Chartered Institute of Information Security

State of the security profession

2023/24

Introduction

Our aim with the annual “State of the security profession” survey is to provide an overview of the industry. The report covers topics such as demographic changes, career prospects, skill gaps and how to fill them, and the impact of AI on both the industry and professionals. This provides readers with valuable insights into the current state of the profession and emerging trends.

Introduction

It's always a pleasure to work on the CIISec "State of the security profession" survey. For those that have been in the industry for some time; those who like statistics; and those who have been at the coal face of defending networks as well as thinking through the strategic impacts and costs of risks, there is much to value in the collective views of their industry. Particularly in a profession that has had to work so hard to keep pace with both the development of technology and the threats that we all face.

This is our ninth annual report. In that time, the survey has covered emerging issues such as the effects of Covid, the rise of ransomware and the economic challenges many countries face. The rapid emergence of artificial intelligence (AI) has changed the business landscape and is presenting significant challenges to the cybersecurity industry. Naturally, it's the theme we chose for the survey and report.

While that technology has come to prominence, society has of course still been battling economic headwinds and dealing with ransomware attacks. As always, we have already seen many changes since the last report.

As high inflation and high interest rates appear to be abating, and post-pandemic supply chain disruptions have eased, we may see some of the aspects that affect our profession stabilise. However, the new UK Government, a presidential election in the US and increasing regulation on certain sectors may yet have an effect on how cybersecurity professionals focus their efforts.

I always hope that this report is interesting to read and useful in making decisions. One successful business case that utilises a single statistic would make it worth the effort.

If you read it and find it of value, please share it and make a point to respond to future calls for responses.

Piers Wilson
Director, CIISec

Contents

Key findings

Each year the results of the survey are interesting, both in the responses to questions, and the trends and themes we pull out as being particularly topical or challenging.

Key findings

AI in cybersecurity

- 51% of professionals believe AI and machine learning will be the most influential technology over the coming year.
- There will be winners and losers. Professionals believe unskilled workers (76%) and older people (61%) will suffer negative impacts, while industry (84%) and, most worryingly, cyber attackers (98%) will thrive.
- There is inevitably a need to react to this emerging technology. But 44% of professionals don't feel their organisation is aware of the impact of AI or has policies in place to address it.

Skills and recruitment

- Worryingly, the highest ever proportion of professionals (14%) say the industry is doing worse at defending systems from attack, protecting data, and dealing with incidents.
- Adequate and relevant training provision remains an important aspect of attracting and retaining staff – cited as a top 5 reason for why professionals take or leave a job. Retaining staff is important because recruitment is both expensive, and risky.
- 46% of professionals believe that the industry needs experienced, skilled personnel to address the skill shortage.

Challenges and threats

- 21% of professionals are still classed as over-worked.
- Long hours are likely to be adding to the stress of the job, which is still the main issue keeping professionals awake – closely followed by the risk of suffering an attack.
- Poorly handled attacks can become notorious. Professionals are almost twice as likely to remember and name a poorly handled attack than a well-handled one.

Careers and the security market

- Cybersecurity is an attractive career. Compared to 2015, mean pay has risen by more than £25,000 - or 7% above inflation.
- Pessimism about the security market is higher than ever before – 80% say budgets aren't meeting threat levels, and a record 19% believe the industry is stagnating.
- At an individual level the picture is still good – 75% say they have good or excellent career prospects.

Demographics

- Professionals are experienced - with a high level of education (79% to graduate degree or higher), and on average 18 years' experience.
- The profession is still overwhelmingly white (81%) and male (88%), potentially related to how long people have been in the industry.
- Industry sectors are becoming more diverse, with the highest ever percentage working outside the traditional heartlands of technology, government and finance.

51% of professionals believe AI and machine learning will be the most influential technology over the coming year.

PART ONE

The shape of the profession

As attracting new recruits and fresh perspectives into the profession should always be a priority, so understanding the profession's demographics is an essential element of this report.

This year, we again see that this is largely an older profession. Reported ages sit mostly within the 46-55 and 56-65 age brackets, and the mean age of 48 is trending closer to the historic mean than in previous years.

It's also notable there are fewer young professionals than in previous years, with only 15% being under 35 – compared to 22% last year. This suggests that the industry needs to do more to attract younger new recruits.

15% of respondents are under 35 – compared to 22% last year

Age of respondents

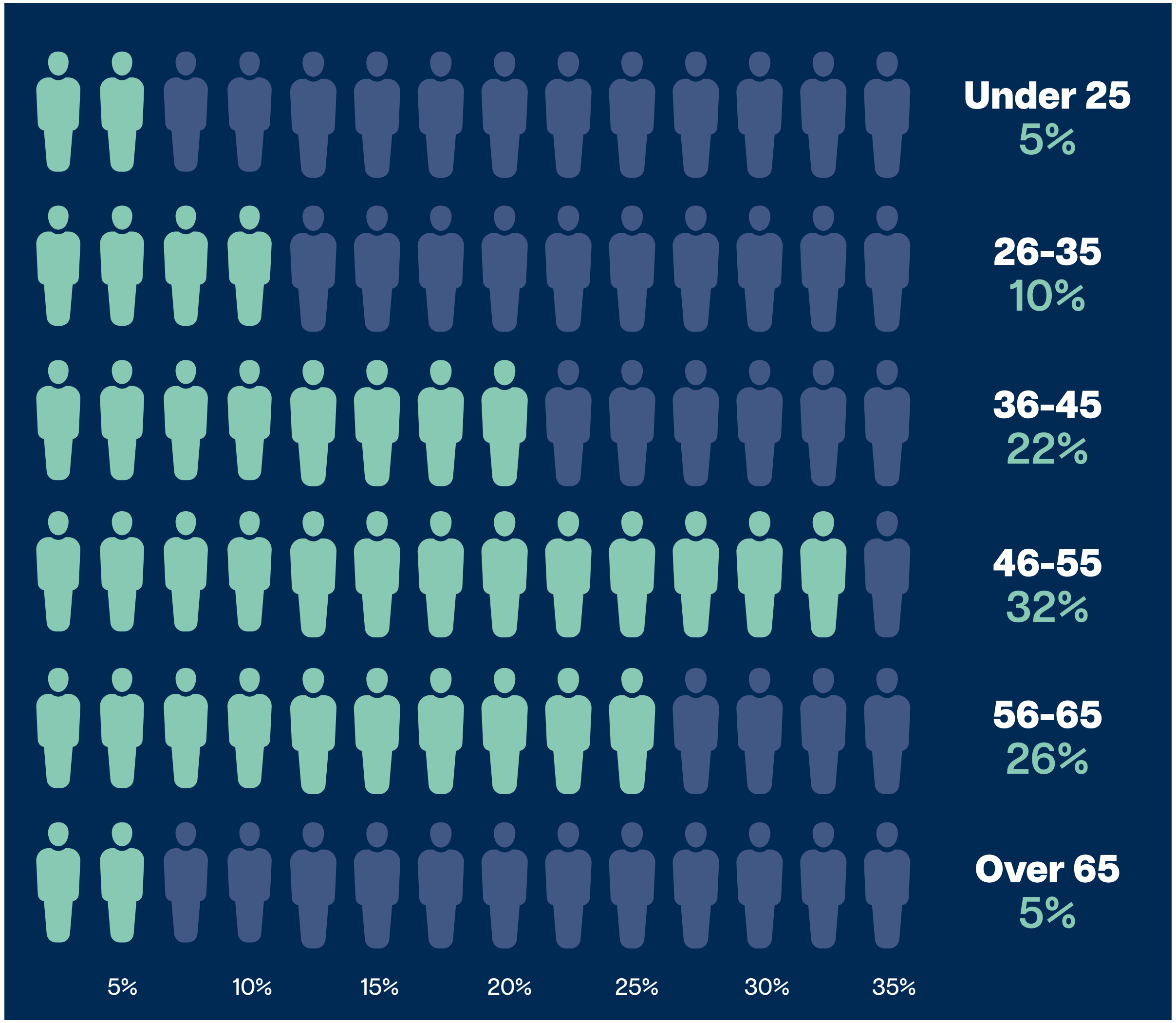


Figure 1 – Age group by band

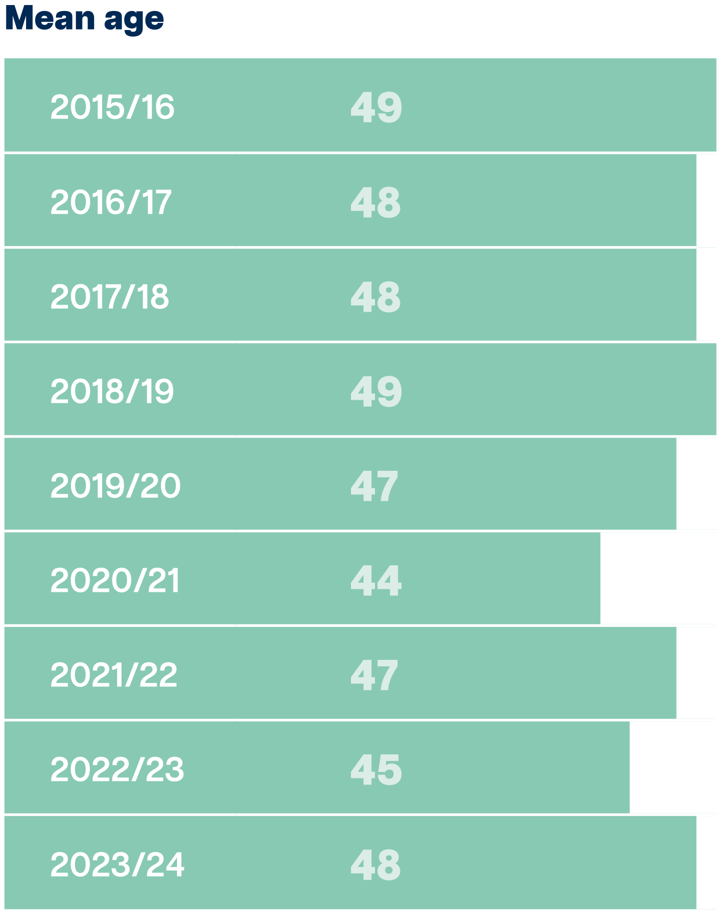


Figure 2 – Mean age year-on-year

Gender balance

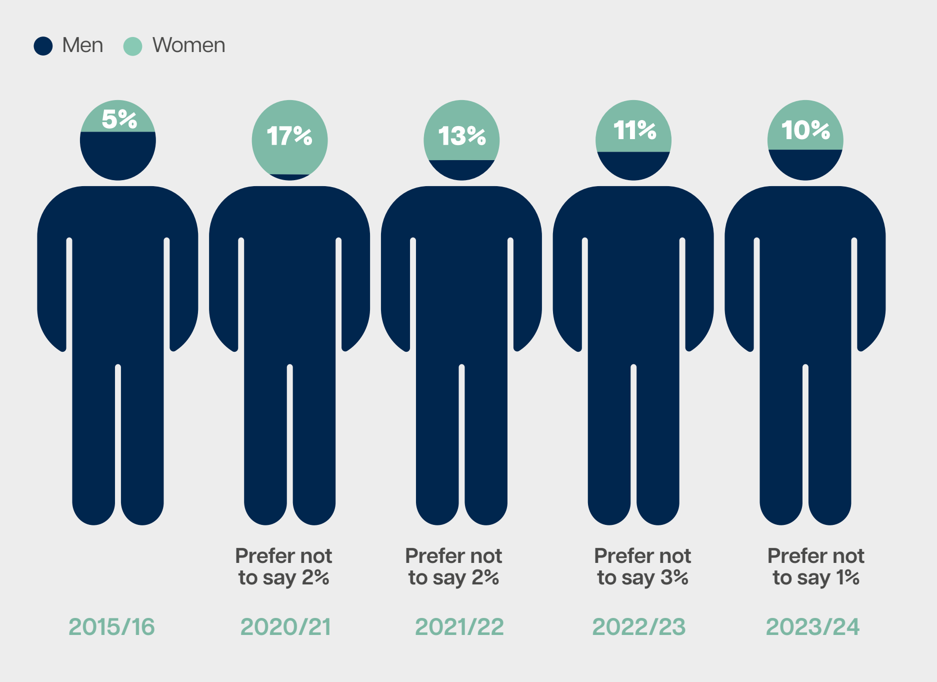


Figure 3 – Gender by year

Women are still better represented in the profession compared to our first survey in 2015/16. However, since 2020/21, there has once again been a downward trend in female representation.

This year, men outnumber women by nine-to-one. This suggests a trend and highlights continuing challenges in tipping the gender balance towards a more even industry.

Industry

	2015/16	2020/21	2021/22	2022/23	2023/24
Other	10%	8%	12%	14%	18%
Non-profit	-	2%	2%	2%	1%
Health & Pharma	2%	2%	3%	1%	3%
Utilities	4%	2%	3%	2%	3%
Education	6%	3%	6%	5%	5%
Aerospace	6%	5%	4%	4%	3%
Business support	7%	5%	6%	4%	3%
Finance	11%	32%	15%	19%	15%
Government	24%	17%	26%	23%	23%
Telecoms/ Technology	30%	26%	25%	27%	27%

Figure 4 – What sectors do professionals work in (%)

Cyber professionals are still largely employed in the telecommunications & technology, government and finance sectors.

However, the number of professionals working in “other” industries is growing year on year, almost doubling since we first asked this question in 2015/16. This suggests that cybersecurity is becoming more prominent in industries outside of the traditional sectors where it has always had more attention.

As a profession we should welcome this change. Government, IT services and finance do entail significant risks, but ransomware attacks in recent years have been reported across all sectors and so the value of cybersecurity in general has been rising.

