Chartered Institute of Information Security

The Security Profession

2022/23

Introduction

As in previous years, this survey continues to give us fascinating insights into the industry and its members, their careers and the challenges they face. But it also helps us to understand new industry developments and emerging threats and how they might affect us.

I'm pleased to introduce the eighth year of CIISec's 'State of the profession', our annual review of the security profession.

As I write this, we are all struggling with a period of economic uncertainty, with interest rates still high and political unrest and war in some regions. Meanwhile, technology changes continue to bring along new concerns, for example, the rise and impact of AI on business.

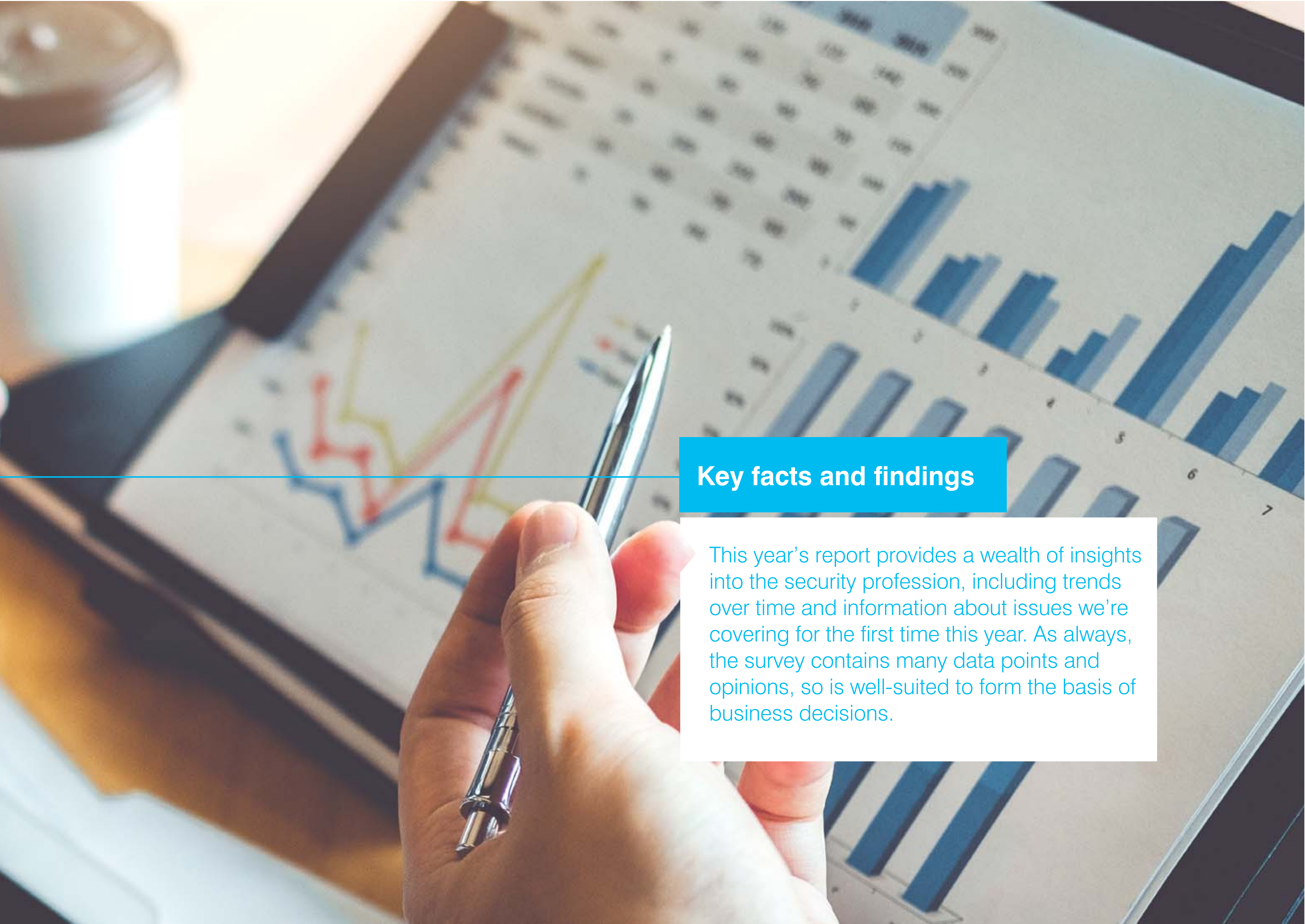
As a result, this year's survey has a focus on this economic environment. What challenges does it create for the security profession? Who do members believe will be most affected? And can we interpret some of the data we gather year-on-year with this in mind?

