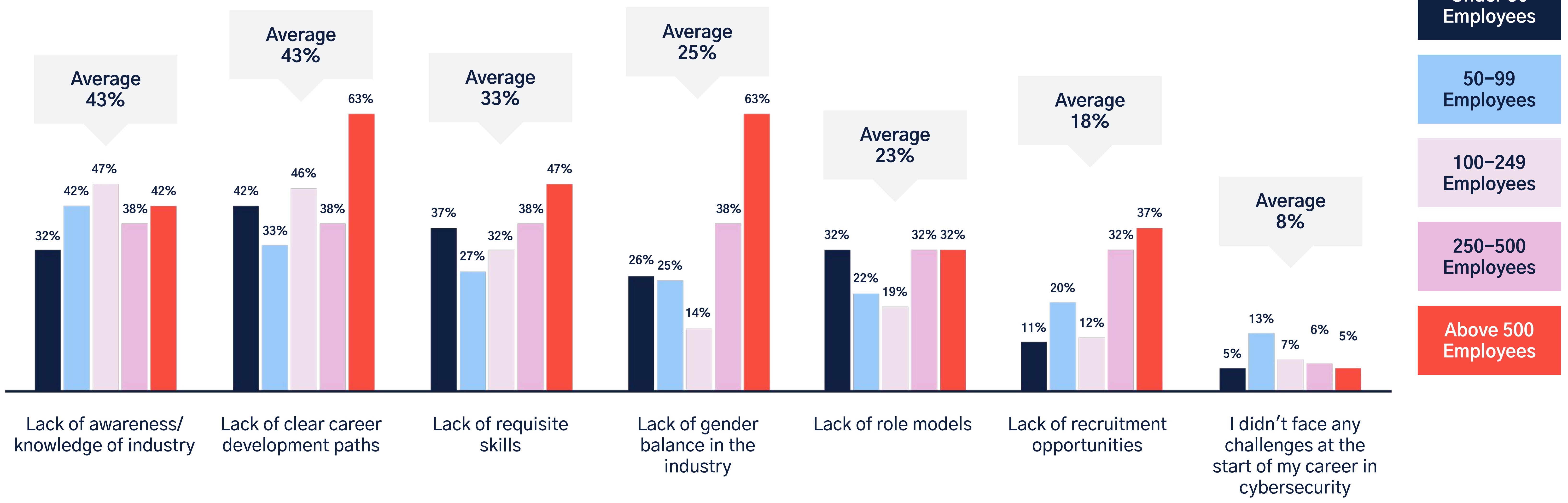
Two thirds of women (66%) in cybersecurity recognize it, and it was noted by women of all ages, from 16–55+.

But, it’s actually not one of the main challenges women currently working in cybersecurity came up against, with just 25% of female cybersecurity professionals citing the lack of gender balance as a challenge they faced at the start of their career. This means that, while it does exist, it isn’t always a barrier to entry.

Experiences vary considerably, however, based on age, company size, job title, and – more than anything else – region.

For example, women between the ages of 45–55+ are almost twice as likely as those aged 35–44 to believe that a gender-balanced workforce would encourage more people to pursue careers in cybersecurity. Likewise, women who work within larger organizations (500+) are almost three times as likely to cite a lack of gender balance as a challenge they’ve faced.

What challenges did you face at the start of your career in cybersecurity?



A gender balanced workforce would encourage more women into cybersecurity roles.

43% Ages 16–24

48% Ages 25–34

43% Ages 35–44

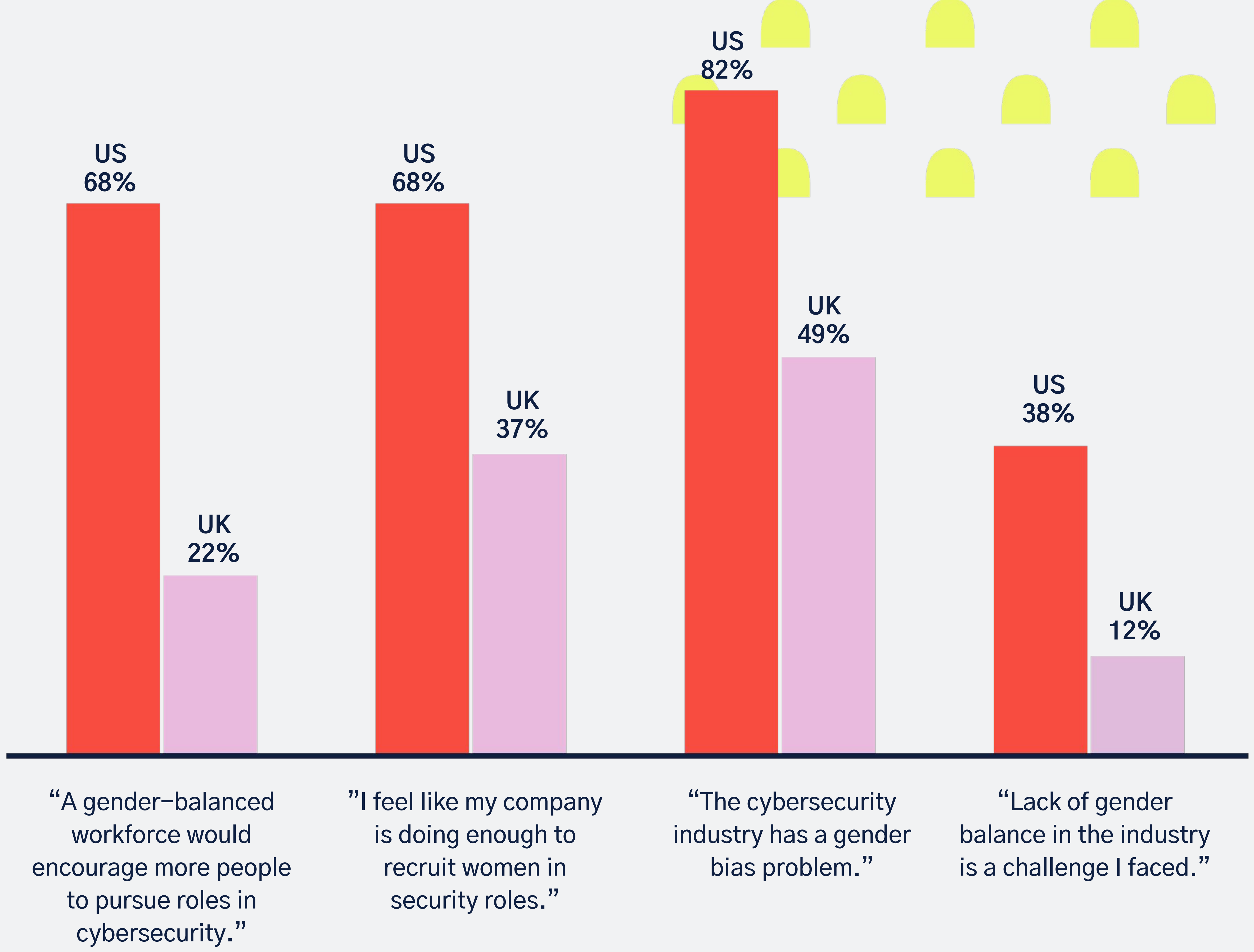
72% Ages 45–55+

The difference in viewpoints between cybersecurity professionals in the US and the UK is the most dramatic with 82% of Americans deeming gender bias a problem in the industry compared to just 49% of British respondents.

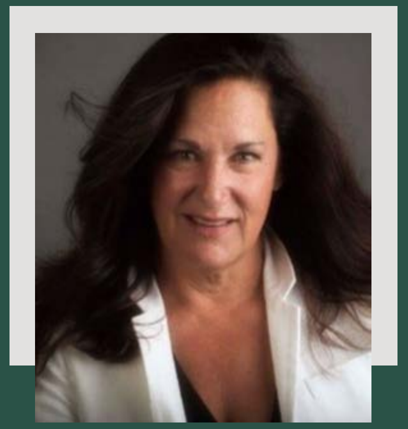
US respondents were also three times as likely to believe that a gender-balanced workforce would encourage more women to pursue roles in cybersecurity.

Fortunately companies don’t seem to be blind to the gender bias problem. 68% of women in the US believe that their organizations are doing enough to recruit women for security roles and 37% of women in the UK believe the same.

Attitudes towards the gender bias problem by country



> “In certain companies – specifically really established companies – **you still have boardrooms that are filled predominantly with white males.** You can’t underestimate the impact that has on a larger organization. It all trickles down.
>
> If you’re a woman in that environment with aspirations to be in senior leadership and you’re only seeing one kind of person in those positions, the career path there can seem very unclear.”



snapdocs

Kim Smathers

Information Security and Compliance at Snapdocs

More and more, we’re seeing diversity and inclusion initiatives directed specifically at women working in information security and cybersecurity. Most recently, IBM launched its “Behind the Code” campaign to give a voice to both male and female developers. Even governments are getting involved, with the Digital Minister in the UK launching four new projects across England to encourage more women into the field at the start of 2019.

Of course, for organizations to actually be successful in the recruitment of more women, they have to understand what’s currently discouraging them from joining, beyond gender bias.

Specifically, women cite a lack of awareness or knowledge of the industry and a lack of clear career development paths as the biggest challenges they faced at the start of their careers. A demystification of the industry is, therefore, required to encourage new entrants.

> "A lot of women in tech might not see cybersecurity as a suitable career path because it is considered quite a masculine profession. That's probably ingrained at a very young age. It's important to not be discouraged by that, though.
>
> Women can be just as successful in this industry and opportunity, recognition, and progression are absolutely available to those who work hard."