Ethnicity

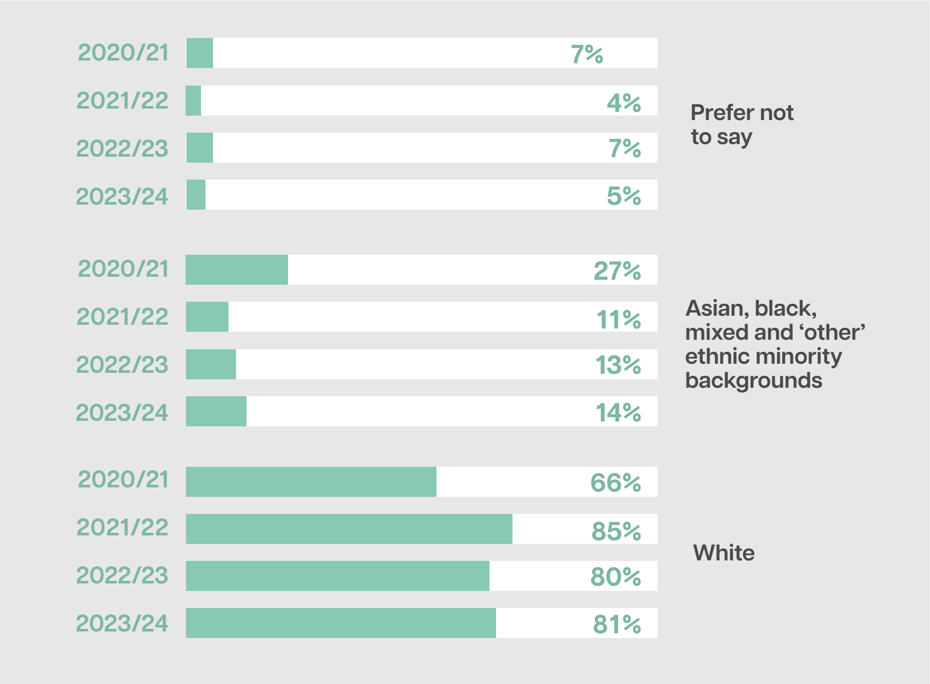


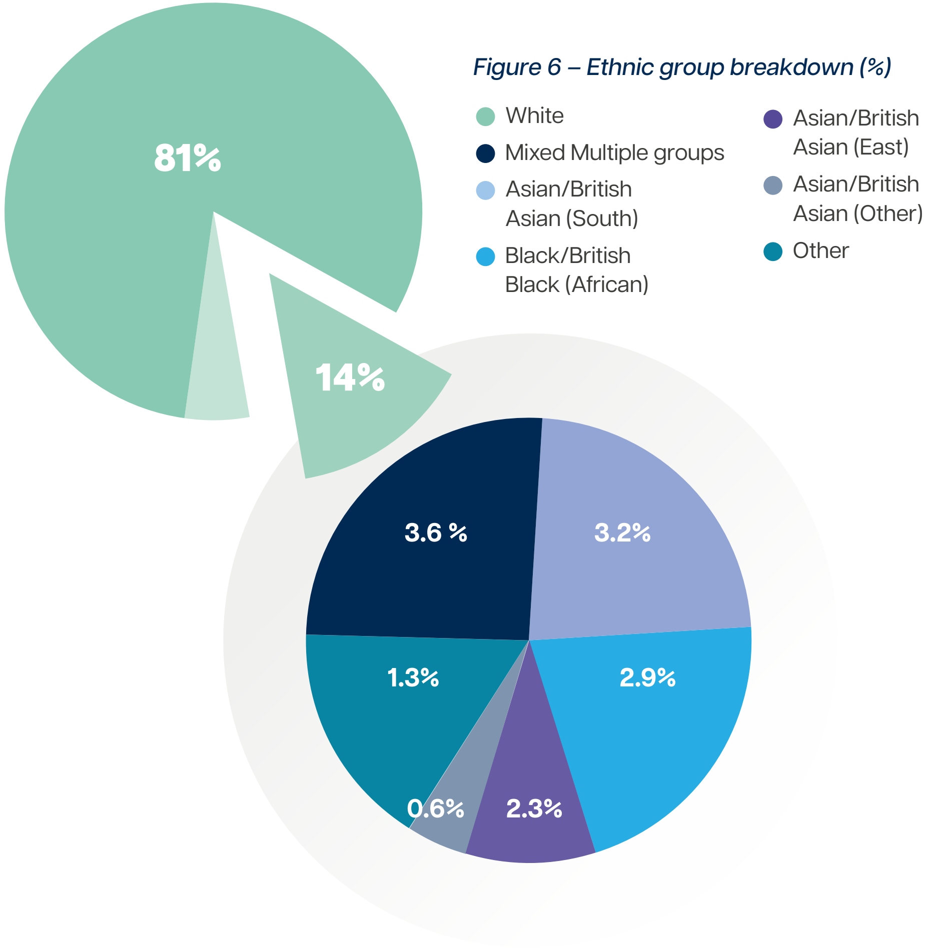
Figure 5 – Ethnic group (%)

Ethnic diversity in the security profession closely aligns with the 2021 national census, with 81% of professionals being white, compared to 82% in the census.

The demographics show a general move towards diversity in the last three years, but remain representative of the UK as a whole. This is a positive sign as the industry continues to push for a broader array of ethnicities entering the workforce.

Drawing in people from a variety of backgrounds with different perspectives is crucial to solving today's complex security challenges and overcoming ongoing skill shortages.

Figure 6 – Ethnic group breakdown (%)



Encouragingly, the industry continues to push for a broader array of ethnicities entering the workforce

PART TWO

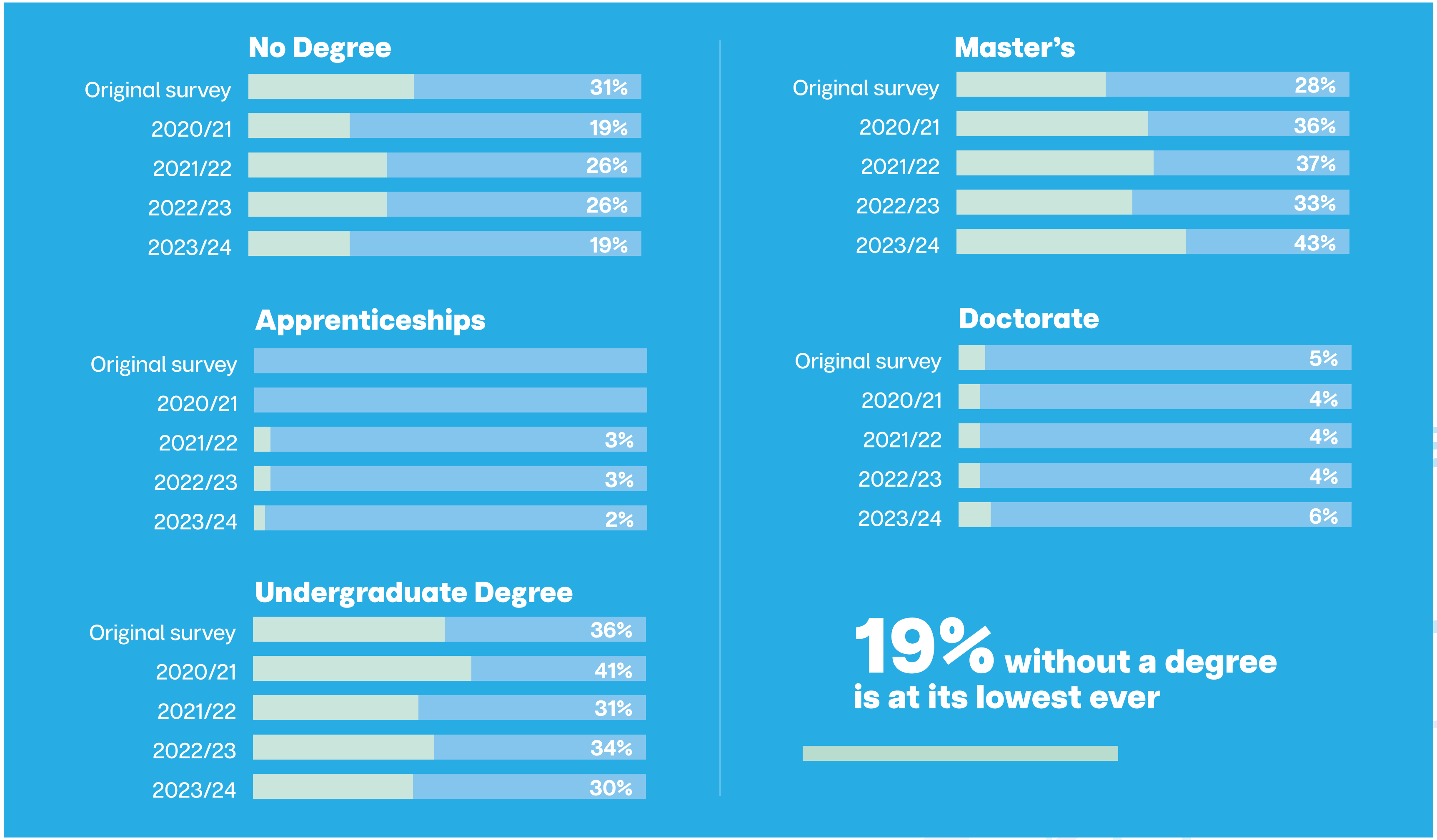
Education and careers

Education is often the stepping stone to a career, and cybersecurity is no different. More than three quarters (79%) of professionals have an undergraduate degree or above. The percentage without a degree is at its lowest ever (19%), a notable difference from the first survey in 2015/16.

The fact that almost half (49%) have attained a Master's or above – the highest proportion of respondents – also shows the opportunities for progression, as some of these will have been achieved after individuals started their careers. In the wake of past initiatives to launch accredited degree and Master's programmes it's good to see this investment appears to be paying off.

49% have attained a Master's or above - the highest proportion of respondents

The level of education of respondents



19% without a degree is at its lowest ever

Figure 7 – Educational background (%)

Career plans

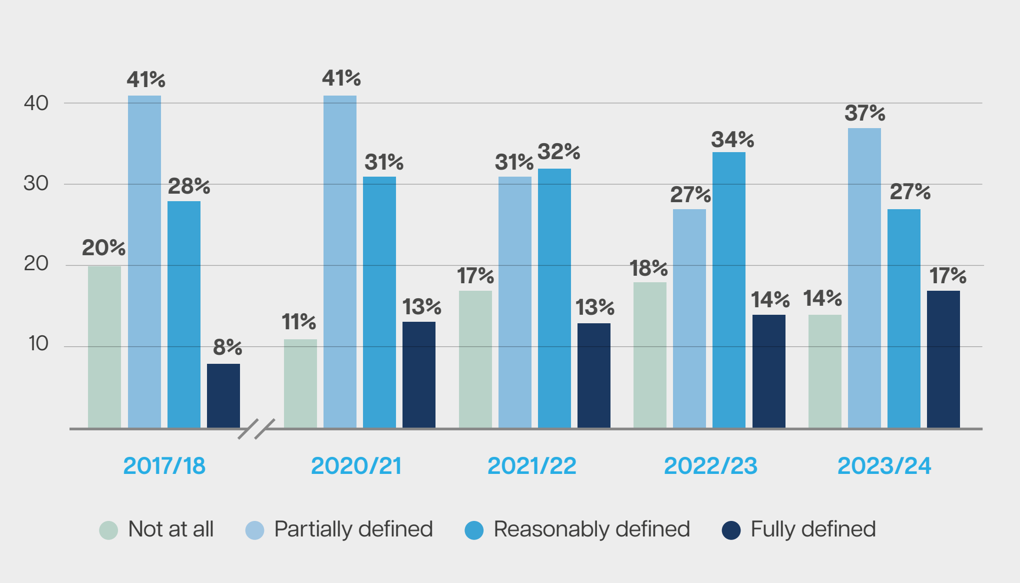


Figure 8 – Career plans of respondents

As well as past education, we also want to understand how defined professionals' future career plans are.

It is heartening to see the proportion of professionals with a fully defined career plan – with this year seeing the highest ever (17%). However, for others their career plans are less concrete, with more than half (51%) having only a partially defined career plan or no plan at all.

While the proportion of professionals with no plan is at its second lowest ever point, there is still the opportunity to support peoples' careers and help them plan better. Professional development and higher education, as we've seen, are two key ways to help professionals continue advancing in their careers.

17% of professionals this year have a fully defined career plan - the highest ever

Remuneration

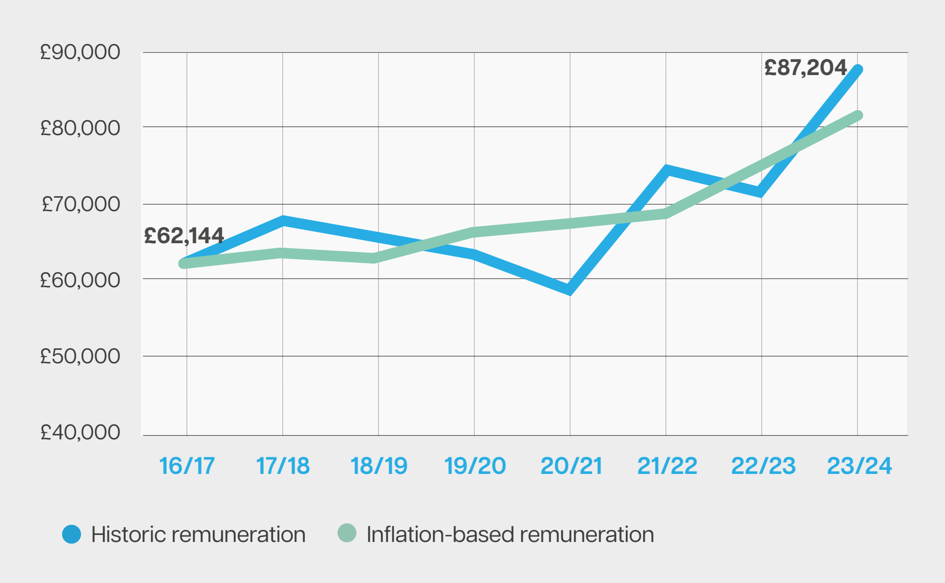


Figure 9 – Mean remuneration by year compared to inflation

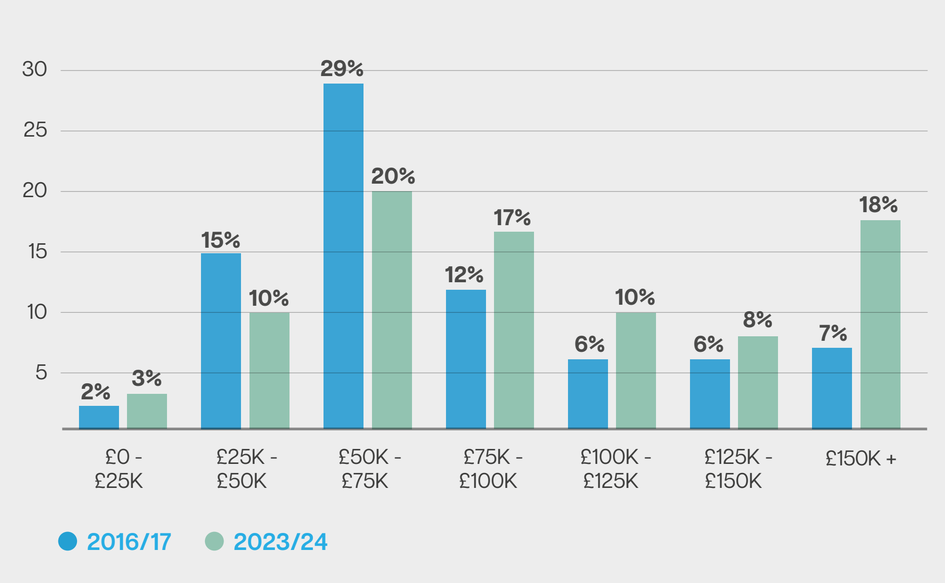


Figure 10 – 2023 remuneration by band

With the UK's average wage in 2024 sitting at £34,900, cybersecurity professionals are well compensated. On average, we can see a clear increase over the last seven years.