We have also found that the profession appears to have moved on somewhat from the pandemic – while doubtless some people are still worried at a personal level, it does not feature as a significant issue in people's professional or career concerns any longer.

As ever, we hope you find this report and our findings useful. Please do lean on the data to support decision-making, or for learning and education, wherever it may help. The survey, being annual, will once again be issued later in the year, and will have its own specific theme for 2023/24, so please take the opportunity to respond when that is available.

Piers Wilson
Director, CIISec

The results in this survey reflect the views of **302 respondents** across the UK cybersecurity industry, including both **CIISec members** and those outside the organisation.



Key facts and findings

This year's report provides a wealth of insights into the security profession, including trends over time and information about issues we're covering for the first time this year. As always, the survey contains many data points and opinions, so is well-suited to form the basis of business decisions.

Here are some of the key findings:

The economic climate

- Security professionals are concerned that the economic climate will lead to increased risk – especially from fraud and insider threats.
- They also believe that the impact of this will be mostly felt by smaller businesses and less wealthy individuals, who have less resources to protect against threats and are less able to withstand and recover from a successful attack.
- Despite this, the direct impact of the worsening economy on security departments seems to be muted – potentially because the function is seen as 'recession-proof' due to the heightened and visible risks from ransomware and geopolitical events.

Stress and working habits

- One impact of the worsening economy that professionals flagged is the effect on working hours and stress.
- Worryingly, 22% of professionals work more than the 48 hours per week mandated by the UK Government, and 8% work more than 55 hours which, according to the World Health Organisation, marks the boundary between safe and unsafe working hours.
- Asked what keeps them awake at night, the two main sources of stress for cyber professionals are day-to-day stress/workload (identified by 50%) and suffering a cyber attack (32%).

Industry and careers

- Despite the economic climate, professionals are still positive about the industry and their opportunities – almost 80% say they have 'good' or 'excellent' career prospects, and more than 84% say the industry is 'growing' or 'booming'.
- There is also notable growth in the number of cyber security professionals with detailed career plans – suggesting most have long-term ambitions and their employers are building more robust arrangements to support development.
- The reasons people leaving jobs have changed since 2022. In particular, a poor working environment – whether through poor management, unsatisfying work, or a bad atmosphere between colleagues – is an increasingly common factor.

Threats and skills

- Respondents agree that the greatest challenges in security come from people first, then processes, then technology.
- They also agree with the common factors behind a good response to a security breach: open, consistent communications and rapid response.
- Finally, respondents agree on the most important skills to deal with cyber threats: analytical and problem-solving skills, followed by communication, then technical skills. The number identifying management skills is rising, but they are still in a very small minority.

> Asked **what keeps them awake at night**, the two main sources of stress for cyber professionals are day-to-day stress/workload **(50%)** and suffering a cyber attack **(32%)**.

Respondent Demographics

The age of survey respondents

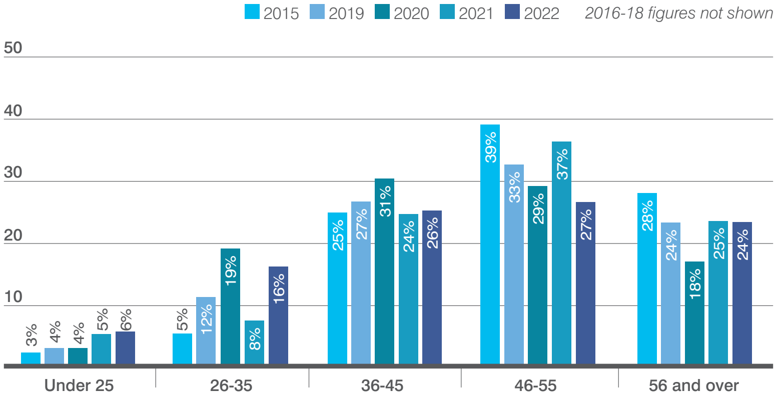


Figure 1 – Age group (%)