HERBERT SMITH FREEHILLS

Amy Johnson

Security Manager at Herbert Smith Freehills

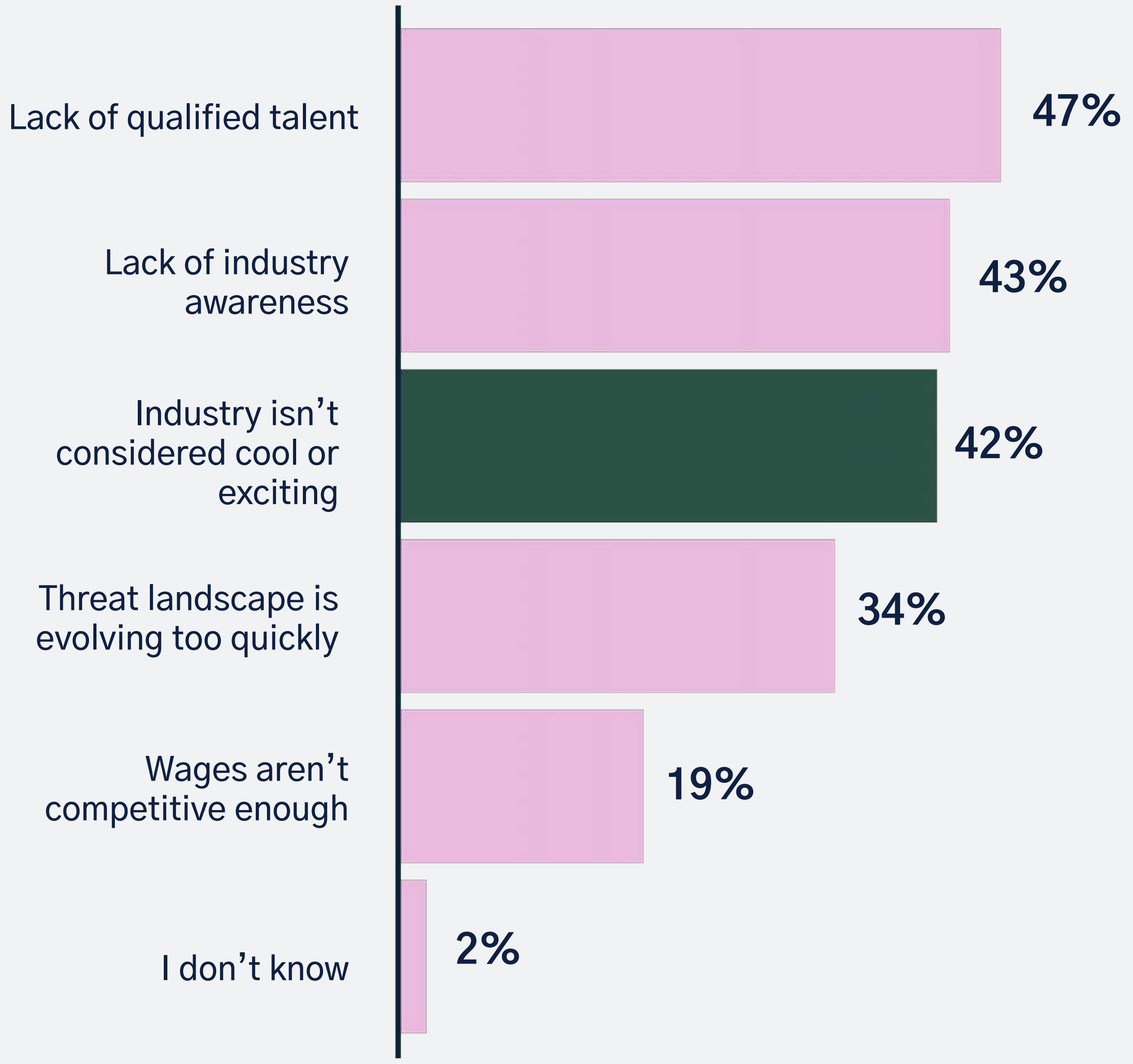
IMAGE PROBLEM

No hoodie required

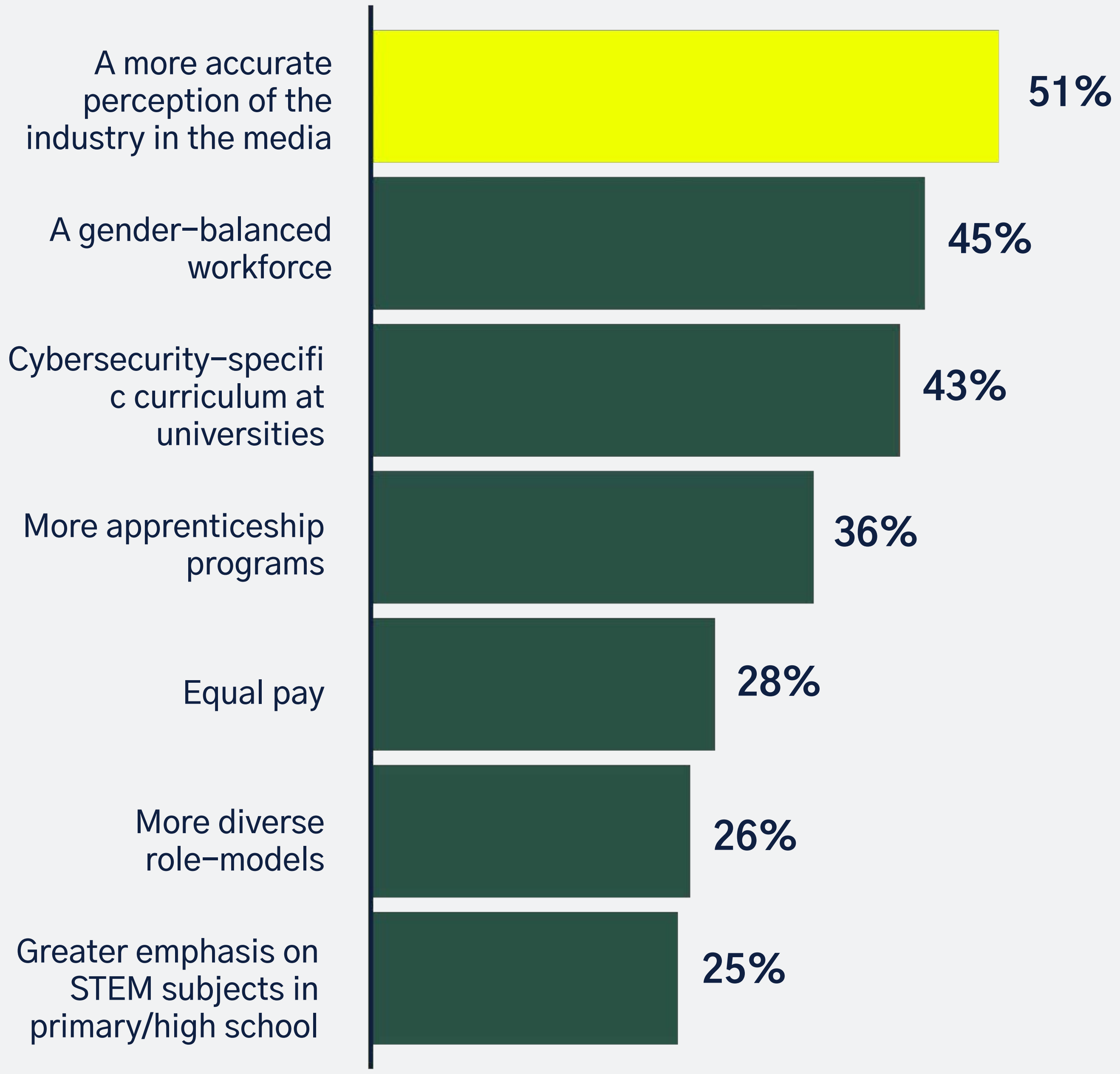
Cybersecurity has an image problem; over two-fifths (42%) of our survey respondents say that the industry isn't considered cool or exciting. On top of that, half of women believe representations of the industry in the media need to change to encourage more women to explore cybersecurity roles.

In fact, our survey respondents ranked more accurate media representations as the number one way to encourage more women into cybersecurity, followed by a more gender-balanced workforce, equal pay, and cybersecurity-specific school curriculums.

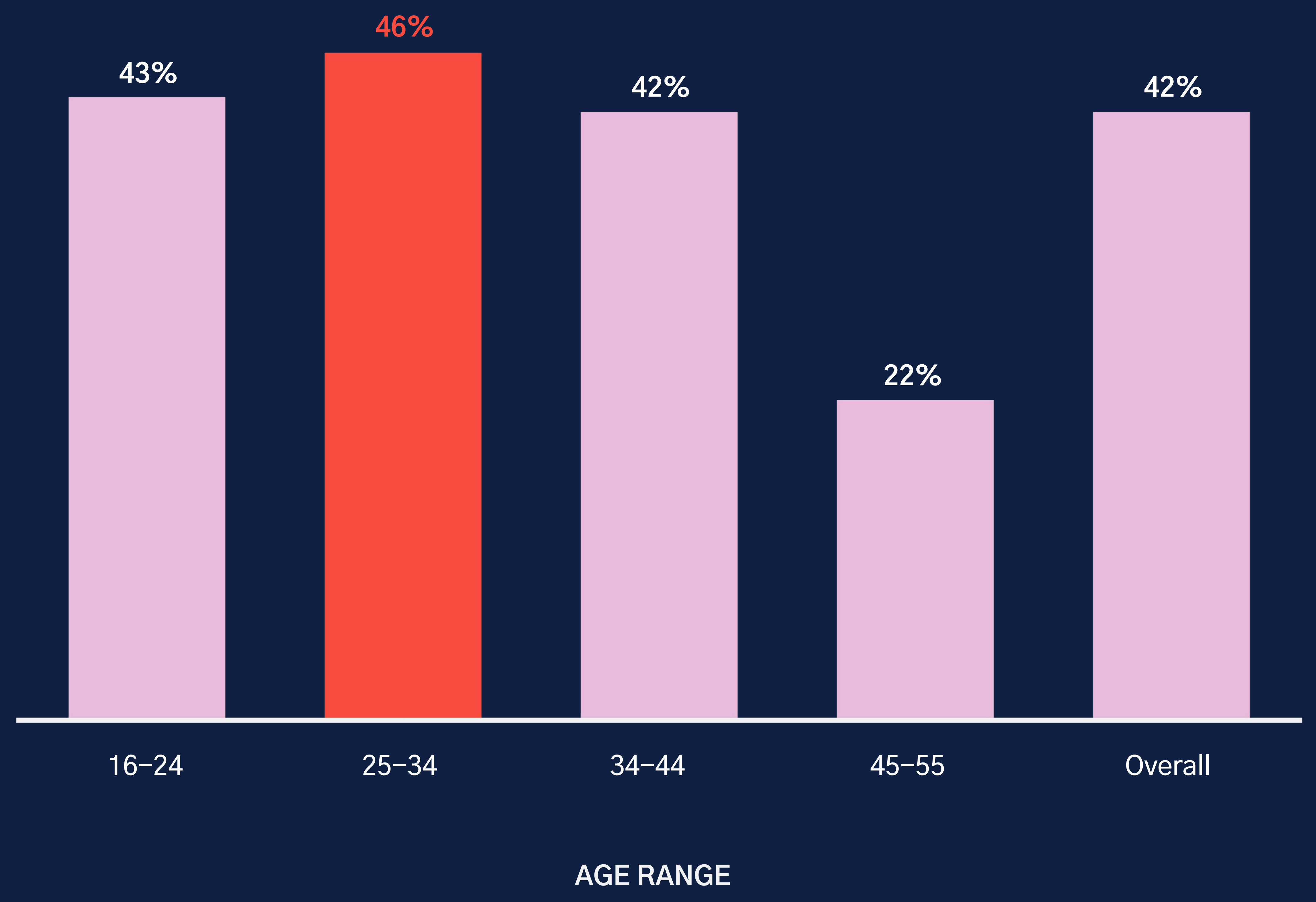
Why do you think there are over 4 million job vacancies in cybersecurity?