Comparing 2016/17 to 2023/24 using inflation rates from the Bank of England we can see that wages for cybersecurity professionals have risen beyond inflation.
The mean £62,144 wage in 2016/17 would have been worth £81,616 in 2023/24 – showing a 7% increase in real terms.

If we compare the actual increase of £25,000, the picture is even more stark – it is 29% higher than the £19,500 increase if remuneration had simply followed inflation..

This is further emphasised in the remuneration by band statistics, compared to 2016's figures. Almost a fifth (18%) of professionals this year earn more than £150,000, compared to just 7% in 2016, showing how wages are rising across the board. This is further emphasised by the mean wage – which this year is more than £25,000 higher than the 2016/17 level.

Time in the industry

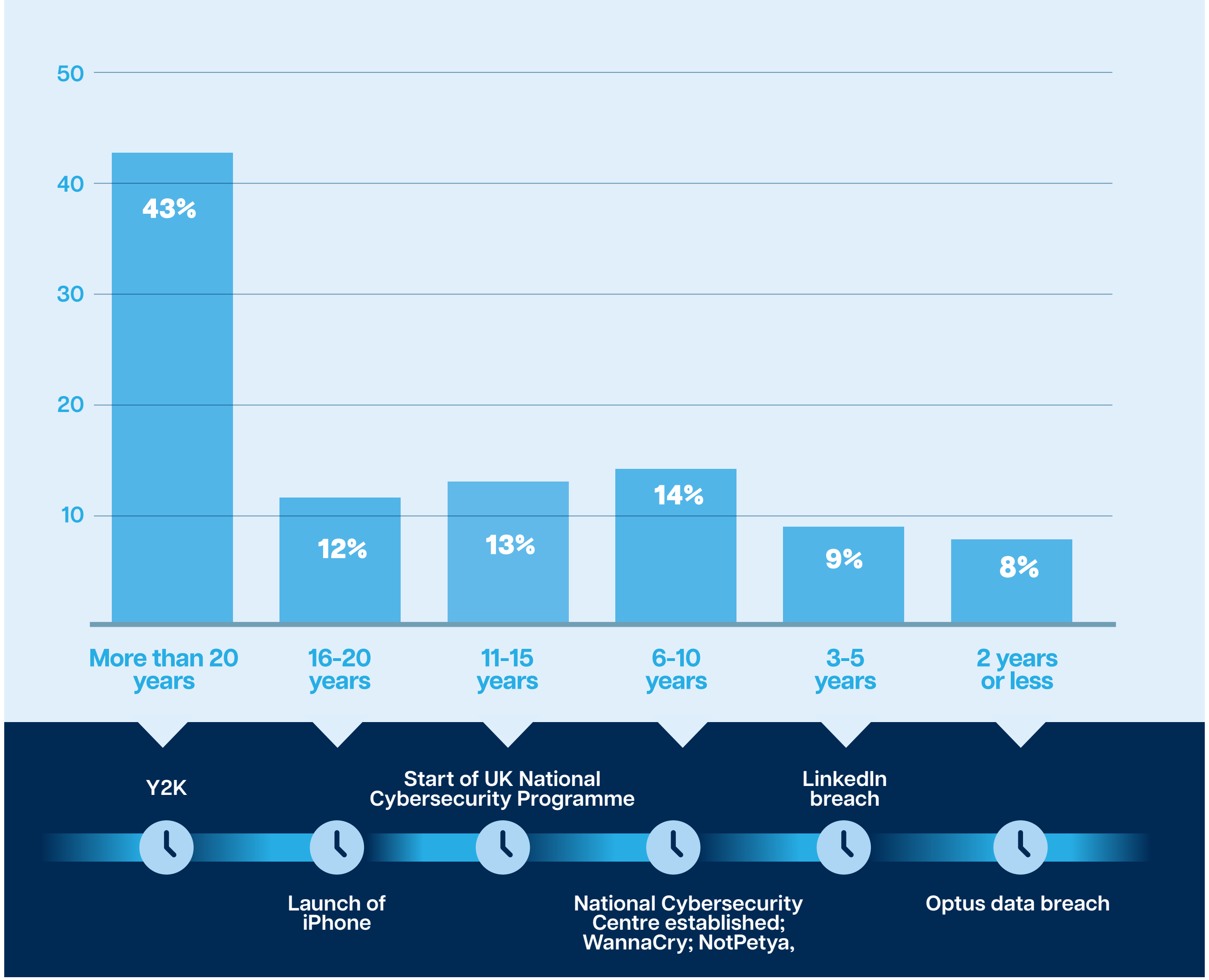


Figure 11 – Breakdown of the number of years 2023/24's respondents have spent in the cybersecurity industry

Following the demographic trend, professionals have spent on average 17.2 years working in cybersecurity. This shows the attractiveness of cybersecurity as a long-term career, with opportunities to grow, try new roles and develop new skills.

Almost half of professionals (43%) have been in the industry for more than 20 years, compared to just 17% who have been in the profession for less than five years. This shows that there is almost certainly space to attract new blood who will bring new perspectives to the industry.

43% have been in the industry for more than 20 years

Time spent in current roles

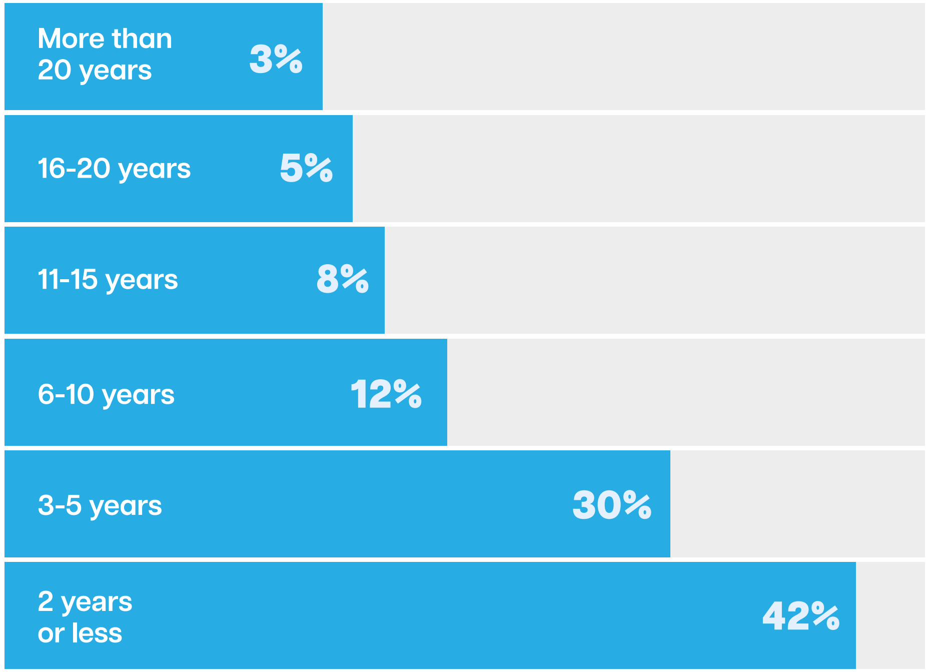


Figure 12 – Breakdown of number of years in current role

Just as professionals tend to stay in the industry for a long time, they tend to remain in their roles. While almost three-quarters (72%) of professionals have been in their current role for less than five years, on average they have been there for 4.8 years – remaining consistent with last year's 4.7 years, and broadly in line with the UK average.

When correlating against the time in the industry statistics (see Figure 11), this suggests that respondents have typically changed jobs 3-4 times throughout their careers – showing that there are opportunities to try new experiences, develop new skills, and keep progressing one's career.

Likelihood of remaining in current role

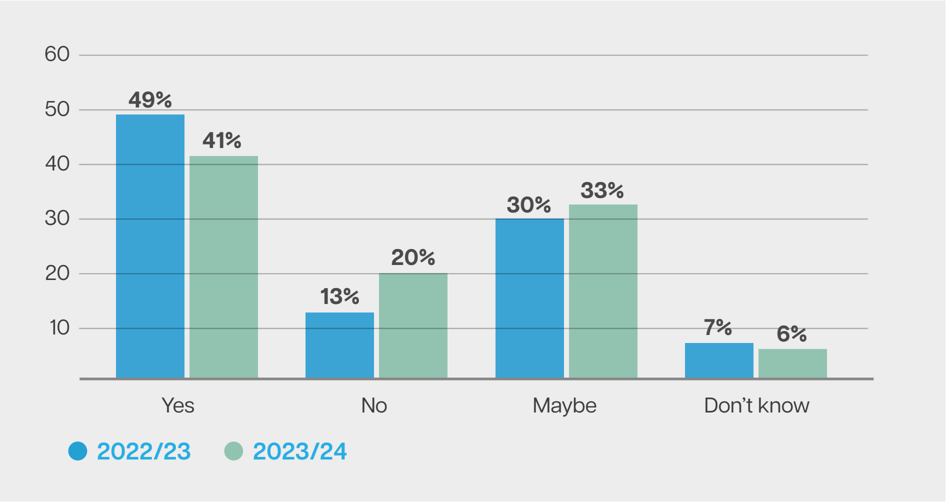


Figure 13 – Likelihood of respondents remaining with their current employer in two years' time

Despite these figures, professionals are less positive about staying in their current role than reported in the last survey. When asked whether they see themselves working for the same employer in two years' time, a fifth (20%) of respondents said 'No', compared to just 13% in 2022/23. A higher proportion were also unsure, with 39% responding 'Maybe' or 'Don't know' compared to 37% in 2022/23.

There are multiple potential causes for this mentality. On the positive side, it may reflect people who are keen to take the next step in their careers as the economy continues to improve from 2022 – especially those who have said they have "good" career prospects.

On a more negative side, it may also be an effect of ongoing uncertainty around the technology market. While reports show that there are many opportunities, professionals will also have seen highly publicised job cuts over the past year and so be either less confident in their current role, or looking for new challenges.

Skills and training

Analytical and problem-solving skills are still key to most professionals – and are vital to identifying and solving the various people, process and technology challenges they will face in their careers.

What's notable in this survey is that communications skills have surged in importance, at the cost of both analytical and technical or subject matter skills. Similarly, we see that the number of professionals citing technical skills as most important is declining, reflecting the multi-disciplinary and complex nature of cyber threats.

Given the importance placed on communication skills, this is perhaps unsurprising. After all, communication will be critical in both helping colleagues avoid mistakes that put the organisation at risk, and to investigate what's happened in the aftermath of an incident.

What's notable this year is that communication skills have surged in importance

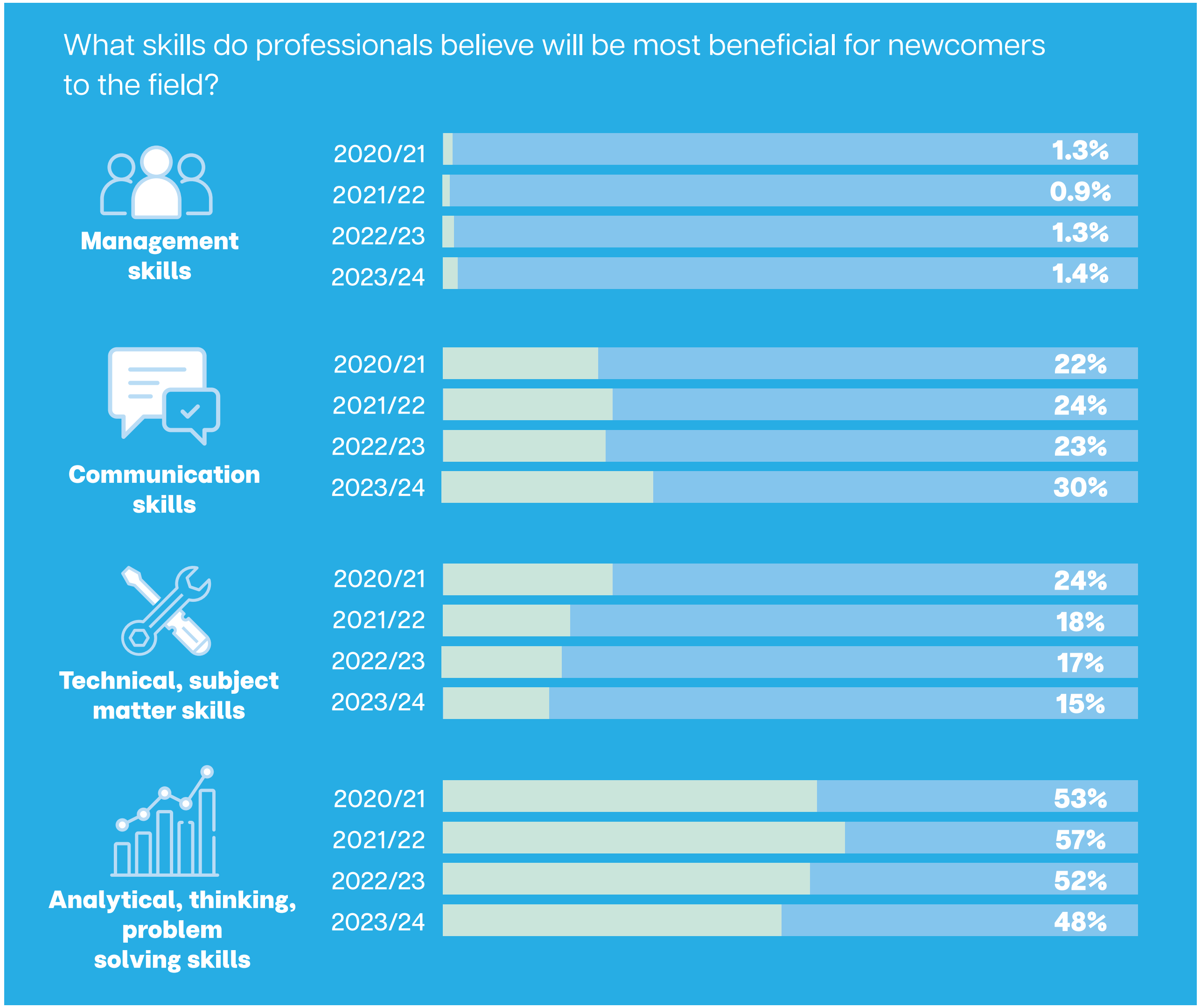


Figure 14 – What are the most important skills / abilities when entering the security profession?