This year, it's noticeable that the reported ages of our respondents are back to where they were a few years ago – at least in the 36-45 and 56+ cohorts – compared to 2020's results, where we saw a greater proportion of younger respondents.

However, other cohorts have remained steady, and it will be interesting to see how this changes in the years to come. It does suggest that the 2020 result was not simply a 'blip'. It is also good to see even a small rise in younger members of the profession, representing success in our collective ongoing efforts to attract new recruits.

This year's breakdown by age is also particularly interesting, as most of the cohort from our very first survey has moved up a whole age bracket since the survey first began.

Gender balance

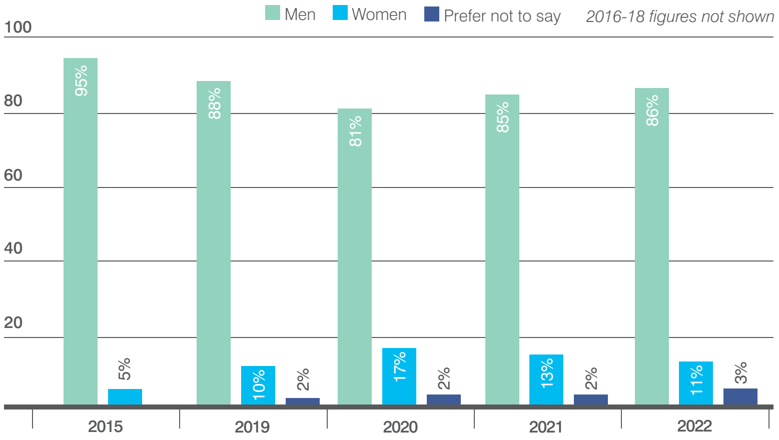


Figure 2 – Gender (%)

On average, the ratio of male to female members has improved overall since 2015. However, it's clear there is still a long way to go to achieving equality – not only because the proportion of women in the gender mix remains very small, but also because the number does not seem to show any further improvement since 2020, it has actually fallen since then.

Nobody expects the gender balance to be an overnight change, but we look forward to seeing more positive progress in years to come.

Ethnic group

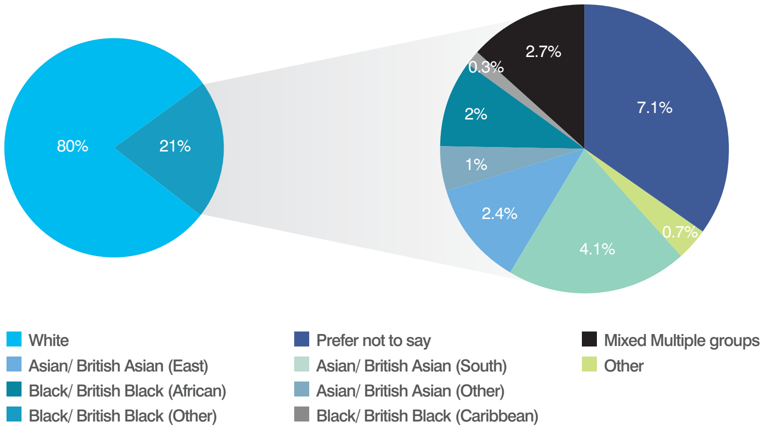


Figure 3 – Ethnic Group (%)

The ethnic diversity in the profession is a mixed picture. We see almost 80% reporting as white, which is close to the 82% reported in the 2021 census. However, there is clearly more to do to encourage a more diverse range of backgrounds to enter the security profession.