What do you think would help encourage more women into cybersecurity roles?



Percentage of women in cybersecurity who say the fact that the industry isn't considered cool or exciting is preventing people from joining the industry



For professionals working in the industry, it's clear not only that people on the outside have the wrong idea, but that these false perceptions are becoming one of the biggest barriers to entry, especially for younger generations.

When asked why there are over four million unfilled cybersecurity positions, 46% of 25–34 year old respondents said it is because the industry isn't considered cool or exciting. Only 22% of survey respondents aged 45–54 agreed. This highlights the importance of changing perceptions in order to inspire the next generation of cybersecurity.

So, what is cybersecurity actually like? It depends on your role within the field. And contrary to popular belief, the opportunities available are incredibly diverse.

We asked female cybersecurity professionals from companies in both the US and the UK to describe their role in a tweet; their responses ranged from people management, to solution building, to threat monitoring, proving that industry is multi-faceted.

But these women don't just have diverse roles. They also have diverse backgrounds.

Amber Pham studied Psychology while Carolann Shields studied Business. Amy Johnson had an HR career before taking on her first cybersecurity role, and Sara Zahid worked as a business analyst. Some earned – and are still earning – cybersecurity certifications and Computer Science degrees, while others learned on the job. It goes to show, you can't define the entire industry with a single identity.

CLICK ON EACH IMAGE TO READ THEIR FULL INTERVIEWS ↗

Amber Pham – Information Security Officer, Iovation

I'm a people manager, which is probably my most important role. I ensure people feel supported and in cohesion with other teams to learn and grow. I'm also the central point of contact for the corporate business and, as a part of that, I work with Development and IT teams to get security work done.

Amy Johnson – Information Security Manager, HSF

I monitor system user behavior and I review client security requirements and questionnaires. I'm very much forward-facing and part of my job is to guide the firm and our people on how to work with information and technology in a safe and secure way.

Carolann Shields – Former CISO, KPMG

I lead a team with complimentary talents and skills to work together effectively and bring transparency to an organization's cyber risk in order to identify and design solutions and processes to mitigate those risks. I also educate and influence behavior to ensure compliance and protection while making security a commercial benefit, not just a cost.

CLICK ON EACH IMAGE TO READ THEIR FULL INTERVIEWS ↗

Gisela Rossi – Software Engineer, Tessian

I work with Python to build and create products that are used by Tessian's clients to protect their Human Layer from data breaches. I work closely with product and customer success teams to ensure we're building solutions that make an impact.

Hayley Bly – CyberSecurity Architect, Nielsen

I build tools that our incident response team uses. This could be implementing a vendor tool or building something from scratch. We do both, and this includes designing how the tools are made, implemented, and deployed throughout the larger company.

Kim Smathers – Head of Infosec & Compliance, Snapdocs

My job is all about giving people an understanding of risk and figuring out how to translate, address and resolve that risk.

Hillary Benson – Director, Product, StackRox

My job is to distill business opportunity into a technical vision and development roadmap for our flagship security product, the StackRox Kubernetes Security Platform. We're building a product that enables security practitioners to rethink their approach to security by leveraging container technology.

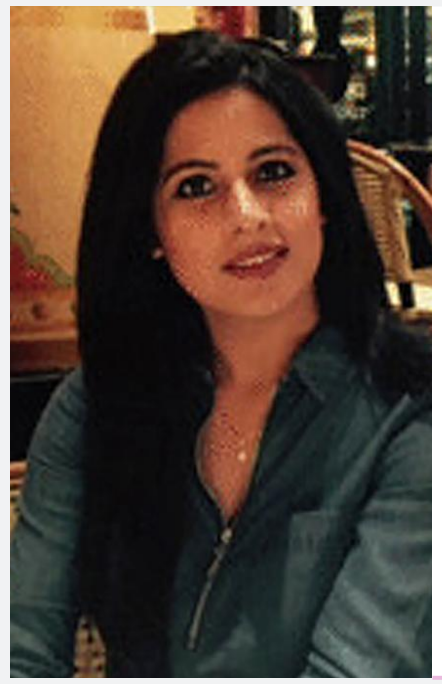
Niki Tailor – Platform Engineer, Tessian

Security, stability, scalability, reliability, and automation of our Human Layer Security platform. As a Team Lead, I have people management responsibilities too, but day-to-day my work involves solving problems, building new architecture, and empowering our engineering teams.

Shamla Naidoo – Former CISO, IBM

A CISO's job is to protect an organization's brand and reputation by managing cybersecurity threats. Protecting a corporation's digital footprint supports business growth and enables the acceleration of innovation.

CLICK ON EACH IMAGE TO READ THEIR FULL INTERVIEWS ↗



Jefferies

Sara Zahid – Assistant VP, Jeffries

I am responsible for requirements gathering, simplifying requirements, testing, organizing sprints, managing the sprint cycles, delivering requirements, communicating with stakeholders and management, and other business analysis and project management activities across Jeffries' Global Information and Technology umbrella. As a manager, one of my key responsibilities is to make sure the team stays organized.

Google

Parisa Tabriz – Director of Engineering, Google

I am a director of engineering at Google, overseeing the security of the Google Chrome web browser and managing a team of "hired hackers" called Project Zero. Our team conducts security design and code reviews, finds and fixes vulnerabilities in tech products, and delivers security engineering training. Years ago, I gave myself the title "Security Princess" – it sounded less boring and mundane than "Information Security Engineer".

KIVU

Tess Frieswick – Client Success Manager, Kivu Consulting

I help customers navigate the ever-changing cybersecurity landscape by articulating complex technical matters in a clear and concise way. I also provide technical and product support through threat intelligence research. My ultimate objective is to ensure Kivu remains a trusted advisor to clients by helping them improve and maintain their overall security posture.

Funding Circle

Swaty Lay – CTO, Funding Circle

I am responsible for delivering the right technology platforms for Funding Circle employees, borrowers and investors across all geographies. That includes everything from engineering, platform services, corporate technology, data, architecture and information security.

"Cybersecurity isn't about who you are or what degree you have. **It's about what you can do, what problems you can solve, and how well you can work with other people** to get the job done.

You don't have to play politics because your work speaks for itself. I love that."

nielsen

Hayley Bly

Cybersecurity Architect at Nielsen

SKILLS NEEDED

Creative minds needed

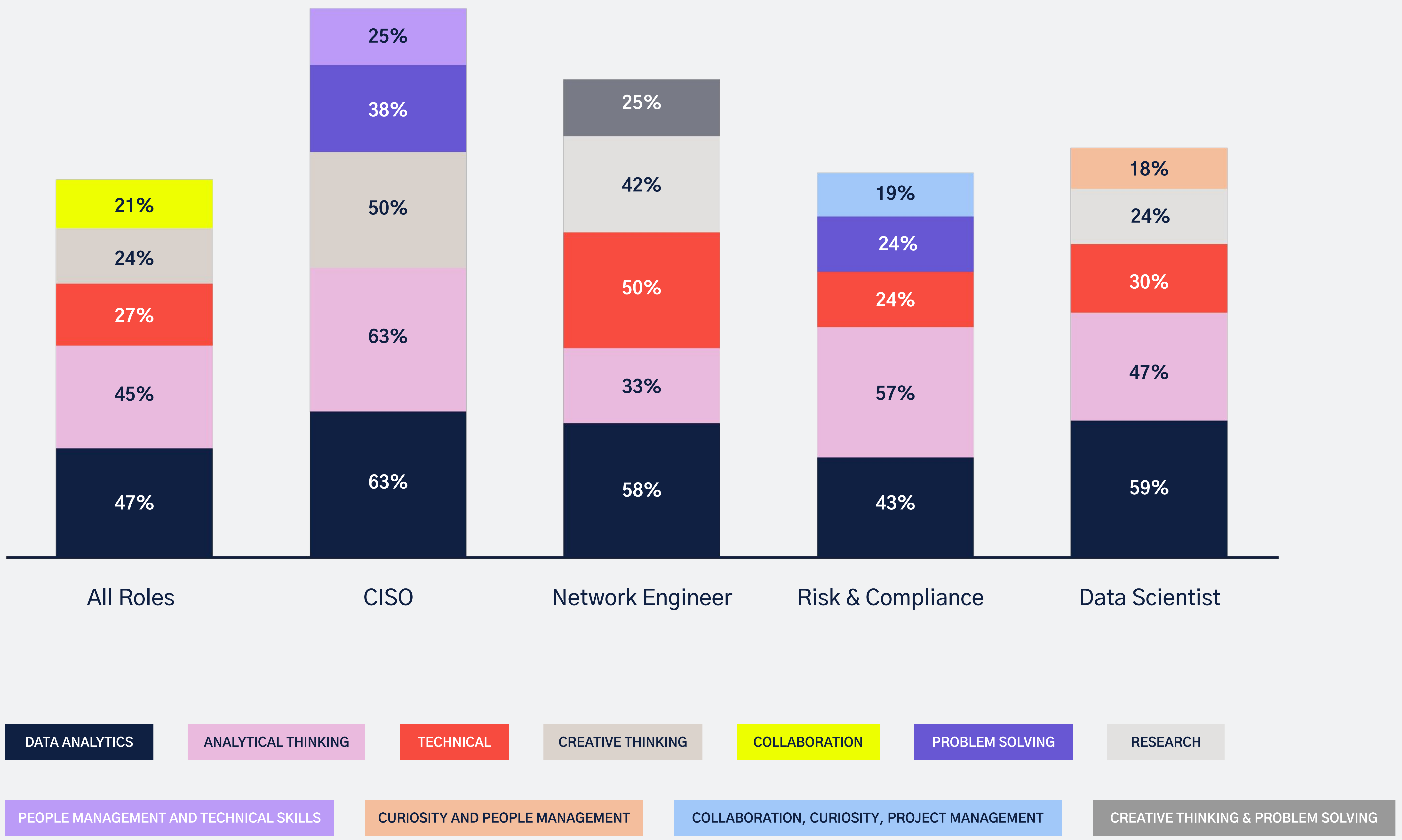
While preconceived notions about qualifications and culture mean that cybersecurity is often considered an unattractive or unobtainable option, cybersecurity professionals are steadfast that the industry isn't just for "tech people".