Tackling the skills shortage

There is no debate that the industry is facing a skills shortage. The big question is how to address it. To do this, we need to identify where exactly the shortage lies.

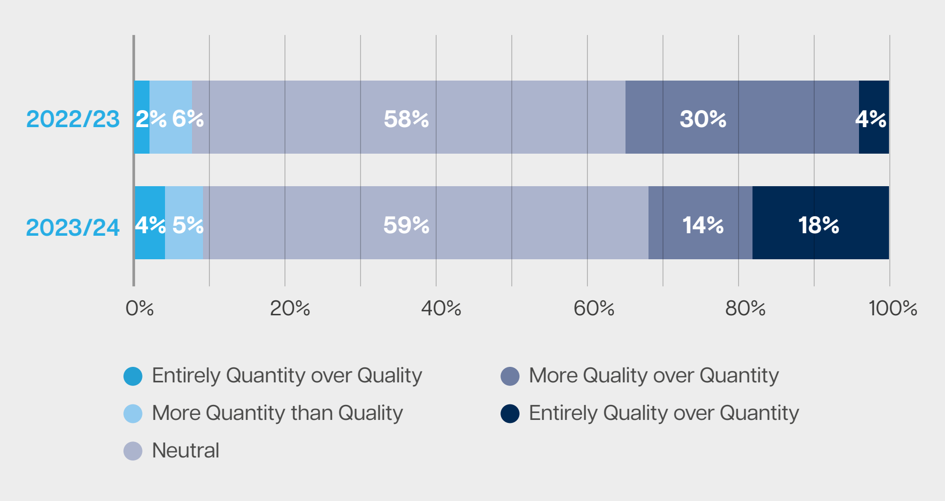


Figure 15 – Is the skills shortage a question of quantity or quality?

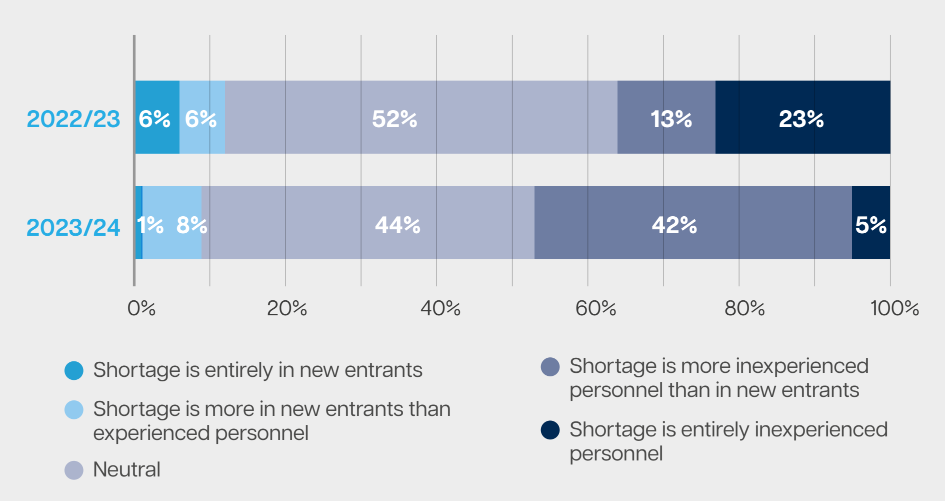


Figure 16 – Is the skills shortage more in new entrants to the industry or experienced personnel?

First, we need to understand whether the shortage is more a matter of "quantity" – i.e. the number of resources and people available – or "quality" – i.e. the level of skills people in the industry have.

It's clear professionals think the issue is one of skill levels, rather than the size of security teams.

This is also reflected when asked if the skills shortages are reflected in a lack of new entrants to the industry, or of experienced personnel. Professionals are clear that the profession does not have enough experienced personnel. And this feeling is stronger compared to 2022/23.

There is no denying increasing the number of experienced personnel with high-level skills would be a significant boost to the profession and reflects respondents' opinions on how to grow capability. However, it does leave questions.

First, there is the question of where to find these experienced, skilled personnel the profession needs. At present, security practitioners are a finite resource. Training and bringing practitioners to the right level will be essential but will still take time. Finding those team members who want to upskill, and encouraging and supporting them, will be vital. Attracting people with the right skills from other disciplines, and building on those skills where necessary, will also be important.

Second, in the long term the profession will still need to attract fresh talent. After all, these new entrants will become the skilled, experienced personnel of the future.

Whether professionals are new to the profession or have years of experience, they still need to learn in the most effective way.

Preference for learning and development

	2019/20	2020/21	2021/22	2022/23	2023/24	5-year Average
On-the-job learning	**66%**	**75%**	**63%**	**75%**	**66%**	**69%**
Attending in-person courses	70%	55%	59%	56%	50%	58%
Professional events/ seminars	45%	48%	51%	48%	50%	48%
Reading	48%	46%	44%	46%	47%	46%
Online courses	35%	46%	45%	43%	43%	42%
Focused, 1-to-1 mentoring	27%	33%	30%	39%	25%	31%
Conferences/ trade shows	20%	23%	19%	19%	23%	21%

Figure 17 – What are the most effective ways to learn and develop new skills?

Ultimately, on-the-job training is still seen as the most effective method of education. In-person, face-to-face training courses are the next most effective – although they are apparently still not as effective as they were before the COVID-19 pandemic. This may be because there are not as many opportunities as there were pre-pandemic.

Yet while both on-the-job and face-to-face training have fallen, there hasn't been a notable corresponding increase in other methods. Online courses have grown in popularity, but they aren't at their 2020 heights, while other methods, such as reading, are quite static.

Ultimately, on-the-job training is still seen as the most effective method of education

Personal job prospects

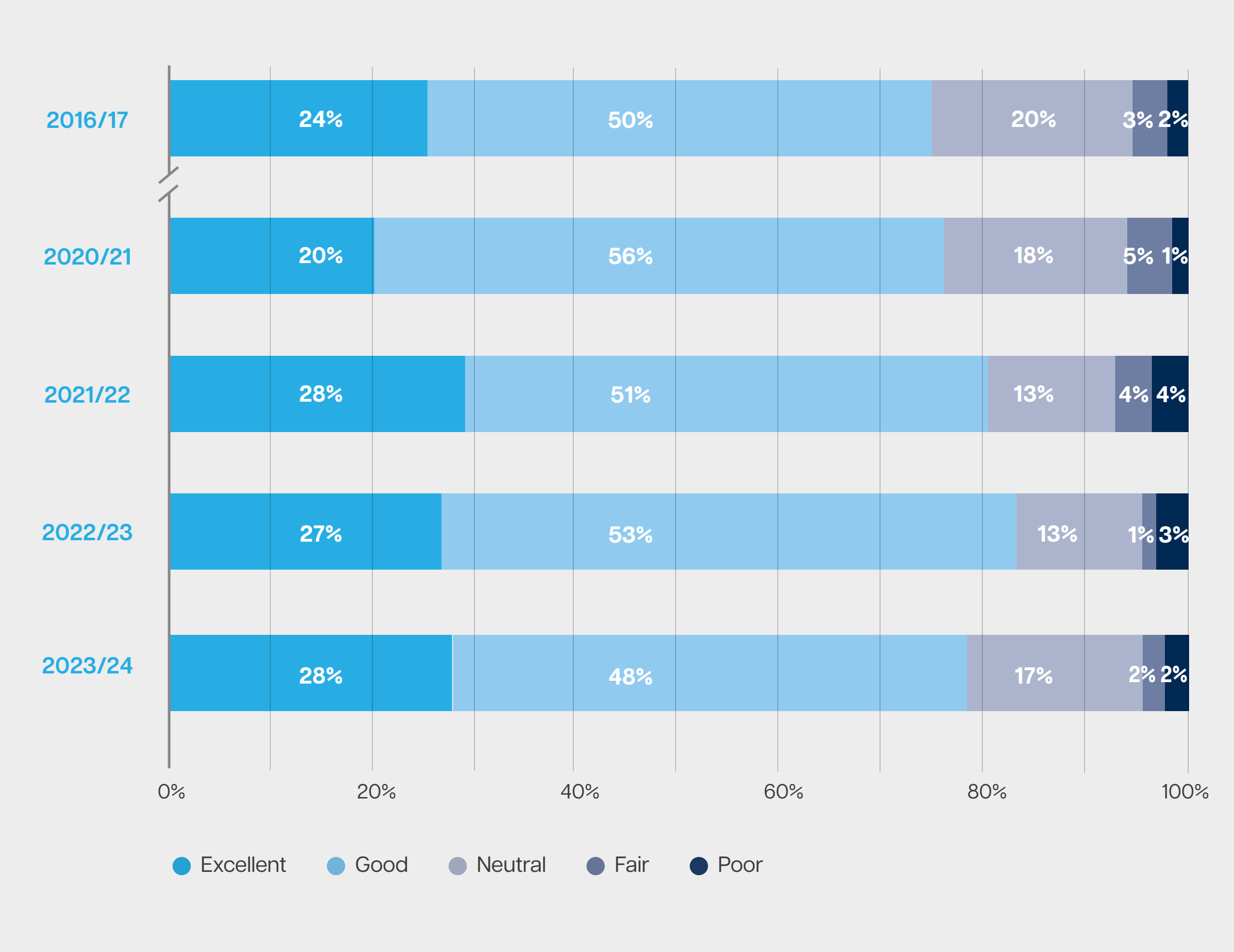


Figure 18 – What are your current personal job prospects?

Personal career prospects remain largely positive, with 75% of professionals saying they are good or excellent, which is consistent with previous years' data. This suggests that skilled cybersecurity practitioners are still considered extremely valuable and are in high demand.

75% say their prospects are good or excellent

Attracting and retaining talent

When we look at the industry as a whole attracting and retaining professionals is key. Organisations need to make sure that their existing teams are happy in their positions, are not stressed or overworked, and aren't likely to leave for a more attractive position, or a different career altogether.

As in previous years, the survey asked what professionals believe attracts people to cybersecurity roles; and what causes them to leave.

One notable fact is that stress and/or overwork is no longer one of the top five reasons for leaving a job

Factors for and against cyber security jobs

Top 5 factors that attract people to TAKE security jobs

2023/24

1. Money/remuneration
2. Opportunity/scope for progression
3. Variety of work
4. Training opportunities
5. Autonomy/scope for initiative

Figure 19 – Factors professionals believe attract people to cybersecurity jobs

Top 5 factors that cause people to LEAVE security jobs

2023/24

1. Money/remuneration
2. Opportunity/scope for progression
3. Bad/ineffectual management
4. Insufficient training
5. Boring work/lack of variety

Figure 20 – Factors professionals believe cause people to leave cybersecurity jobs

The main incentives are still financial – whether remuneration, or the extra opportunities and rewards that come with promotion. This makes sense: ultimately cybersecurity professionals are human and want to be compensated for their efforts.

However, job satisfaction is also key. This includes the quality of management, which cannot be too suffocating but instead allow for personal freedom and initiative; opportunities for training, self-expression and the feeling one is progressing in one's career; and work that actually engages the professional.

This is a valuable lesson for organisations. Not all will have the resources to compete for the best talent on pay alone. Quality of management, opportunities for training and progression, and offering interesting, varied work present a much more level playing field.