It may still be too early to tell how these initiatives are going, but non-white members are clearly split across multiple ethnic groups, which is an encouraging sign.

We will continue to pay attention to our sampling for future surveys to ensure the broadest mix of respondents that we can, and as now seek to do our part to increase diversity.

Level of education

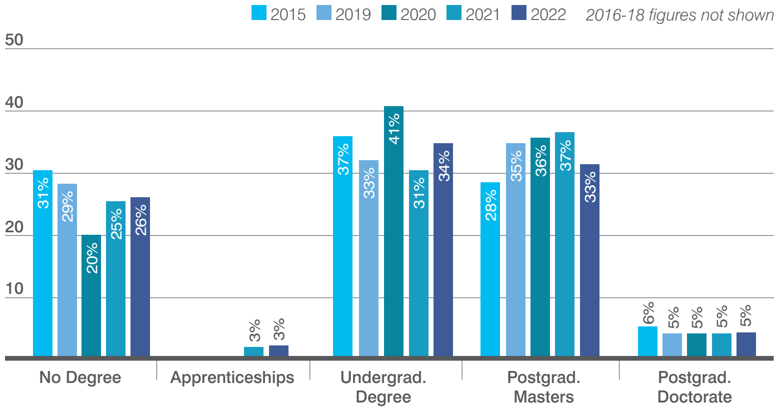


Figure 4 - Educational background

Last year, we were able to add apprenticeships to our question about the level of education of our respondents. In this second year, the numbers seem to be consistent, but it is too early to make any firm conclusions.

In other results, we're now confident that the high proportion of undergraduates recorded in 2020 was an anomaly – while numbers have increased since last year, the increase is within a reasonable margin of error.

Similarly, the drop in professionals with master's degrees looks significant, but may simply be due to this year's sample of respondents.

... the drop in professionals with master's degrees **looks significant**, but may simply be due to this year's sample of respondents.

Membership status

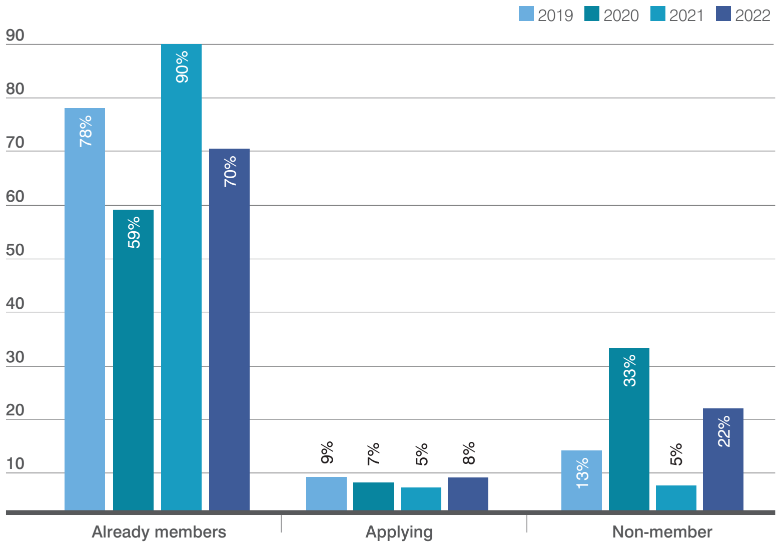
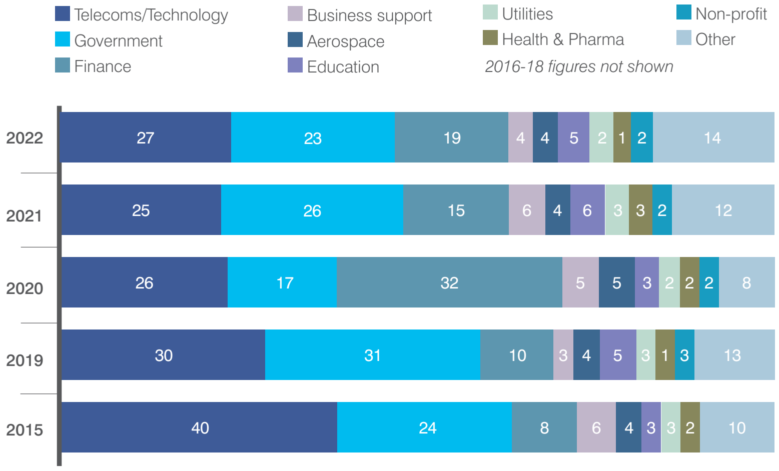