Creativity and collaboration rank in the top five skills needed to thrive in cybersecurity, alongside data analytics, analytical thinking, and technical skills. Of course, the skills needed vary depending on the role, and CISOs answered differently to Data Scientists, who answered differently to Incident Responders.

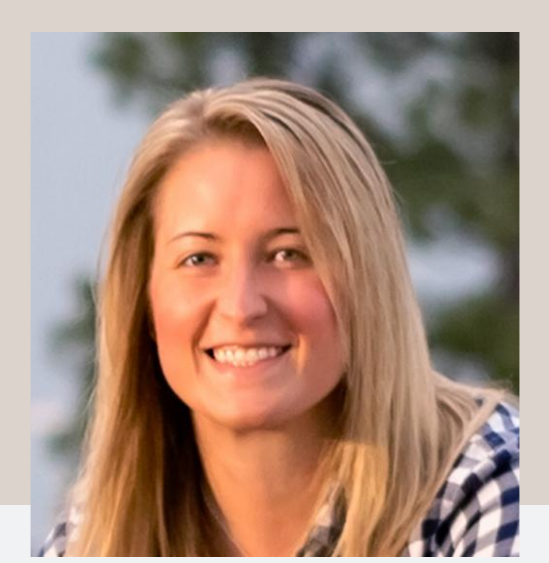
Communicating the range of skills needed to thrive is paramount for successfully recruiting women, with 43% of our survey respondents saying a lack of industry awareness is causing the cybersecurity skills gap.

This came second to a lack of qualified talent, meaning even those who are qualified may be discouraged from applying for jobs in the field.

What do you think are the most important skills to thrive in your role?



> “People hear “cybersecurity” and think of **hackers in hoodies.** That’s a bit of a caricature, maybe with some legitimacy to it—and that was even part of my own experience—but **that’s not all there is.**”



StackRox

Hillary Benson

Director, Product at StackRox

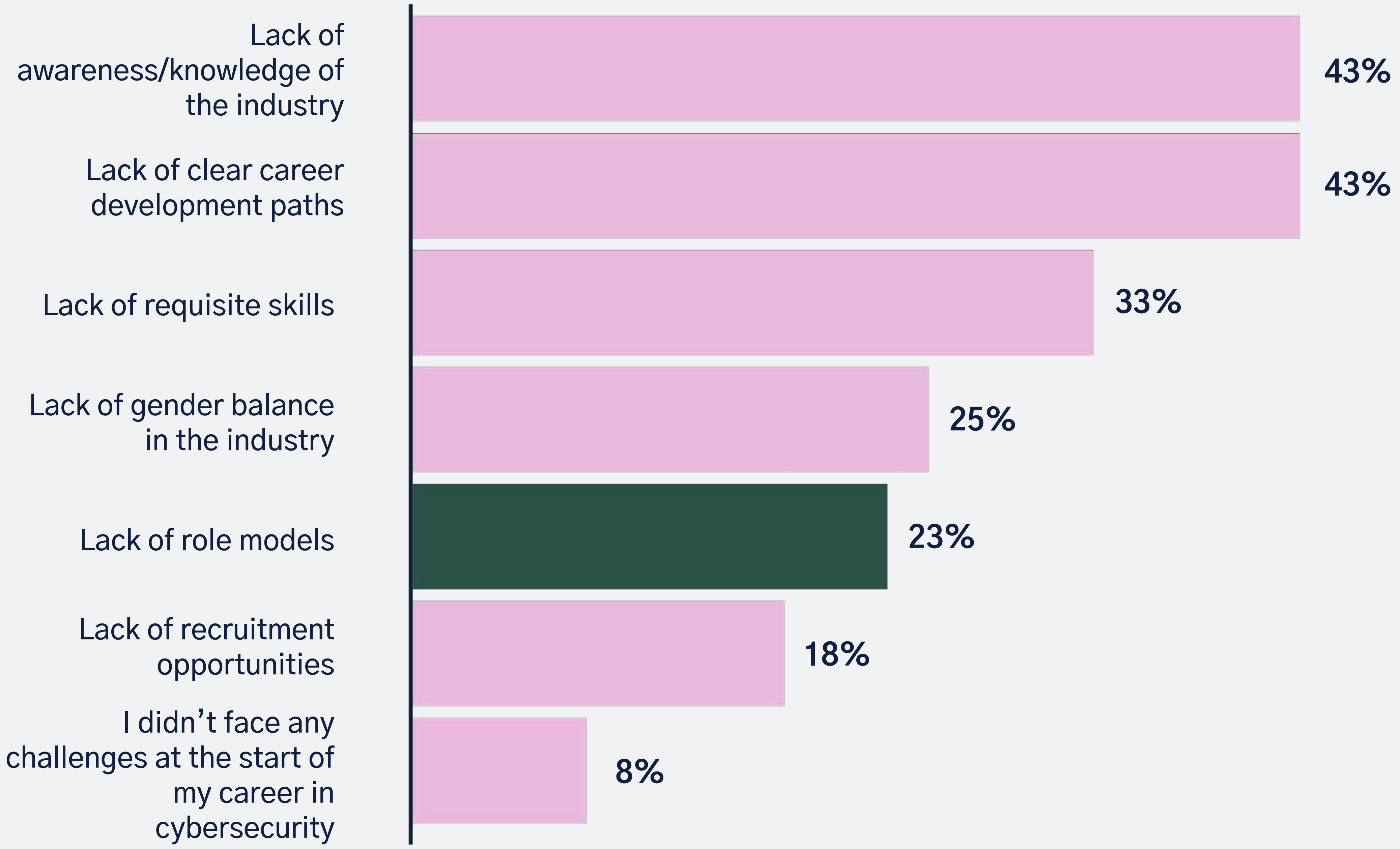
IMPORTANCE OF ROLE MODELS

Women inspire other women

While a greater emphasis on STEM in early education, more cybersecurity-specific curriculums at the university level, and more apprenticeship opportunities would help individuals develop relevant experience and raise awareness about the industry, visible role models who demonstrate the diversity of requisite skills are also sorely missed.

23% of our survey respondents said that a lack of role models was a challenge they faced at the start of their career and a further 26% said that more diverse role models would encourage more women into cybersecurity roles.

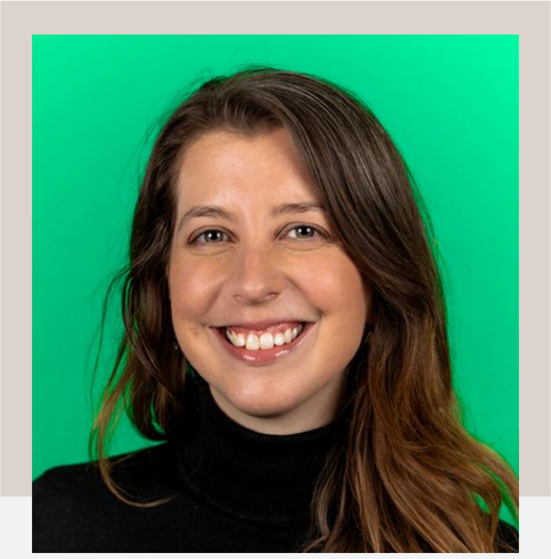
What challenges did you face at the start of your career in cybersecurity?



"I think mentorship is especially important for minorities – not just women – because we have to overcome different challenges. And those challenges aren't necessarily big hurdles. For some people, it can be several small things.

It could be a professor you have or a bad internship. One bad manager or experience isn't representative of the whole industry, but it can be demotivating if you don't know that there are more positive environments where these things don't happen.

That means those of us already in the industry have to fight the fight!"