Stress and overwork

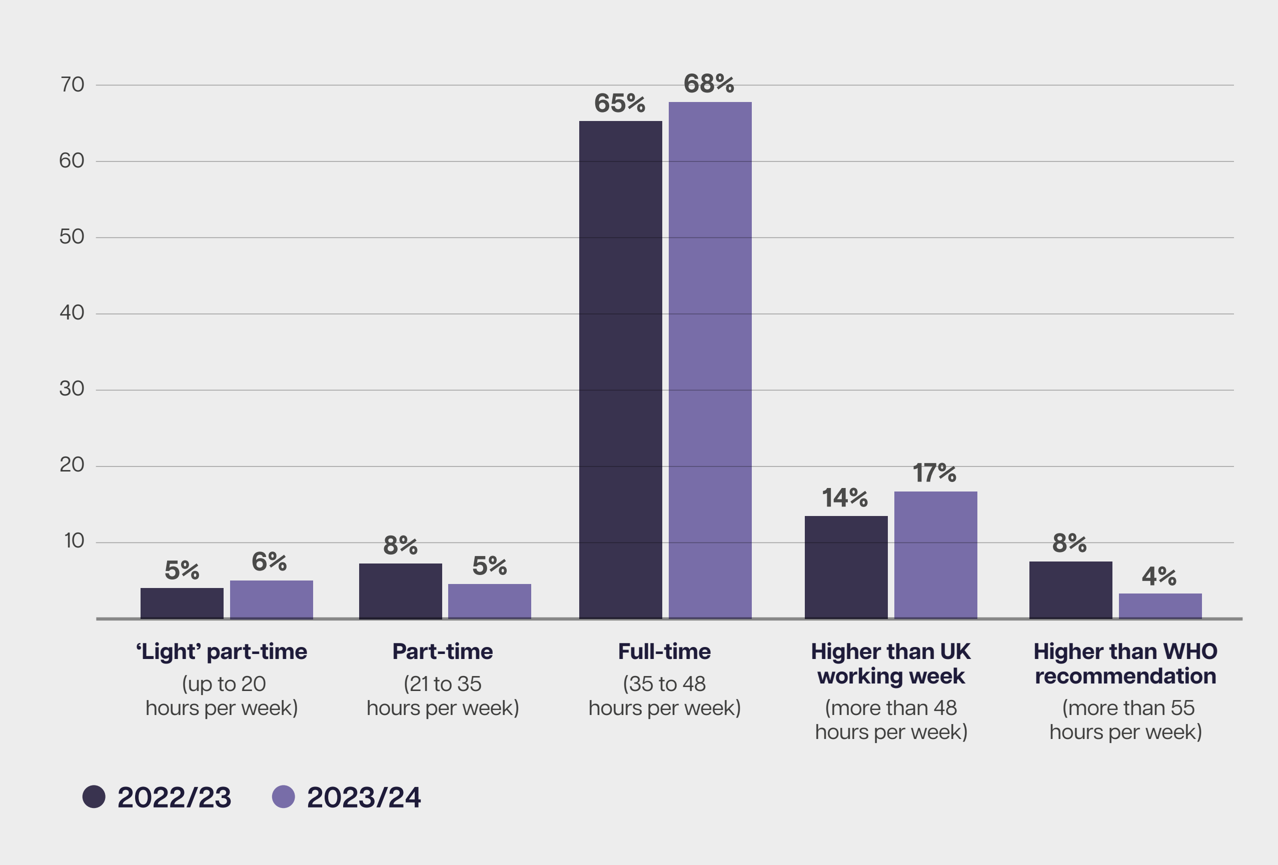


Figure 21 – Hours worked per week by professionals, 2022/23 vs. 2023/24

One notable fact is that stress and/or overwork is no longer one of the top five reasons for leaving a job. While it could be considered a side effect of bad management, it used to be a regular feature in the tables as a factor in its own right.

However, this doesn't mean that the issue has disappeared.

In particular, we can see that the proportion of professionals who would count as "over-worked" (i.e. working more than the UK recommended working week) has remained approximately the same at 21%.

There is a positive side to this: the proportion of "over-worked" professionals has shifted so only 4% are exceeding the World Health Organization's recommended safe working hours of 55 per week – half that recorded by the previous survey. There are also more professionals working full-time hours, giving a mean working week of 42 hours.

21% of professionals are putting in hours that class them as "over-worked"

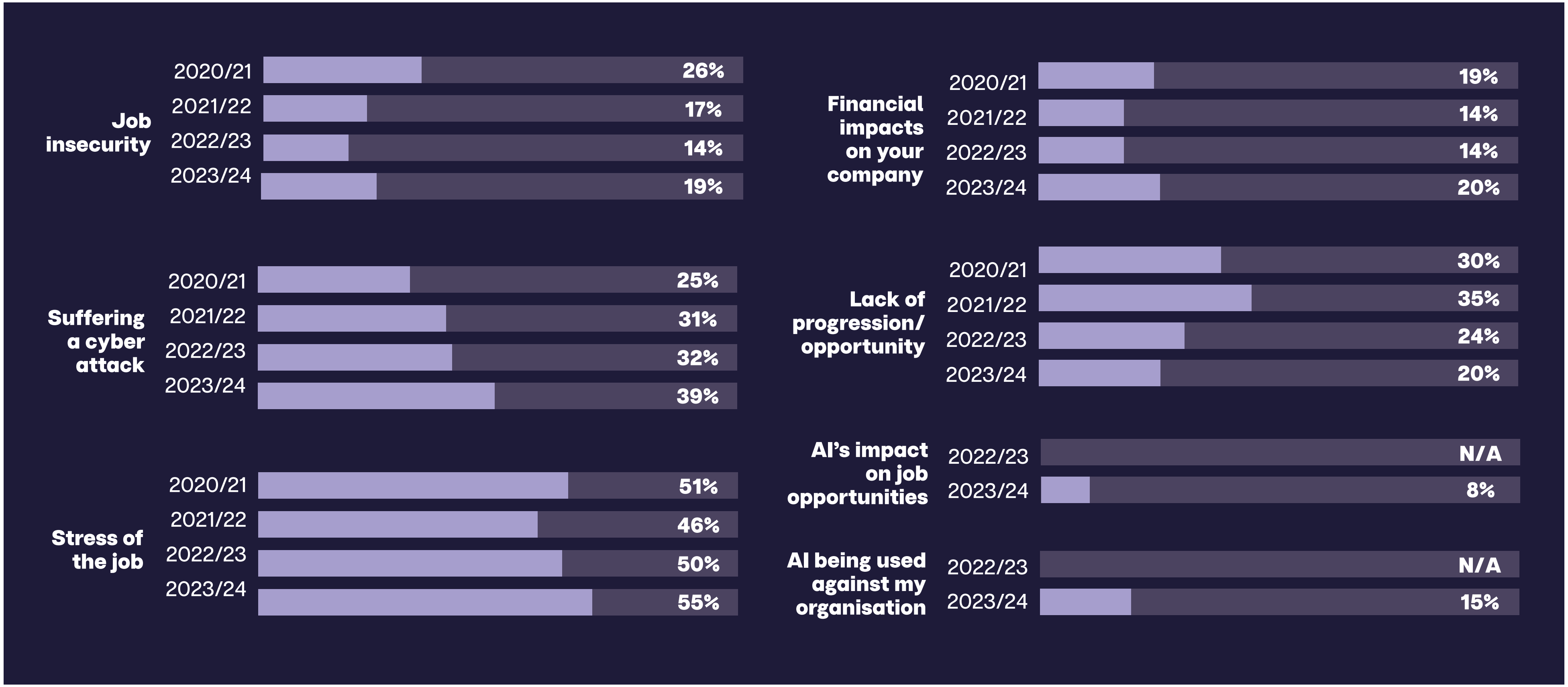


Figure 22 – What keeps professionals awake at night?

More than half of professionals (55%) say the stress of their day job keeps them awake at night, while the ever-present risk of actually suffering a cyber attack is also creeping up in people's minds – reaching a high of 39% of professionals this year. Concerns about financial impacts on the business are also high – even higher than in 2020/21.

Interestingly, while AI has burst onto the scene recently as a new concern for security professionals, at present it is still relatively low as an overall cause of stress compared to other, more "traditional" sources.

After surging in 2020/21 and then dropping year-on-year, job insecurity is once again rising as a concern.

PART FOUR

Cybersecurity challenges and capabilities

The most important question for the cybersecurity profession is whether it can effectively defend systems against attacks, safeguard data, and manage incidents as they arise.

57% believe the industry is doing better or much better than previous years when defending against and dealing with incidents

Defending against, and dealing with, incidents

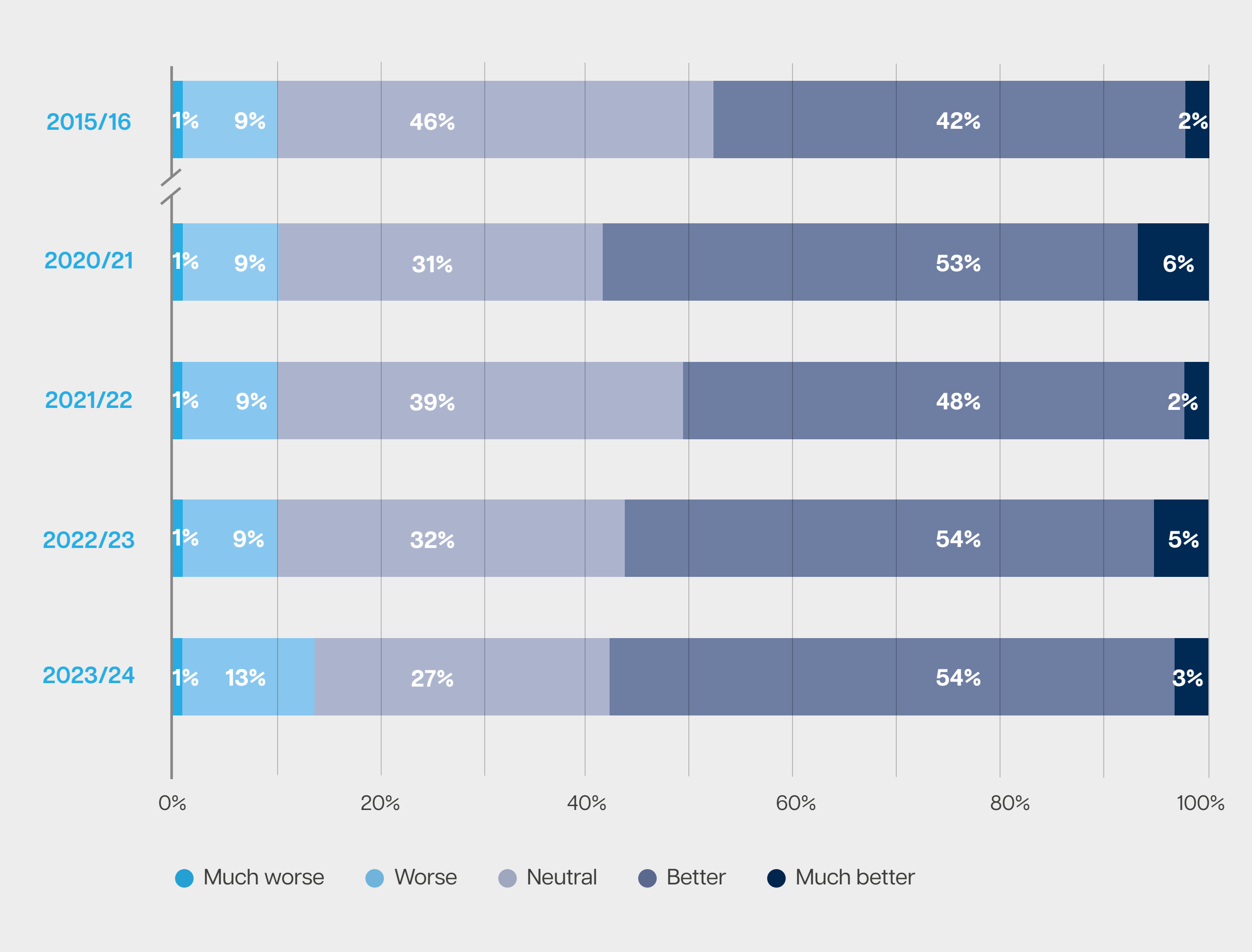


Figure 23 – How is cybersecurity performing at defending systems from attack and protecting data?

At first glance, the outlook is positive. 57% of professionals believe the industry is doing better or much better than previous years, while only 14% believe it is doing worse or much worse. However, looking deeper, there is a concerning trend.

While the proportion of "neutral" responses is falling over time, the percentage of professionals who believe the industry is performing worse has increased, suggesting many previously neutral professionals' opinion has worsened.

Overall, the profession is performing well, but this is a warning against complacency. The cybersecurity profession needs to ensure it is anticipating and responding to new threats and trends to prevent the "worse" percentage from steadily creeping up .

The same is true when we look at how cybersecurity handles incidents when they occur. Again, the outlook is overwhelmingly positive, with 58% saying cybersecurity is performing better or much better, while only 13% say it is performing worse.

Yet again, the number of professionals saying performance is worse has taken a notable leap – the highest recorded so far.

Worse, as with defending systems from attack and protecting data, there is a slow but noticeable decline in professionals saying cybersecurity is performing “better” or “much better” from its high point in 2020/21. The profession needs to arrest this decline, since, at present, it seems like the poor performance recorded in 2021/22 is no longer an anomaly, but part of a trend.