Figure 5 - Membership status of respondents

Since 2019, the survey has asked those responding whether or not they are CIISec members. This year has the second lowest number of member respondents, apart from 2020.

This does not correlate to growth (or decline) of membership numbers, and the results should be read with this in mind. It is more reflective that the survey responses have come from a wider cohort of the profession that just those with whom CIISec has a direct relationship. As the survey is not a "member survey" this is encouraging – its profile as a worthwhile research project is growing.

Sector



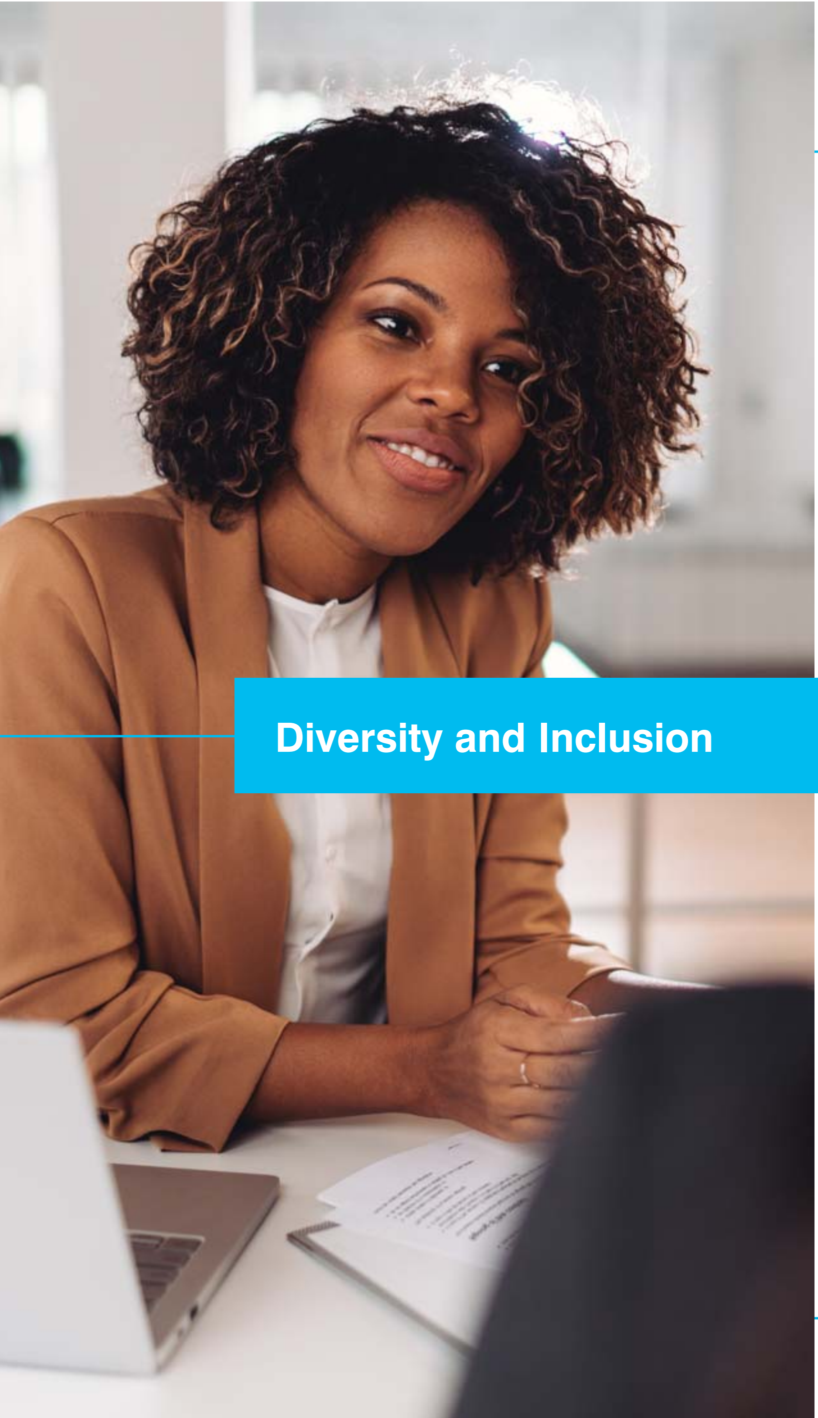
2016-18 figures not shown

Figure 6 - What sectors do respondents work in?

Although the top five industry sectors our respondents belong to remain similar, it is interesting to see the changes in proportions since our first survey.

In particular, the split of people across the top three sectors has changed, with Finance having a steadily larger cohort (especially in 2020), and Government and Telecoms / Technology challenging each other for the number one position every year.