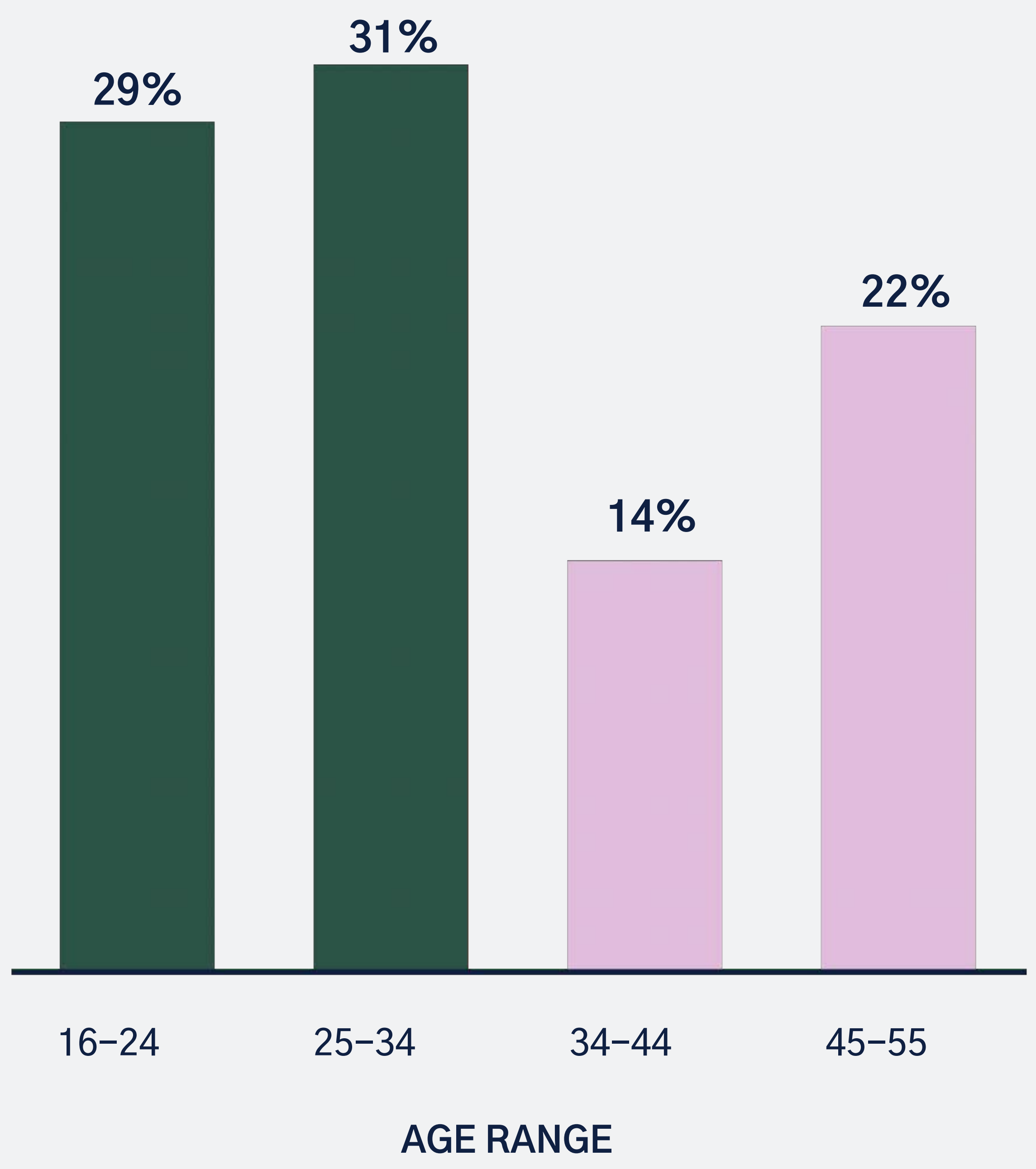


TESSIAN

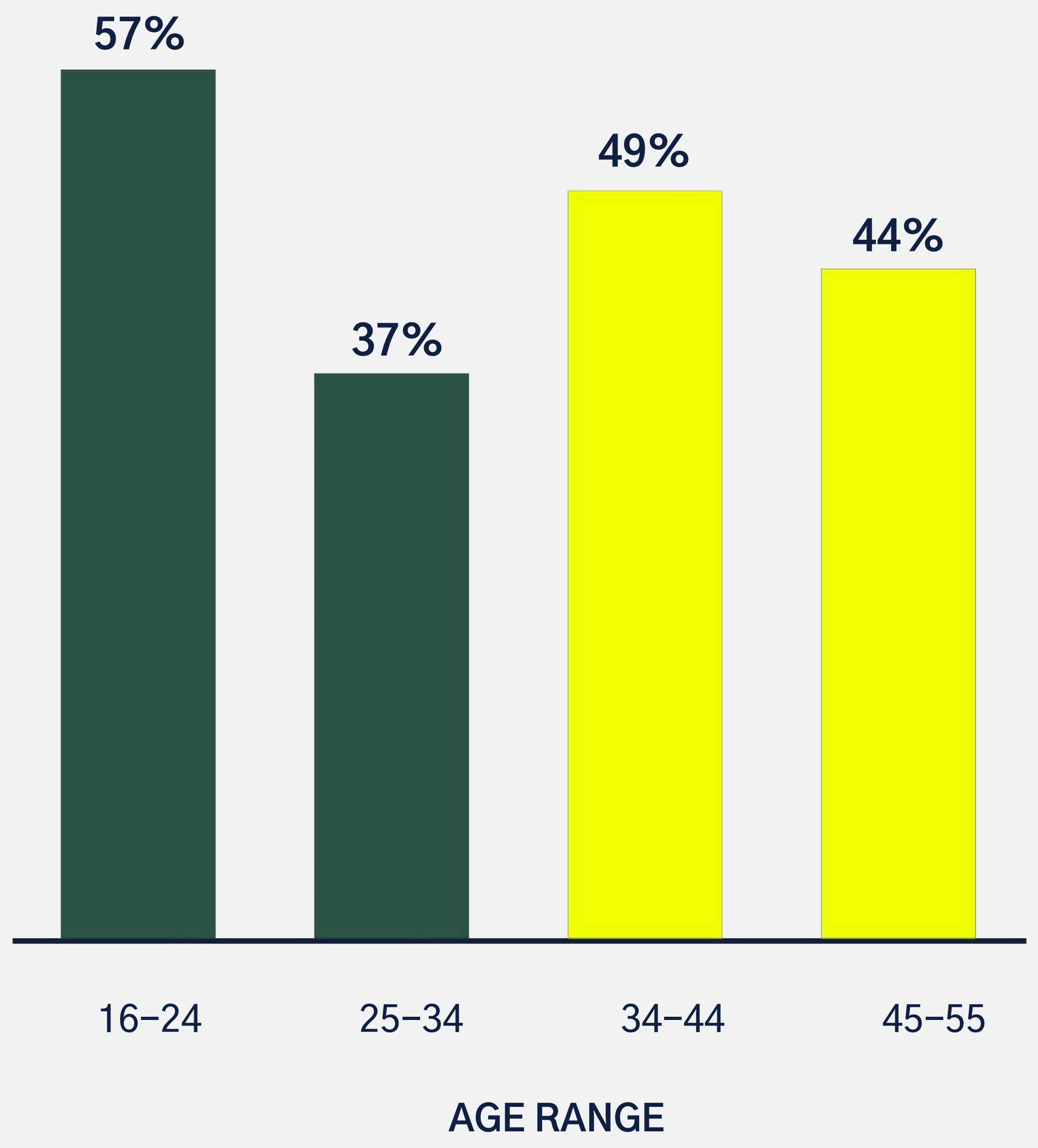
Gisela Rossi

Software Engineer at Tessian

Percent of women in cybersecurity who say that a lack of role models is a challenge they've faced



Percent of women in cybersecurity who say that a lack of career paths is a challenge they've faced

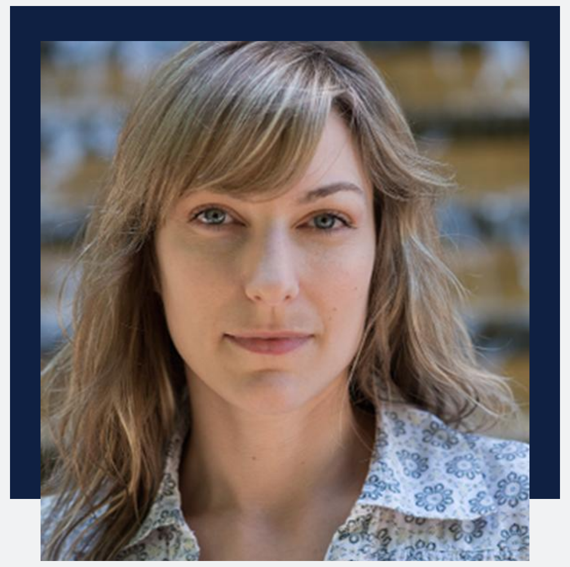


These feelings were more commonly shared amongst younger cybersecurity professionals, with 29% of 16–24 year olds and 31% of 25–34 year olds citing a lack of role models as a challenge they've encountered.

A lack of clear career development paths – potentially perpetuated by a lack of role models – was another challenge women faced at the start of their cybersecurity careers, ranking higher than a lack of requisite skills. Again, younger generations struggle with this even more, with 57% of our youngest respondents agreeing that career development paths aren't clear, and that it's something they had to overcome.

Women working in leadership positions are attuned to the problem, though, as every CISO and manager we interviewed said mentoring is a top priority for them. At the end of this report, you'll find an extensive list of cybersecurity–specific groups, mentoring opportunities, and other resources that promote female empowerment, all of which have been recommended by women currently working in the industry.