58% say cybersecurity is performing better or much better at dealing with incidents

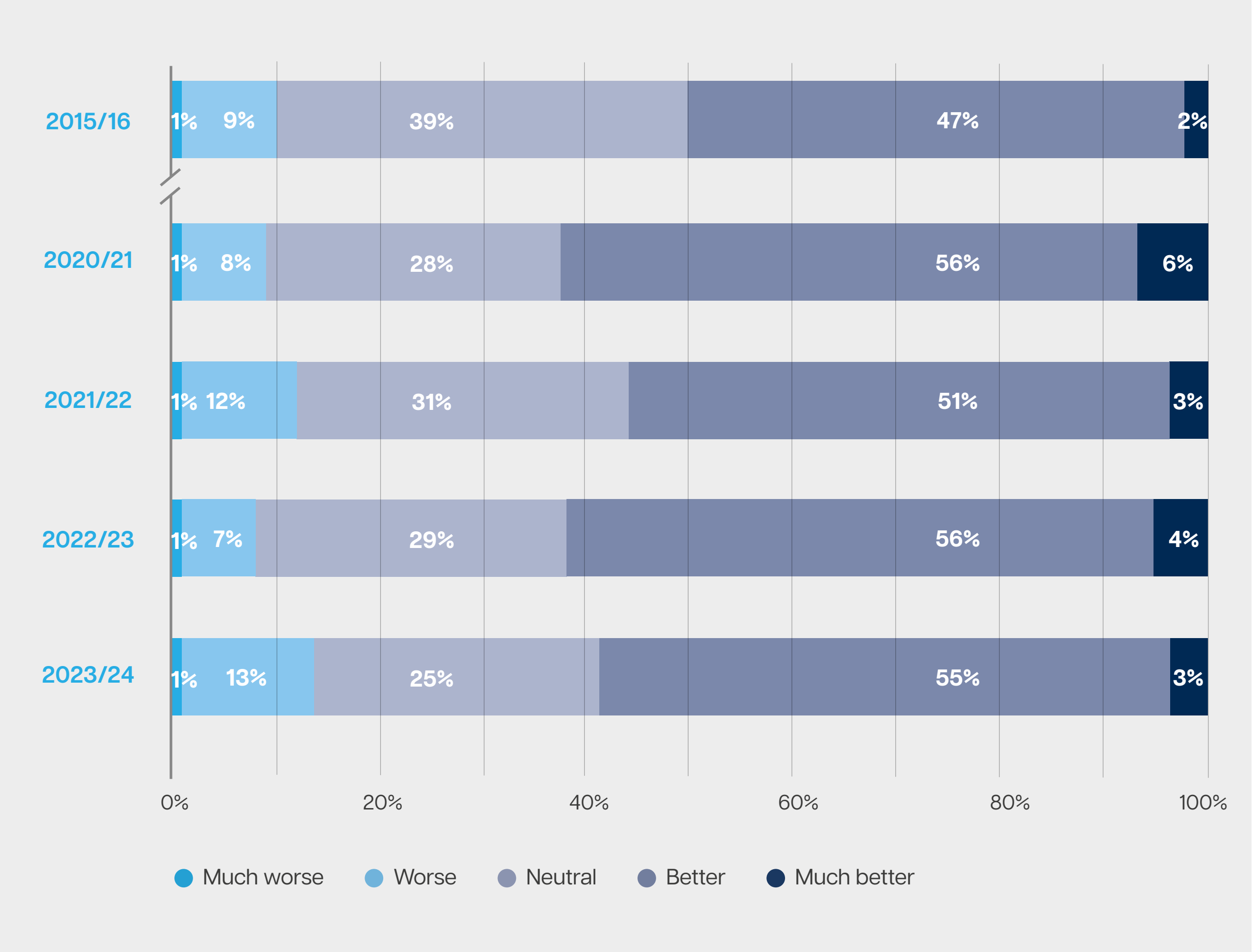


Figure 24 – How is cybersecurity performing at dealing with incidents when they occur?

Facing challenges

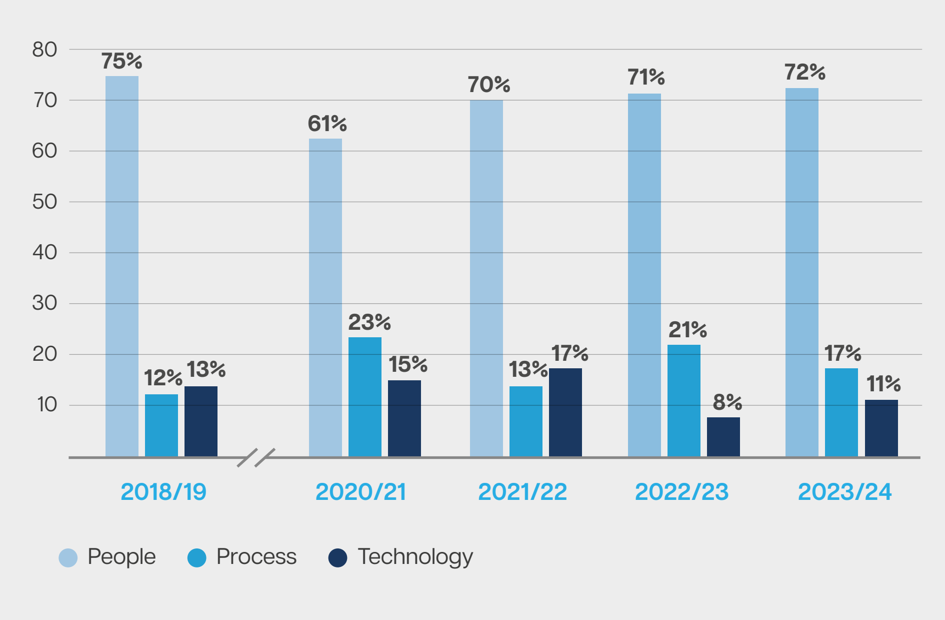


Figure 25 – What is the greatest challenge facing cybersecurity teams?

To arrest this decline, the profession needs to understand the challenges it faces. As in previous years, "people" is seen as by far the greatest challenge to security, distantly followed by "process" and "technology".

Interestingly, this marks the second year in a row that "process" has been seen as a bigger challenge than "technology". The trend appears to be that protecting technology – and having the right technology in place – is viewed as relatively straightforward. However, ensuring the processes are in place to use that technology safely, and adapting to humans' near-infinite capacity to do the unexpected and create unforeseen issues, are where the real challenge lies. In turn, this means security teams need the capabilities to match.

Building and maintaining capability

To ensure the profession doesn't lose more ground when defending against and reacting to incidents, and can face its challenges, it needs to build its cybersecurity capability in the right way.

1	**Developing/training existing security professionals**
2	**Cross-training from other technical areas**
3	**Recruiting experienced security staff**
4	**Cross-training from other business areas**
5	**Apprenticeships**
6	**Graduate recruitment**

Figure 26 – The most effective ways to build cybersecurity capability

Professionals are very clear on how to build that capability. While detailed ratings have shifted year-on-year since we first asked the question in 2018/19, the ranking of the different approaches has remained consistent. Professionals are firm believers in the need for building on existing skills.

They are currently less convinced of the need for new blood – a theme we will return to later on. Cross-training from other business areas, apprenticeships, and graduate recruitment are still seen as less effective quick fixes, although they will be crucial in the long term.

Changing budgets

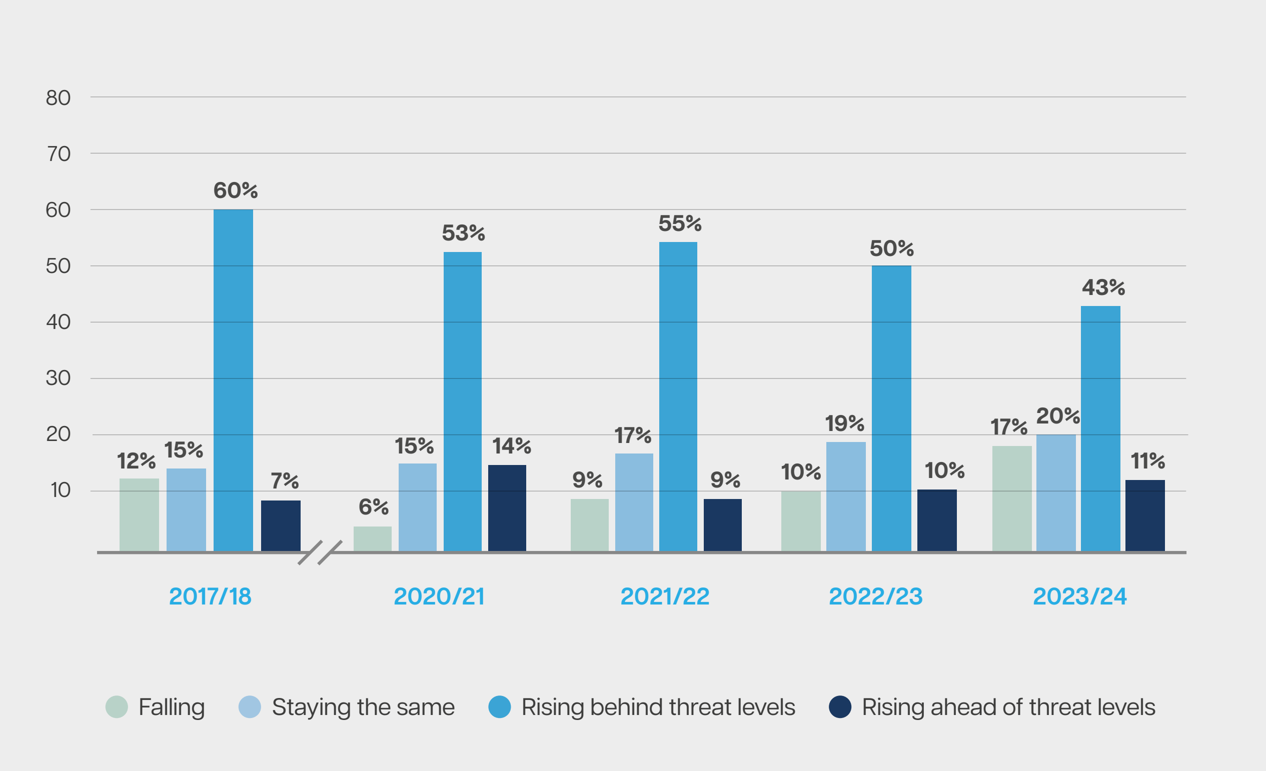


Figure 27 – Professionals' opinion on cybersecurity budgets

When asked their opinions on the state of security budgets, professionals are pessimistic. Although 11% believe budgets are rising ahead of threat levels – the second highest figure since 2020/21 – the number who believe budgets are staying the same (20%) or falling (17%) are both at record highs. 80% think budgets are rising too slowly, staying the same, or falling.

The results show a consistent trend since 2020, with those thinking that budgets are rising ahead of threat levels remaining fairly consistent; those that see budgets rising behind threat levels dropping; and the number of respondents that believe budgets are remaining the same or falling are both steadily rising.

This may be due to turbulent economic circumstances, with security budgets affected by events such as the UK entering recession at the end of 2023. However, with the consistent trends that have emerged, it is clear that the security industry is having to do more with less and find new ways to cope with emerging threats without increasing spend.

11% believe budgets are rising ahead of threat levels

A growing market

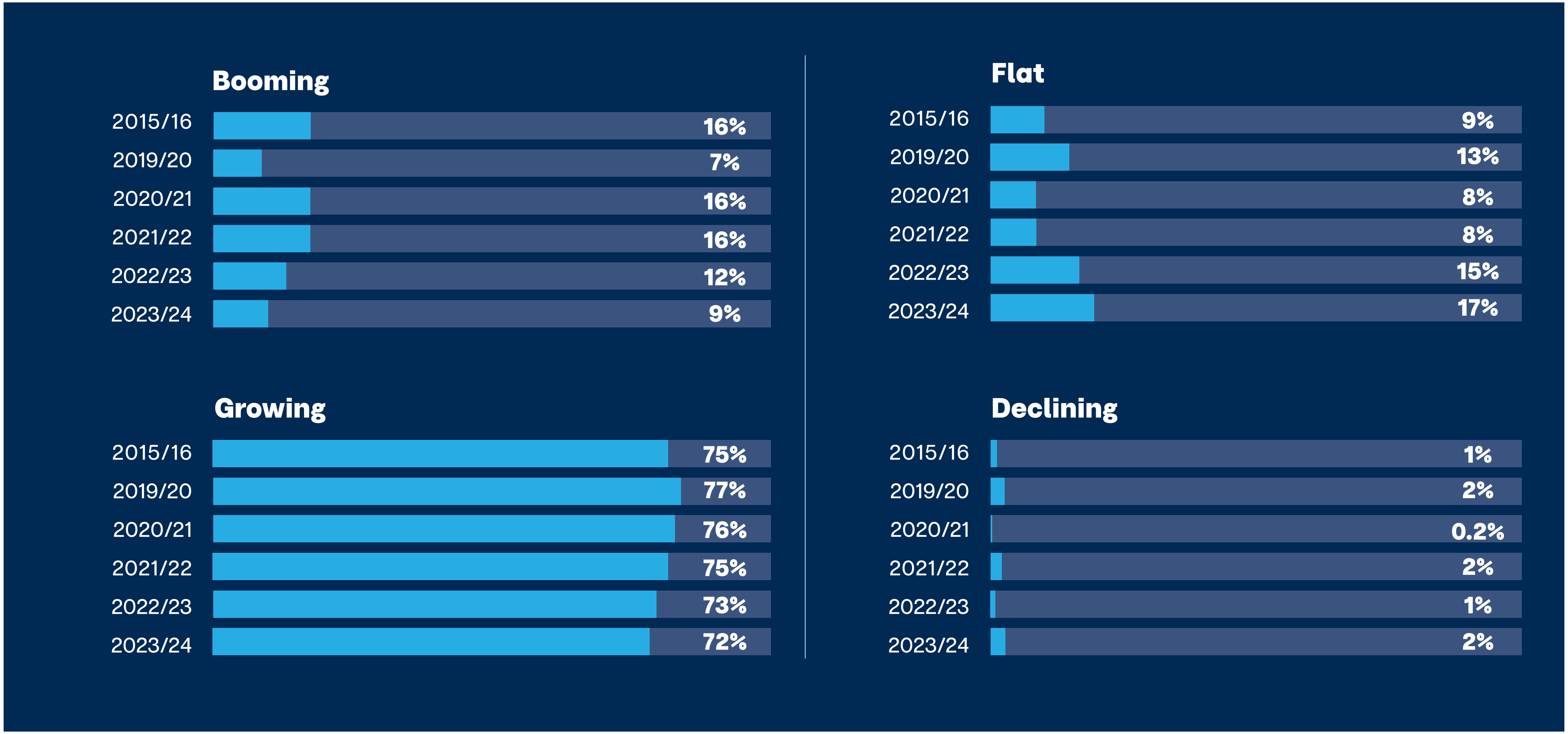
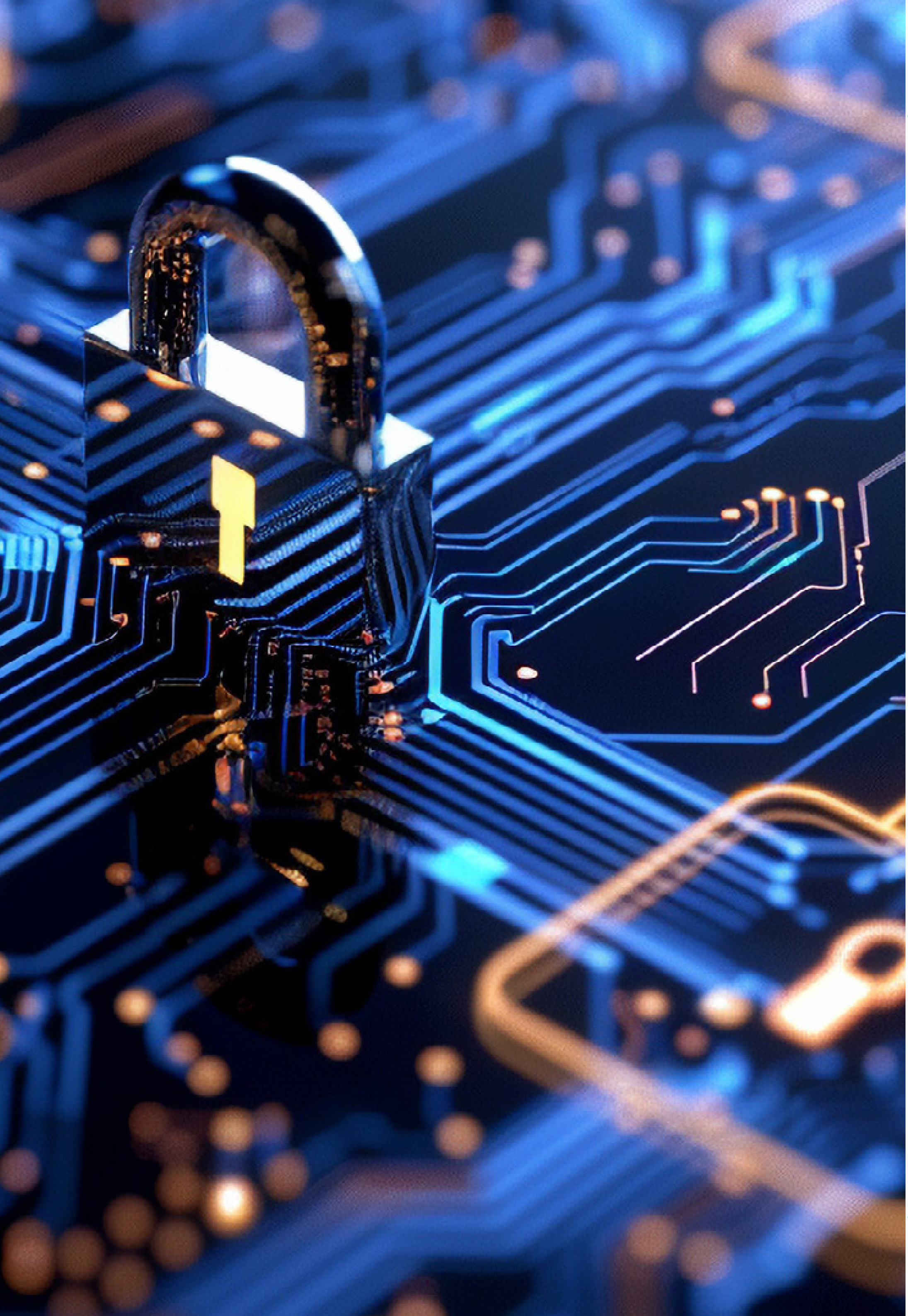