Also worthy of note, is that the proportion of respondents in Education has, aside from 2020, remained remarkably consistent – and at a higher level than Aerospace and comparable with the numbers of people working in the Business Support sector.



Diversity and Inclusion

Encouraging diversity

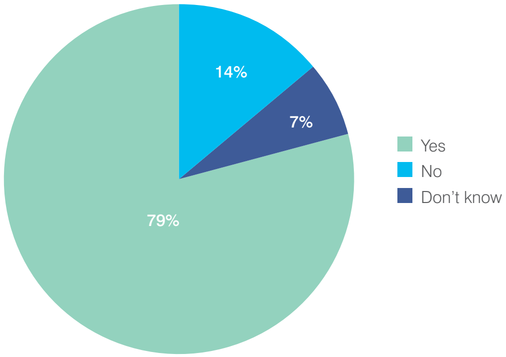


Figure 7 – Respondents' views on whether their organisation is doing enough to encourage diversity

In last year's survey, we asked about diversity and inclusion, using respondents' experiences to get a broad picture of the profession. This year we focused more on how respondents believe the industry is performing, and what it can do to improve diversity.

In particular, we can see that the majority of respondents think the industry is doing enough to encourage diversity. However, we should also bear in mind the makeup of respondents themselves. It may be that a largely white, male sample (as per the results above) is less aware of the need for diversity and what that may entail.

For similar reasons, we're not surprised to see a relatively large number of people responding 'don't know' to this question. Those without direct experience may not feel comfortable answering one way or the other.