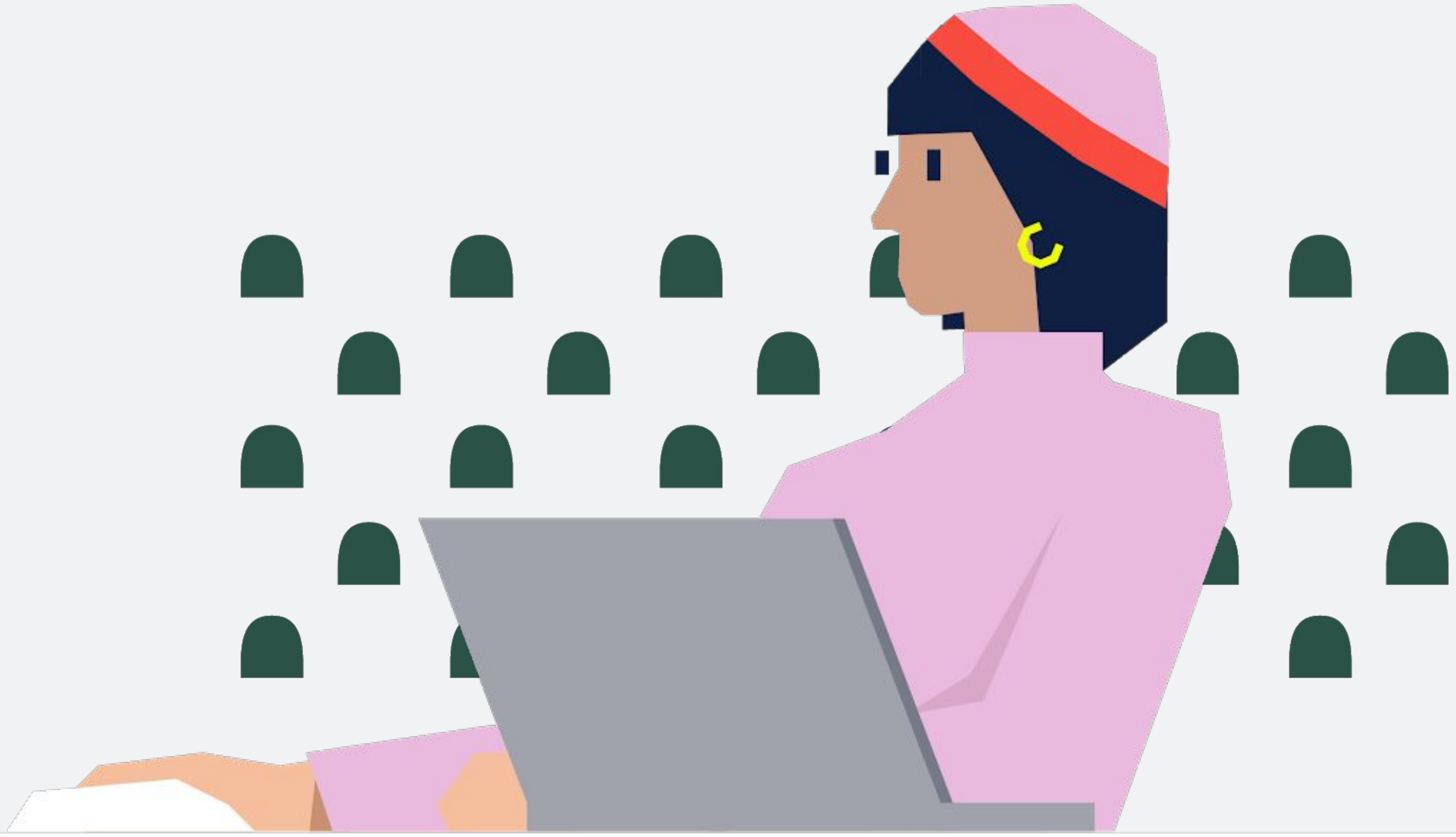
> “Most men I work with that are at a certain level credit their success to a mentor. I feel like I’d be years ahead if I’d had one. That’s why I say ‘yes’ every time there’s a Women in Cybersecurity function, a mentorship program, a local event, anything. **I always say yes.**
>
> You don’t have to be an activist to get involved and help someone.”



iovation

Amber Pham

Information Security Officer at iovation



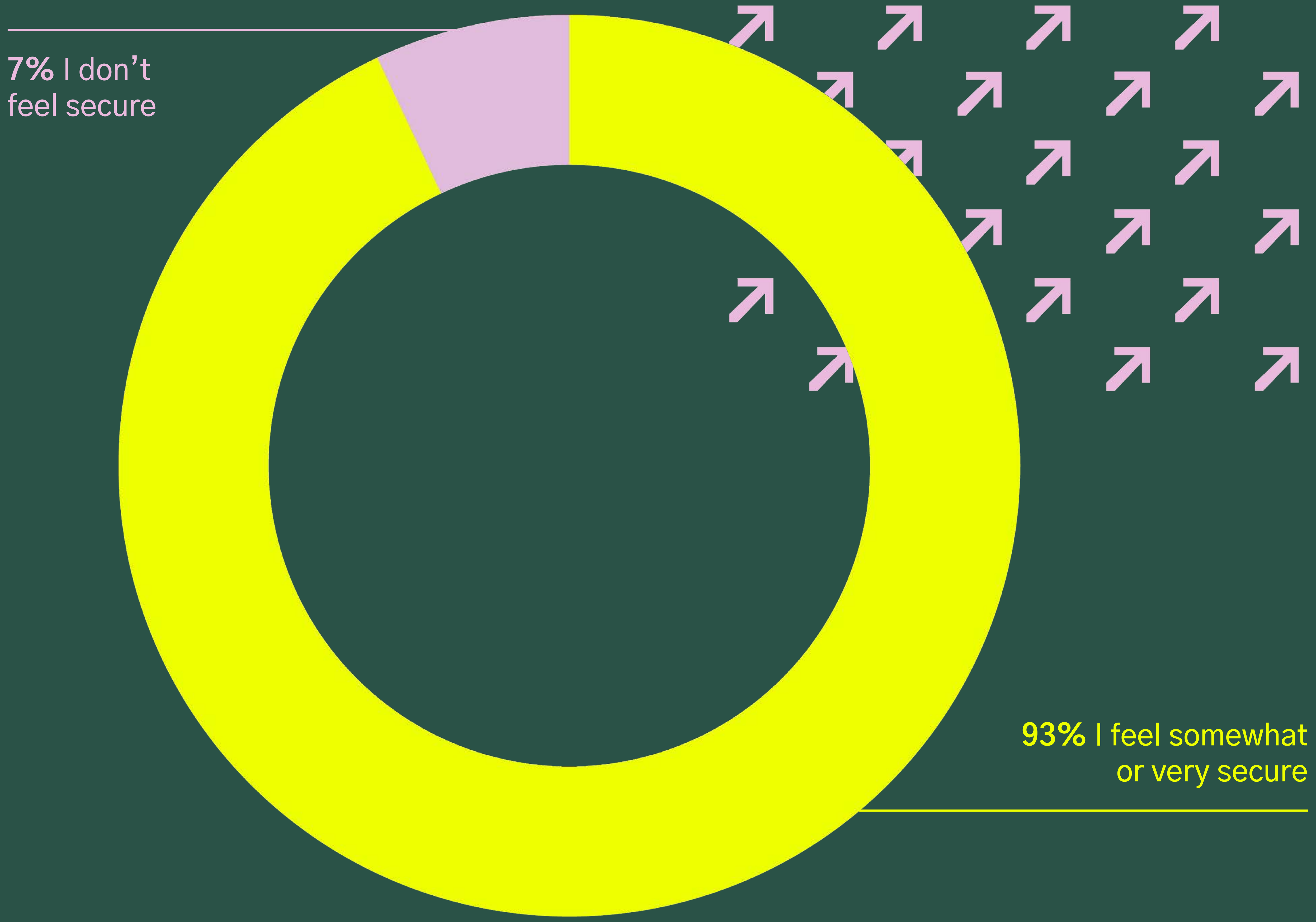
INDUSTRY OUTLOOK

Cybersecurity is future-proof

Despite the challenges women working in cybersecurity have faced, the women we surveyed feel overwhelmingly stable in their jobs, with 93% saying they feel secure or very secure working in this industry.

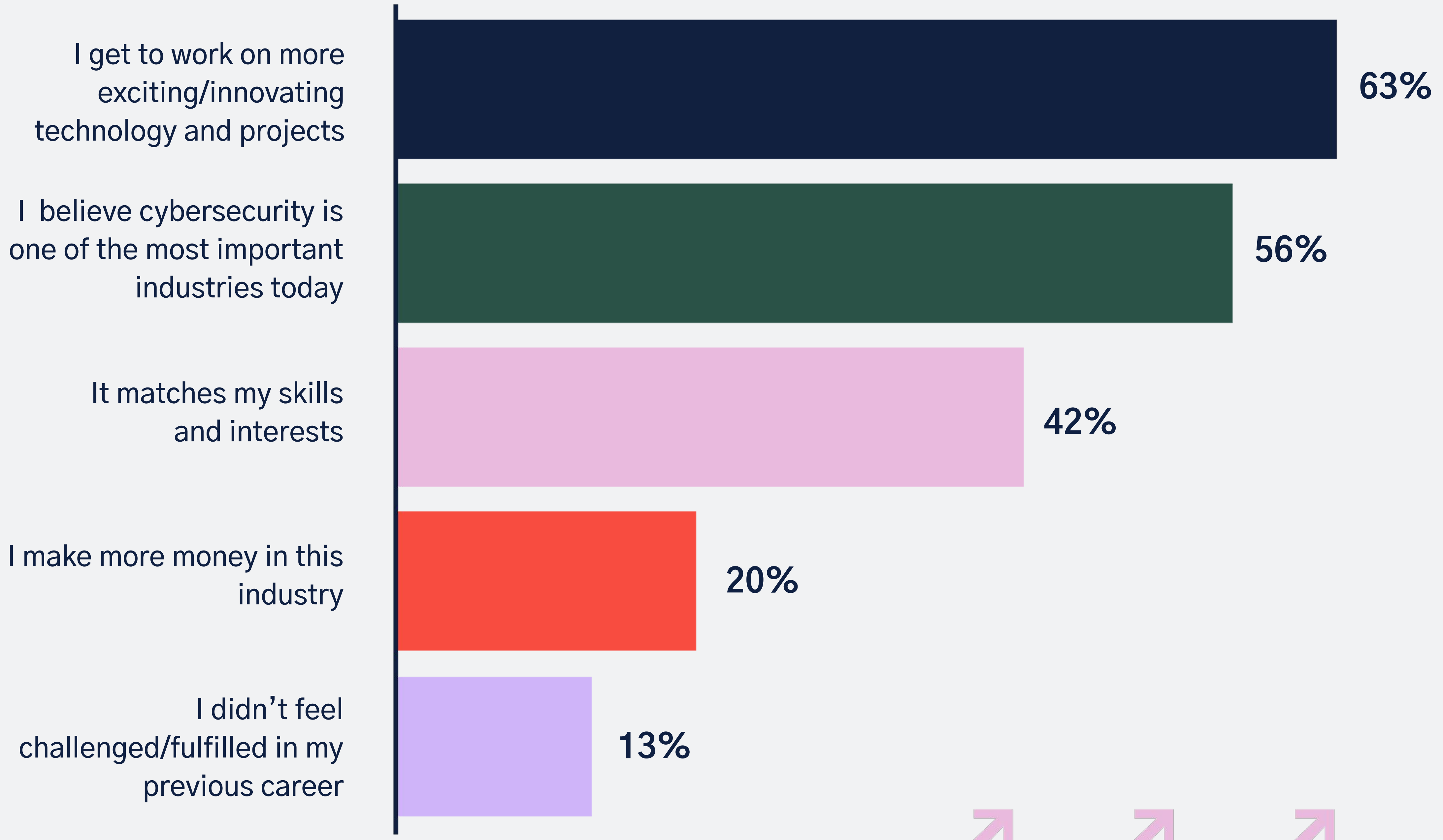
And, when you consider that the global cybersecurity market has grown 30x in the last 13 years[2] and that the industry received record venture capital investment in 2019[3], it's easy to see why perceived job security is high.