Figure 28 – Predicted growth of the security industry over the next three years

This pessimism about budgets is reflected in the overall security market. When asked how they expect the security market to change over the next three years, a higher proportion of professionals expect it to stagnate – either decline or stay the same – than ever before (19%). Consequently, both the "grow" (72%) and "boom" (9%) categories have shrunk.



PART FIVE

Handling breaches

Part of the importance of closing the skills gap is so organisations can react appropriately in the event of a breach. We have seen from earlier questions that an increasing percentage of professionals believe the industry is getting worse at responding to incidents. But what does this look like in practice?

We can discover this by looking at which breaches professionals think were handled well or badly; and what factors affected their opinions.

41% of respondents couldn't name a breach that was handled well

Handling breaches well

Since 2020 which security breaches were handled effectively?

Name of breach	Number of reports
"Cannot think of an example"	21
Cannot answer (e.g. due to NDA)	12
"The most successfully handled breach is one we never hear of"	8
International Committee of the Red Cross (ICRC)	3
Log4j	3

Figure 29 – Top five responses saying which breaches were handled well

Only 55% of respondents were able to recall a single incident, and only ten incidents were named by more than one person.

One thing to note is the high number of professionals who could not think of or provide an answer. Arguably this is a reflection of the fact that well-handled breaches are so rare that it's hard to provide examples.

However, when we consider the professionals who said a successfully handled breach is one you never hear about, we can take a more positive view. Ultimately, people are less likely to learn or remember the name of a breach that's handled successfully as it doesn't attract attention or headlines.

Handling breaches poorly

When asked to identify breaches that were handled poorly, the figures are almost reversed.

Name of breach	Number of reports
Capita	12
SolarWinds	11
LastPass	9
MoveIT	7
British Airways	6

Figure 30 – Top five breaches since 2020 that were handled badly

In stark contrast to well-handled breaches, 82% of professionals could name specific breaches that were poorly handled, with twice as many receiving more than one vote.

Perhaps more worryingly, those breaches were also, on average, identified by many more people. The most identified example of a poorly handled attack, Capita, was flagged by four times as many professionals than those who said ICRC was a well-handled breach.

This speaks to the reputational damage a badly handled breach can cause. Some breaches were mentioned as being handled both well and badly - specifically SolarWinds, Okta, the British Library, and Microsoft. Yet each of these received more negative mentions than positive.

It's also notable that those breaches that were handled well tend to be more recent, while badly handled breaches – such as British Airways, which has been mentioned by respondents since 2018 – can stick in the mind for longer.

To some extent, this may be due to a vicious circle: a badly handled breach is more likely to be reported and gain prominence. This will in turn draw more attention, expose any failure in more detail, and inevitably lead to more awareness.

What factors make the difference?

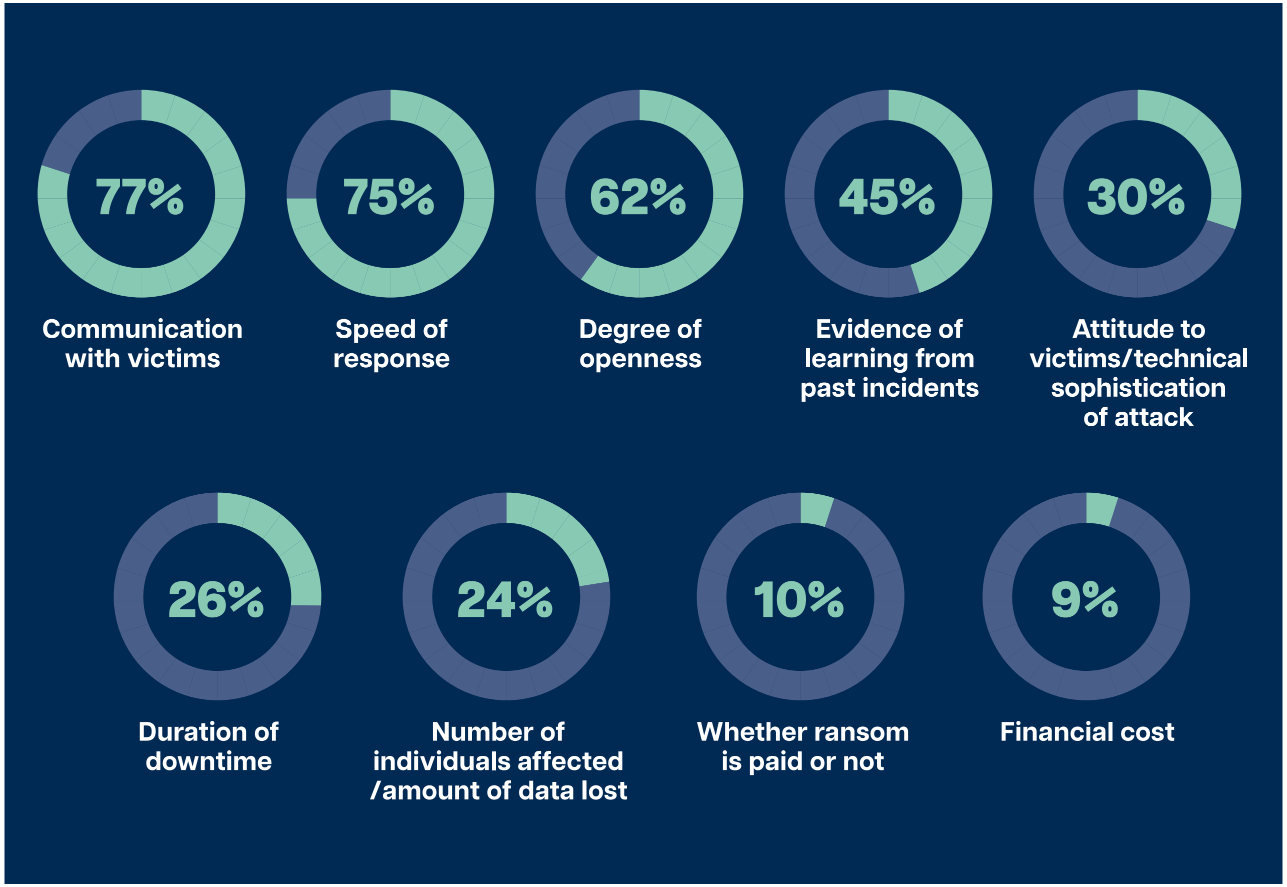


Figure 31 – Factors affecting whether a breach is handled well or badly

Finally on this topic, we asked what factors professionals believed most affected whether a breach was handled well or badly.

The trend with previous years is clear: the most important factors are communication, speed and openness. This doesn't only apply to making victims aware of a breach, remediating the effects and showing that the organisation has taken the right action promptly. It also applies to communication with regulators and other relevant parties.

The most important factors are communication, speed and openness

```
  }

  kfree(group_info);
}

EXPORT_SYMBOL(groups_free);


  nblocks = nblocks ? : 1;
  group_info = kmalloc(sizeof(*group_info) + nblocks*si
  if (!group_info)
    return NULL;

  group_info->ngroups = gidsetsize;
  group_info->nblocks = nblocks;
  atomic_set(&group_info->usage, 1);
```

```
Live link is activate. You can now view guestbook in your browser.
Local:              http://localhost:3000
On your network:    http://192.80.72.55.91:3000

Development book has not been optimized yet...
```

PART SIX

The emergence of artificial intelligence (AI)

Each year we choose one topic to investigate that has the ability to significantly impact the security profession. This year, following the rapid growth of Large Language Models, such as ChatGPT, and the growing realisation that AI could be a game-changing technology for many verticals, we have focused on artificial intelligence.

But first, it’s important to know whether the industry believes AI is truly influential or whether it is surrounded by hype.

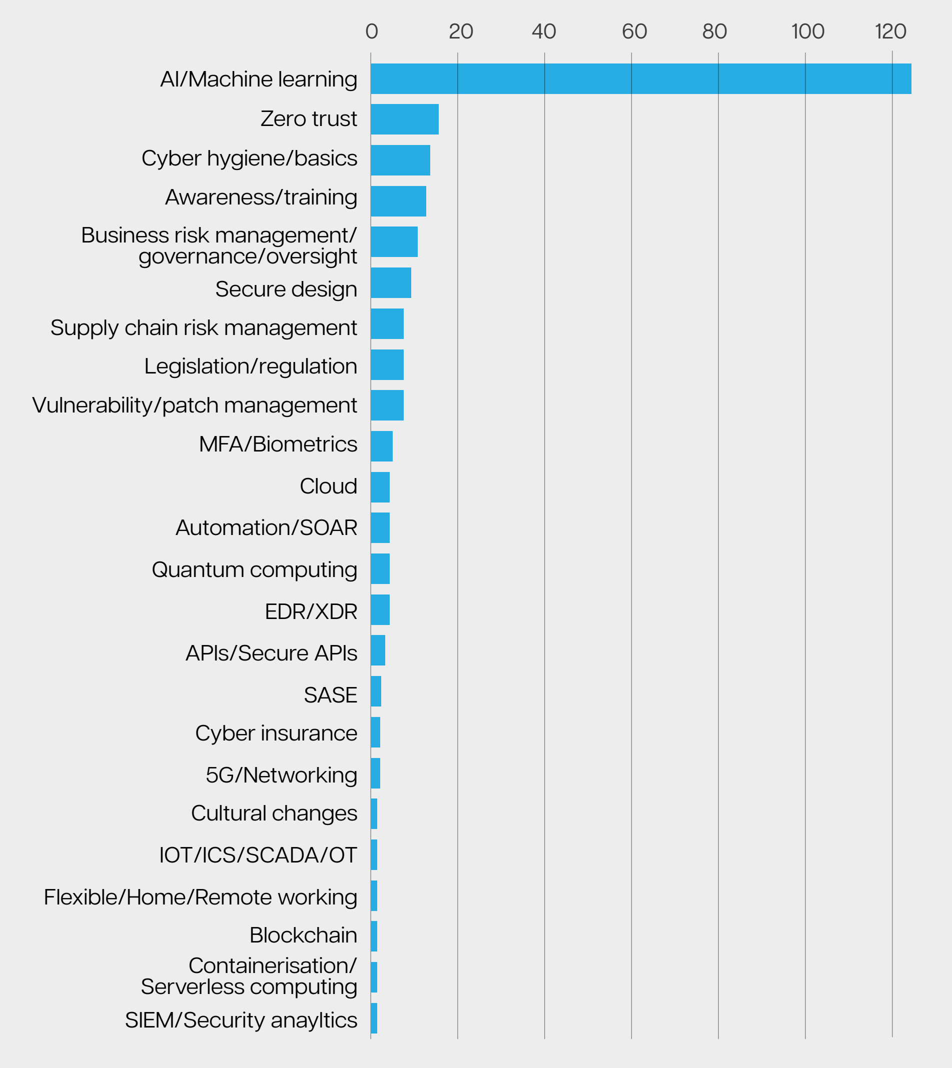


Figure 32 – What do respondents believe will be the most influential technology or innovation over the coming year (number of respondents)?