Barriers to diversity

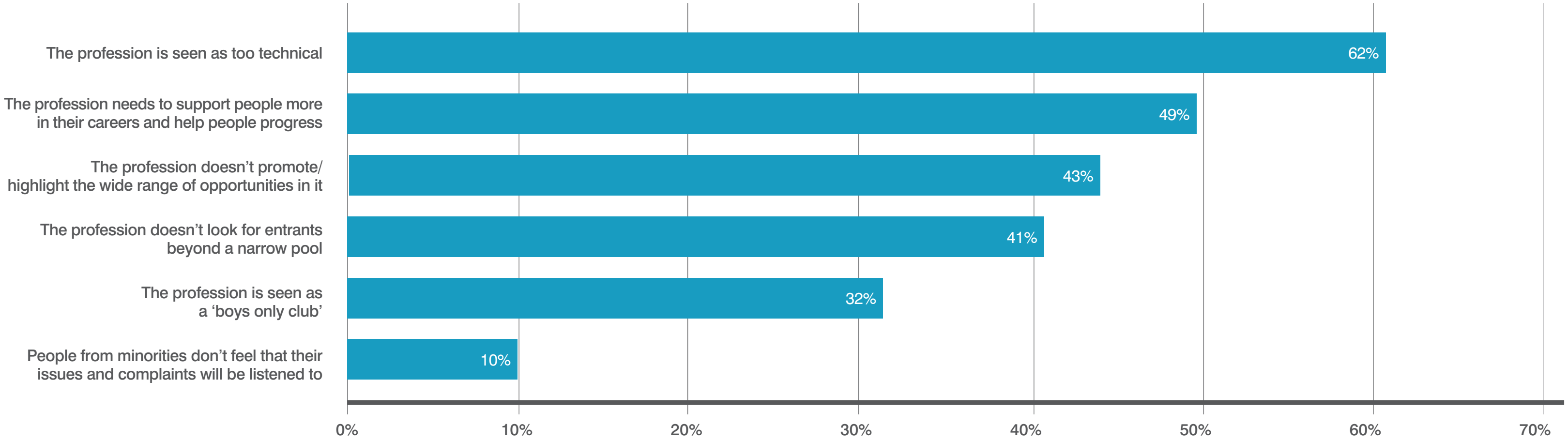


Figure 8 – Perceived barriers to the profession being more diverse

We also sought views on what the profession could do to improve diversity. So, we added questions to our survey about what barriers respondents saw to making it more diverse.

Primarily, it's clear that the profession needs to show the wide variety of roles and opportunities available – that cyber security isn't a purely technical discipline but has opportunities for people from all backgrounds.

In addition, we asked what CIISec itself could do to increase diversity. By far the most common answers were emphasising the range of opportunities available and reaching out to potential industry entrants at a younger age, ideally in schools.

> Primarily, it's clear that the profession needs to show the wide variety of roles and opportunities available – that cyber security isn't a purely technical discipline but has **opportunities for people from all backgrounds**.

Industry Trends

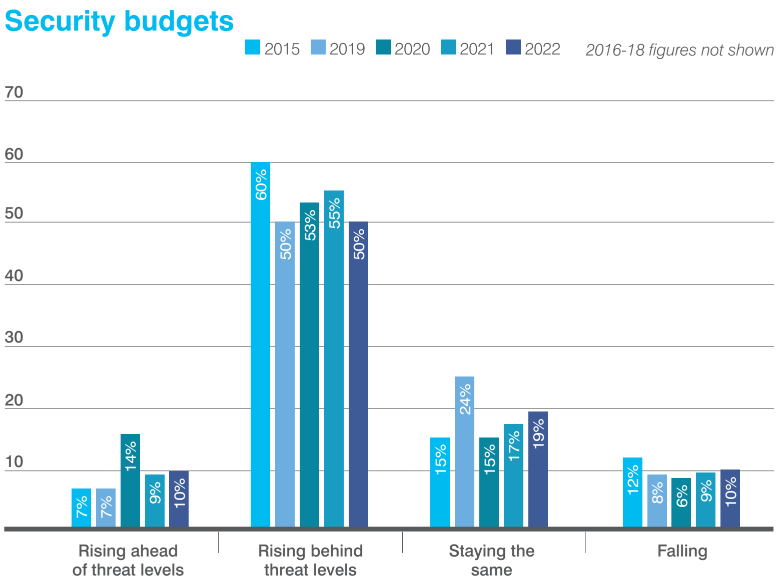


Figure 9 - How are security budgets changing? ("Don't knows" omitted, hence percentages don't add up to 100)

Moving to look at industry trends, there seems to have been little movement in respondents' views of how security budgets are changing since last year's survey.

This might be seen as a positive, in that the impact of the economic crisis hasn't yet hit the security department. After all, cyber security is a critical part of business survival, despite often being seen as a cost. However, all but 10% of respondents still say that budgets are, at best, rising behind threat levels. This is clearly cause for concern.

As we will see later in the report, the cost of living and economic crises are creating new or increased challenges for security teams, and budgets that are already behind threat levels will suddenly become extremely stretched when these new threats really hit home.