How secure do you feel in your job?



[2] Prime Indexes Cybersecurity Industry Overview
[3] Pitchbook & NVCA Venture Monitor Q4 2019

Why did you join the cybersecurity industry?



So, what makes cybersecurity so future–proof? The industry and the people in it are solving real–world problems and are making a positive impact doing so. In fact, over half (56%) of those surveyed said they joined because they believe cybersecurity is one of the most important industries today.

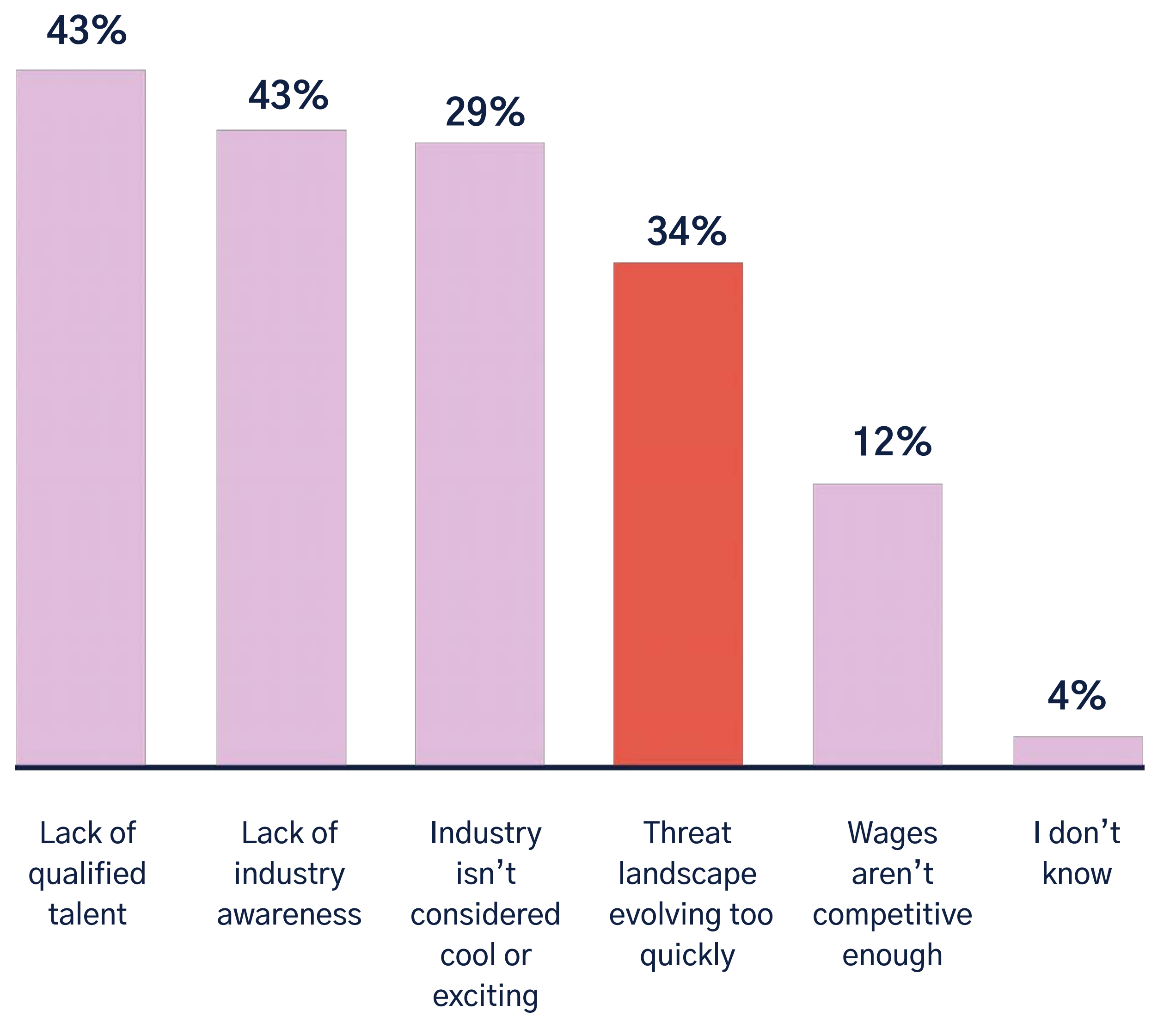
After all, data has become valuable currency and ransomware attacks, phishing scams, and network breaches are costing businesses and governments billions every year. The bottom line is, the field is constantly growing and evolving because cybersecurity professionals have to keep pace with – and stay ahead of – bad actors and new threats in order to protect businesses, people, and data.

> “The 2016 presidential election piqued my interest in cybersecurity. I remember learning about Russian interference, bots, and the manipulation of social media after Trump was elected and recognizing that cybersecurity is bigger than people realize.”

KIVU

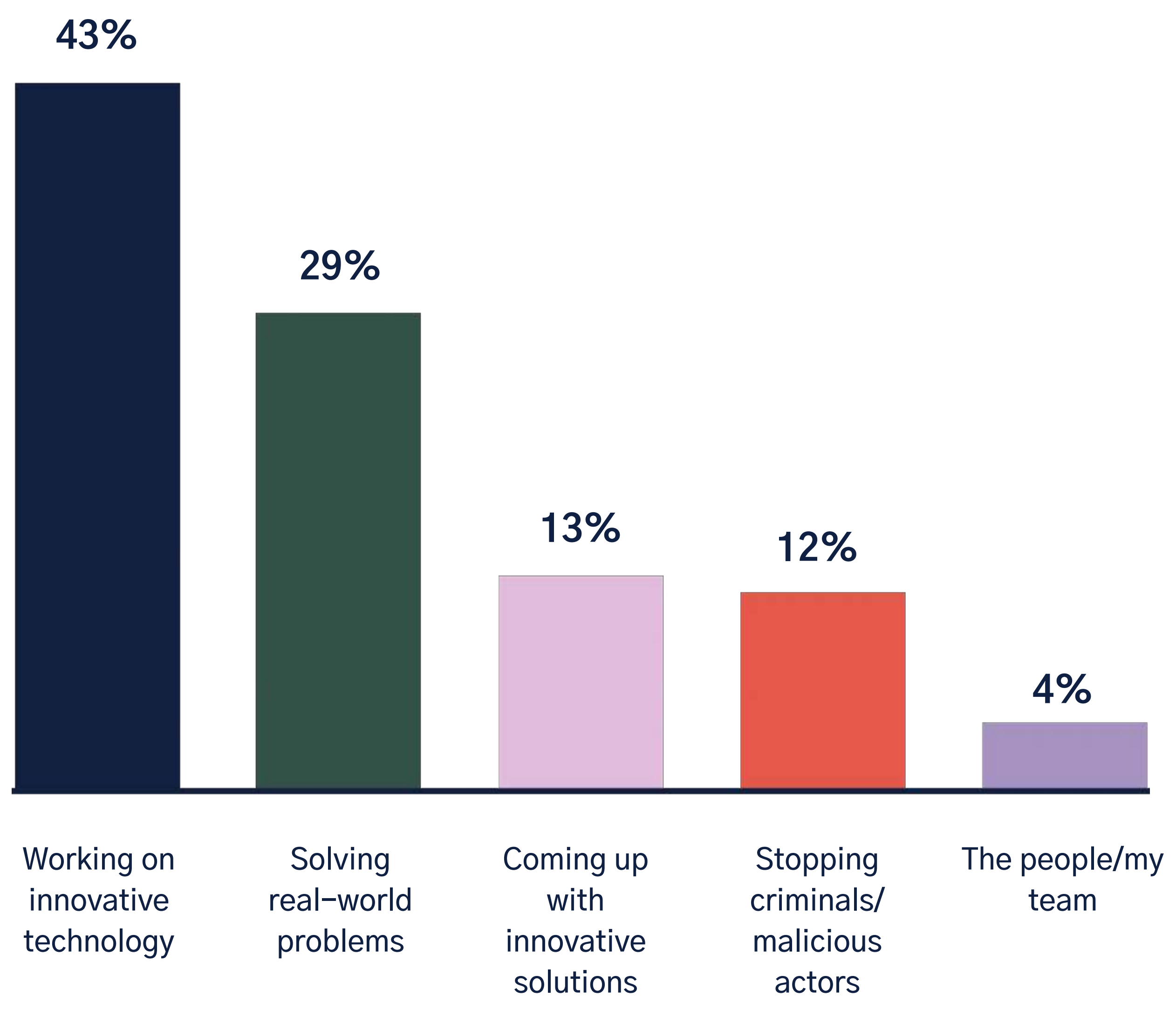
Tess Frieswick
Client Success Manager at Kivu Consulting

By 2021, it is predicted that 4M cybersecurity jobs will be unfilled. Why do you think this is?



According to women working in cybersecurity, this is actually contributing to the skills gap, with a third of survey respondents (34%) saying that there is a skills gap in the industry because the threat landscape is evolving too quickly.

What is the best part about working in cybersecurity?



But, the fast pace is something cybersecurity professionals are equally passionate about, with nearly half of those surveyed (43%) saying that the best part about cybersecurity is working on innovative technology and projects.

"The technical landscape we need to secure is rapidly evolving, even faster than our ability to deprecate the old, yet–to–be–entirely–secured stuff. Threat actors, who often have time and resources on their side, are also quick to adapt to existing defences. **This means we constantly have to learn new things.**

It's challenging; you're dealing with ambiguous problems, imperfect solutions, limited data, and real threats to human safety."

Google

Parisa Tabriz

Senior Director of Engineering at Google

"Working in a start-up that's **trying to solve really interesting real-world problems is the best part** for me.

The challenges around securing sensitive data are immense, but that's where the most interesting challenges lie."