When asked what the most influential technology or innovation will be over the next year, AI and machine learning was the clear winner. More than half of all professionals who answered chose it – more than eight times as many as the next highest option. AI has clearly moved to the forefront in a way it hasn't done in previous years.

The impact of AI on cybersecurity

At present the security industry does not appear to have a unanimous view on the benefits, challenges and opportunities around AI.

It seems the only thing a clear majority of professionals can agree on is that the benefits of AI are as yet undecided. Nearly three-quarters (73%) agree that for some sectors AI will be very bad, while for others it will be very good.

Otherwise, it seems that many organisations are at a tipping point. 39% of professionals say they have had to adjust their views and/or change their approaches to tasks because of AI. And while just over half (56%) say their organisation is aware of the risks from AI and has policies in place, this means a significant proportion (44%) do not.

On other issues, professionals are split almost 50/50, with 54% believing AI will benefit attackers more than defenders. Just under half (49%) think developments in AI will be positive within the security profession. And almost the same proportion (48%) think developments in AI will be positive for society as a whole outside security.

It's clear opinion is divided. The picture is clearer when we look at how AI is likely to impact different groups.

54% of professionals believe AI will benefit attackers more than the risk defending community

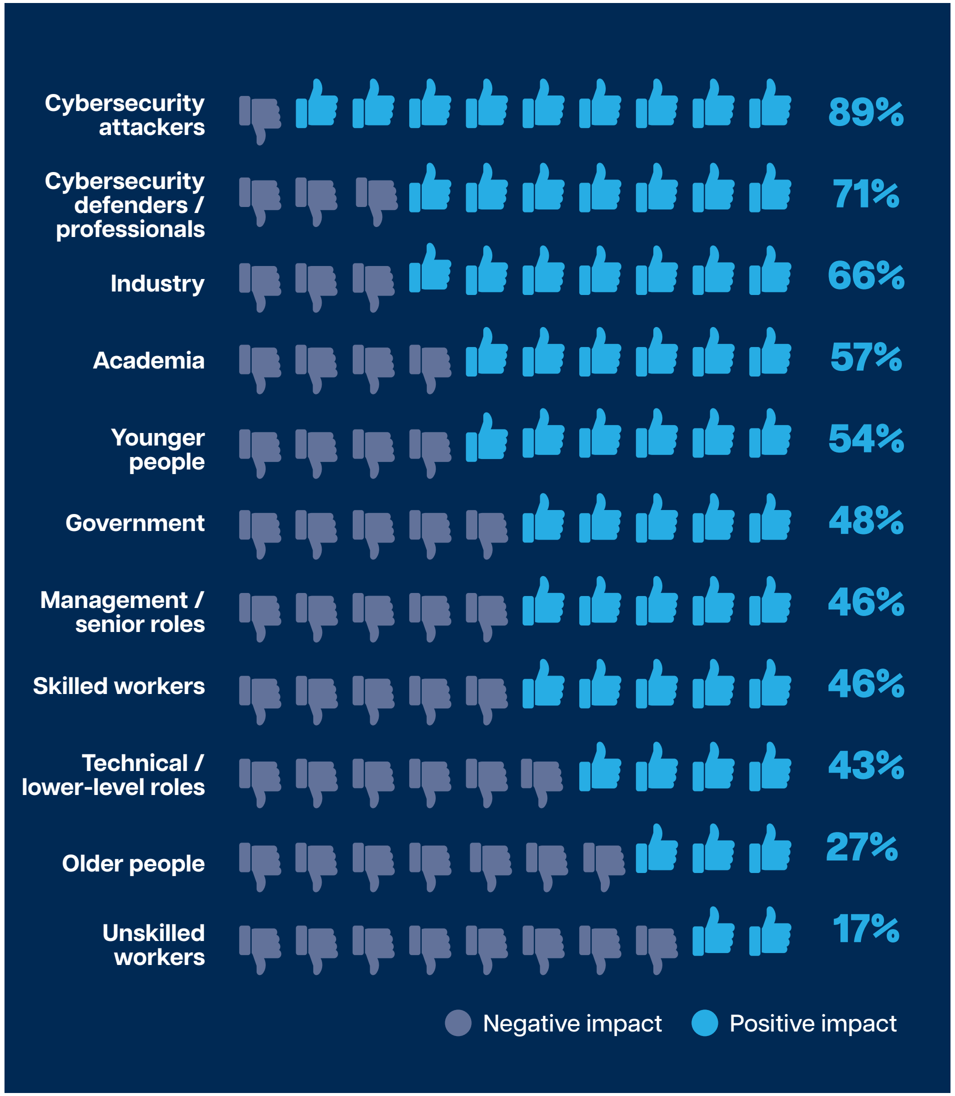


Figure 33 – AI's positive or negative impact on different groups

The impact of AI on different groups

By asking whether AI will have a more positive or negative impact on different groups, we begin to get a picture of who professionals think the real winners will be.

Worryingly, the ratios opposite suggest that cyber attackers, potentially the only group with nothing to lose from AI, will be the biggest winners. Professionals overwhelmingly believe attackers will benefit – considerably more than those who think the same about defenders.

At the opposite end of the scale, professionals are most pessimistic about how AI will impact unskilled workers, older people and, to a lesser extent skilled and technical workers – all of whom could find their roles being taken over, or changed, by AI; or being left behind by business or social developments.

The impact of AI – in security professionals' own words

For a more detailed understanding of who might benefit from AI, professionals described in their own words what job roles or job families AI would be most beneficial or detrimental for.

Once again, there isn't yet a clear consensus. A large number believe that Network / Security Operations Centre (NOC/SOC) and similar roles will benefit from AI – as it will make identifying, triaging and responding to potential threats an operation that can be performed faster, and at greater scale.

However, with automation comes fear of job losses, and a similarly large number believe AI could impact these roles. At the same time they believe AI could give hostile actors a way to flood organisations with AI-generated attacks.

The overall message is more positive when professionals say, in their own words, how AI will impact their roles. The response is more upbeat, with the ability to analyse and triage data more effectively repeatedly flagged.

State of adoption of AI

Next, we come to how individual professionals, and their organisations, are using AI.

Individual

I am at least considering using AI in my role	85%
I am using or experimenting with AI to undertake or gather research on topics	49%
I am using or experimenting with AI to compose text	43%
I am using or experimenting with AI to build into existing technology and tools	38%
I am using or experimenting with AI to create imagery or other content / media	33%
I am using or experimenting with AI to create code, scripts and/or program snippets	33%
I am using or experimenting with AI to process data, identify threats and/or detect patterns	29%

Figure 34 – Professionals' use of AI on an individual basis

At the individual level, most professionals are at least taking their first steps with AI. Yet at present there isn't a single "killer app" that is the most effective use case.

For instance, we can see that almost half are using AI to perform research and effectively act as a more advanced search engine. But this means more than a third are experimenting with AI but not doing this. And despite flagging the ability to analyse and triage data as a benefit of AI earlier, less than a third of professionals are currently using or experimenting with AI for this purpose.

Organisation

My team or wider organisation apart from myself is using AI	87%
We are using or experimenting with AI to compose text	56%
We are using or experimenting with AI to undertake or gather research on topics	54%
We are using or experimenting with AI to create code, scripts and/or program snippets	43%
We are using or experimenting with AI to process data, identify threats and/or detect patterns	42%
We are using or experimenting with AI to build into existing technology and tools	42%
We are using or experimenting with AI to create imagery or other content / media	36%

Figure 35 – Professionals' use of AI on a team- or organisation-wide basis

Across the broader team and organisation, we can see that AI uptake has been higher – although the increase is still small.

For instance, there are clearly more organisations than individual security specialists using AI to process data, identify threats and detect patterns, and it is correspondingly higher on the table. Similarly, many more organisations than individuals are using AI for creative purposes.

3% of professionals have had a problem, health condition or financial issue caused or worsened by AI

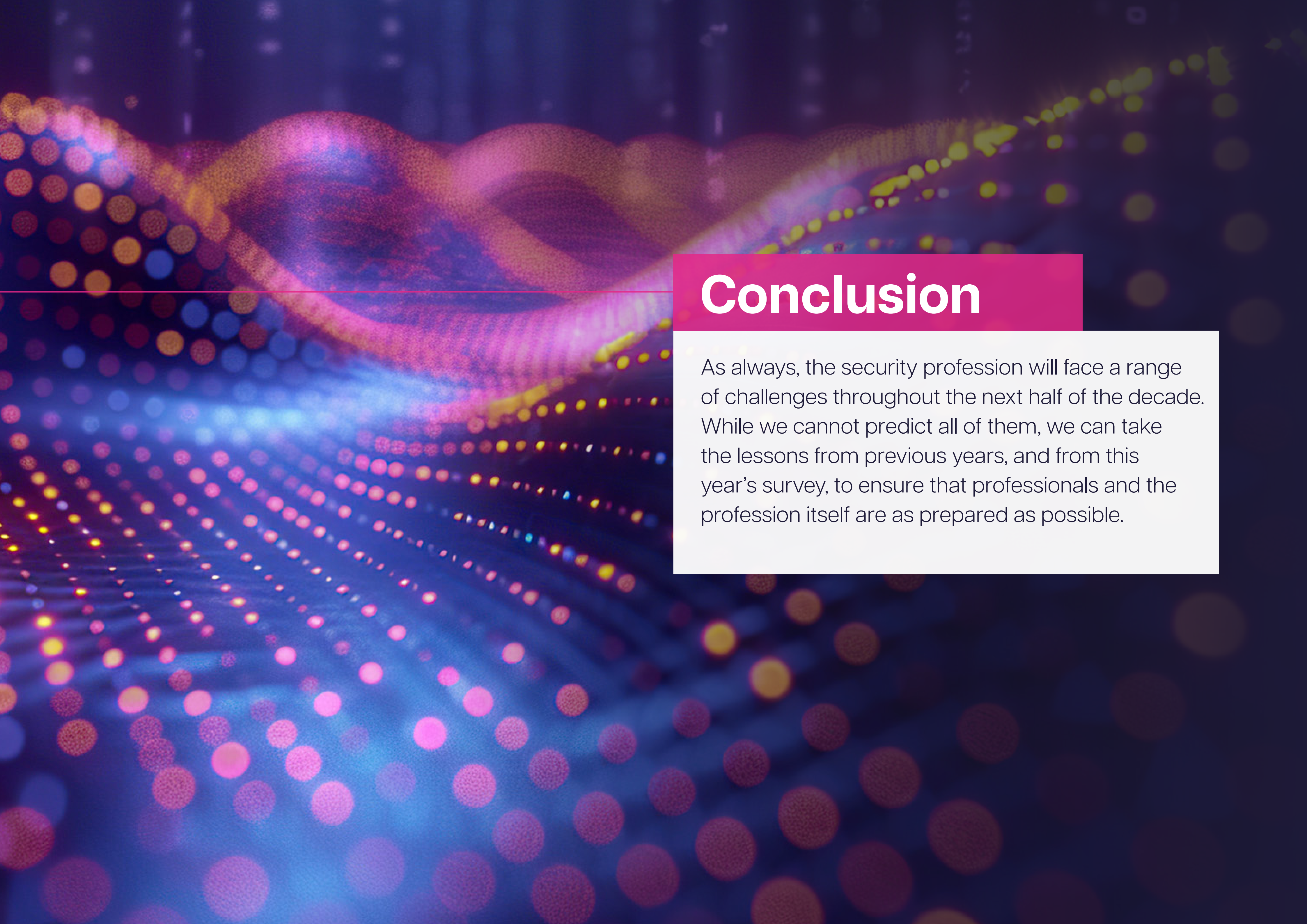
Personal impacts of AI

Finally, there was the question of whether AI has directly impacted professionals' personal lives. So far, this seems to be a rare occurrence. Only 7% have had a problem, health condition or financial issue flagged up, diagnosed or detected by AI. And a mere 3% have had one of these issues actually caused or worsened by AI.

We should bear in mind that in both cases more than 20% said they didn't know – meaning there may be more influence from AI that we as individuals are unaware of.

However, in general, security specialists' main task with AI should be making sure their organisations can use it effectively, efficiently and above all safely.

7% of professionals have had a problem, health condition or financial issue flagged up, diagnosed or detected by AI



Conclusion

As always, the security profession will face a range of challenges throughout the next half of the decade. While we cannot predict all of them, we can take the lessons from previous years, and from this year's survey, to ensure that professionals and the profession itself are as prepared as possible.

Recommendations

- Continuing to attract people from different backgrounds into the profession, offering fresh perspectives and ensuring cybersecurity can adapt to and protect against increasingly diverse threats.
- Ensuring that cybersecurity is a profession that helps people grow and feel appreciated: emphasising the above-inflation remuneration and the opportunity to continue building skills throughout one's career.
- Investing in training and education so that cybersecurity teams can keep building their capabilities and ensuring that the profession does not fall behind the cyber threat.
- Focusing on best practice when responding to breaches: with communication, speed and openness being paramount. Training will be vital here, with role playing and desktop exercises helping to ensure staff are prepared for a breach.
- Understanding new technologies such as AI, recognising both the risks they can present and the opportunities they open up.

Focusing on best practice when responding to breaches: with communication, speed and openness being paramount

Methodology

CIISec performed an online survey of 311 cybersecurity professionals between October 2023 and March 2024. Respondents were drawn both from within CIISec's membership and the wider cybersecurity profession.

About CIISec

The Chartered Institute of Information Security (CIISec) is the natural home for the cyber professional community. As the first institute in the space to be granted Royal Charter status, CIISec provides a universally accepted focal point for cyber and information security professionals at every career stage; CIISec is committed to raising levels of competency, and developing teams effectively, ensuring today's professionals are equipped with the skills and knowledge to navigate the cyber threats of tomorrow. This is achieved through having programmes that support development, recognition and success.

Development - CIISec is the place to go for cyber professional development and ethical practice.

Recognition - CIISec provides an authoritative voice for the cyber industry and recognition of excellence in practice.

Success - CIISec helps you and your business succeed securely in the digital world.

ciisec.org

Head Office

Haddonsacre Station Road
Offenham Evesham
WR11 8JJ

membership@ciisec.org

Chartered Institute of
Information Security