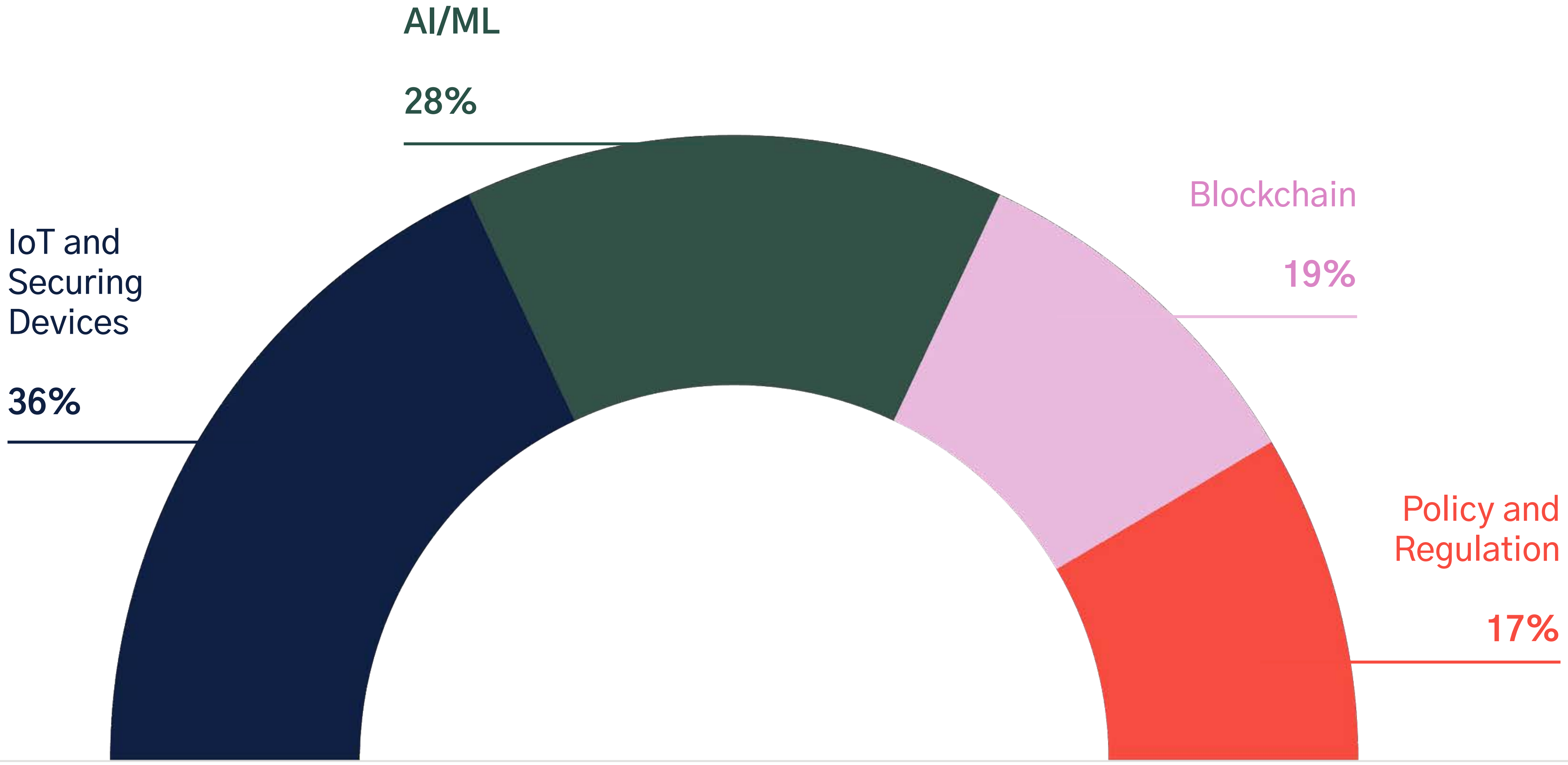
TESSIAN

Niki Tailor

Platform Engineer at Tessian

Women in the field count the Internet of Things (IoT) and securing devices, and Artificial Intelligence (AI) and Machine Learning (ML) as the most important developments in cybersecurity. Many of the women we interviewed, including those women from Tessian, are working on projects that involve both.

What do you see as the most important development in cybersecurity?



Conclusion

Today, people have access to more business-critical and sensitive data than ever before. But, people can make mistakes, break rules, and easily be hacked by astuate attackers, all of which put data at risk.

This industry plays a key role in keeping people and information safe, and the solutions that cybersecurity professionals build, implement, and monitor help protect consumers' privacy and business' most important assets.

Importantly, though, the industry needs diversity if we are going to defend against the ever-evolving threat landscape. We need different ideas and different approaches to problem-solving. And we don't just mean gender diversity.

The field is wide open for a range of educational and professional backgrounds, from psychology majors to business analysts and just about everything in between.

Creativity and collaboration are as important as technical acumen and, today, there is no "stereotypical" cybersecurity professional. Don't believe us? Read the profiles of each of our contributors on our blog.

By creating environments in which women can thrive, correcting false perceptions of the industry, and making career paths clearer, we can better promote all the opportunities in cybersecurity and encourage greater innovation in the industry.

There's over four million jobs available and billions that could be added to US and UK economies. **Challenge perceptions, make an impact.**

Tim Sadler
Chief Executive Officer, Tessian

Methodology

Tessian commissioned Opinion Matters to survey 200 female cybersecurity professionals (100 in the UK and 100 in the US) to understand the challenges and opportunities they experienced in the industry. Survey respondents hold various positions including CISO, network engineer, security architect, incident response, penetration tester, security analyst, software developer, data scientist, risk & compliance, and security operations.

We also commissioned the Centre for Economics and Business Research (CEBR) to quantify the potential economic impact if the number of women working in cyber were to equal the number of men. Finally, we interviewed over a dozen cybersecurity professionals with diverse backgrounds, which provided invaluable context for this report.

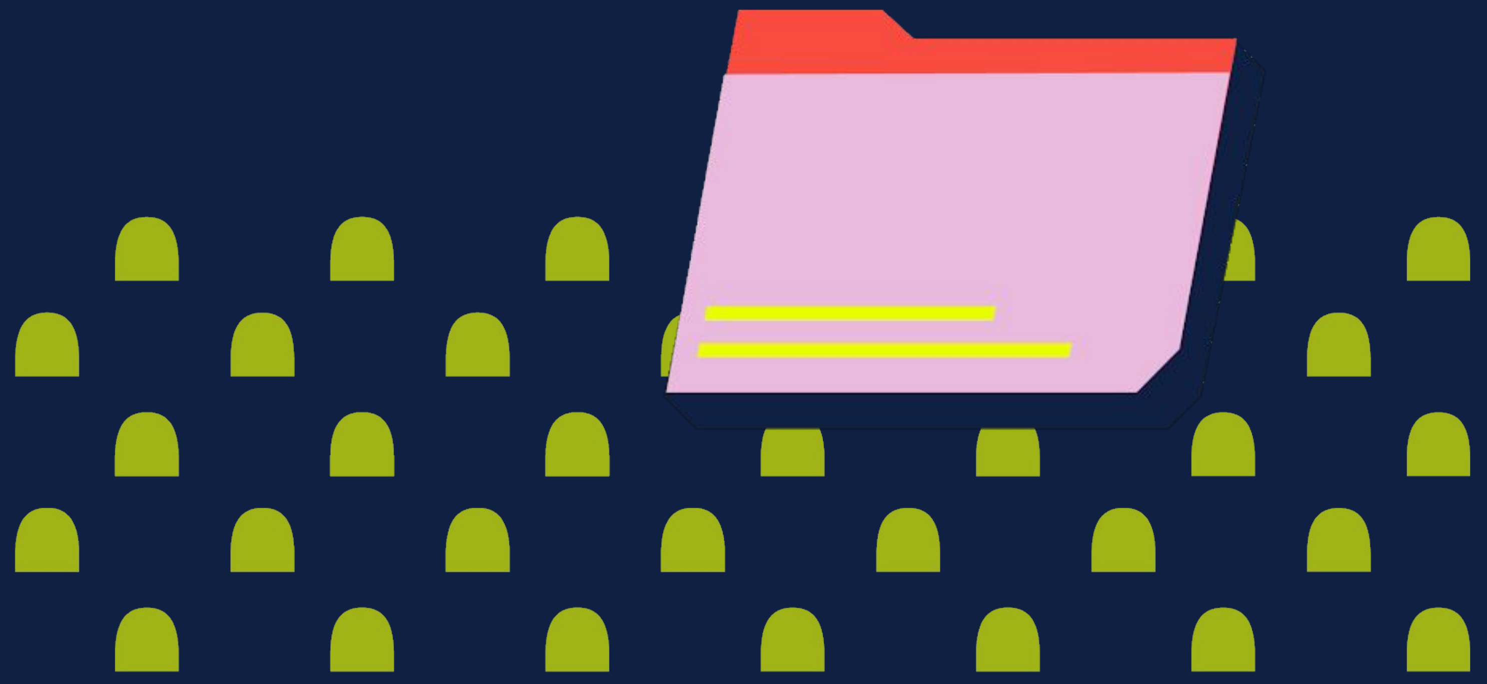
Publically available third-party research was also used, including:

1 (ISC)2 Cybersecurity Workforce Study, 2019

2 Prime Indexes Cybersecurity Industry Overview

3 Pitchbook & NVCA Venture Monitor Q4 2019

Percentages may not always add up to 100% due to rounding.



Resources

The following resources have all been recommended by the women who contributed to this report. This list includes certifications that will help you demonstrate your expertise, cybersecurity-specific groups, and organizations focused on female empowerment. Some are regional while others are global and whenever possible, we've included relevant links to help direct you to the right page.

It's worth noting that many of the women cite their local chapters of these larger organizations as being the most inspiring and helpful, so we recommend that you dig a little deeper to find meet-ups and other events close to you.

Cybersecurity Groups

Bugcrowd

CoderDojo

CybHER

Girls Who Code

HackerOne

Information Systems Security Association (ISSA)

Information Systems Audit and Control Association (ISACA)

(ISC)2

Lean In

Meetup.com

PyLadies

Women in Science and Engineering (WISE)

Women in Technology International

Women in Cybersecurity (WiCys)

Women in Security and Privacy (WISP)

Women Who Code

Certifications

Certified Data Protection Officer (CDPO)

Certified Information Systems Auditor (CISA)

Certified Information Security Manager (CISM)

Certification in Information Security Management Principles (CISMP)

Certified Information Systems Security Professional (CISSP)

ISO 27001 Implementer

Offensive Security Certified Professional (OSCP)

#THE FUTURE IS CYBER