Protecting and recovering from cyber attacks

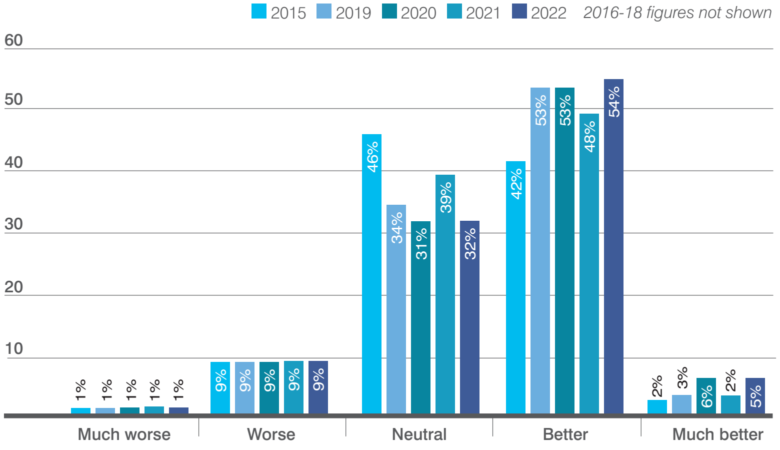


Figure 10 - Is the profession getting better or worse at defending systems?

Dealing with failures, breaches and incidents

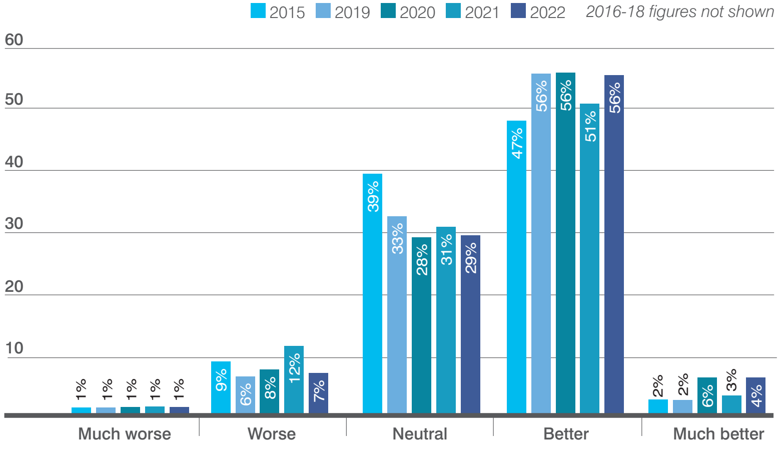


Figure 11 - Is the profession getting better or worse at handling incidents?

> ...the cost of living and economic crises are creating **new or increased challenges for security teams**, and budgets that are already behind threat levels will suddenly become extremely stretched when these new threats really hit home

These perennial twin questions ask how we are improving as a profession.

They look at how we are performing at defending systems from attack (Figure 10) and at dealing with incidents when defences fail (Figure 11).

Overall, the trend for both appears to be positive – following a slight reversion last year, there are fewer respondents giving 'worse' or 'neutral' answers, and more giving 'better' and 'much better'.

In a perfect world we would see a slow-but-steady improvement as the industry adapts to new challenges, uses new tools and techniques to combat threats, and welcomes fresh skills.

Each new breach provides opportunities for other organisations to learn lessons (as we always seem to do) and as regulations tighten, the profession should get better at detecting and preventing more attacks and handle the ones that do elude us better.

Breaches

Asking about memorable breaches

Historically, we have asked respondents to identify their most memorable or noteworthy breaches from the past year. But while this was interesting reading, it was hard data to analyse and draw conclusions from as:

- Individual definitions of 'memorable' are highly subjective.
- A breach could be memorable in one year even if it had occurred previously (e.g. due to action from regulators or new findings).
- The data contained a combination of specific incidents and more generic types of attack.

Since 2020/21, we have instead asked which breaches were handled well or badly, and why. The aim being to get a more nuanced understanding and usable results.

In this third year of our new approach, we have seen an increase in more useful insights into past breaches – not only in terms of which attracted the most attention, but what factors are most common in whether a breach is handled well or badly.

Conclusions – how to handle breaches

Our overall view? The results show that there are key similarities across all the breaches that were handled well, including:

- Transparency and rapid clear communication are consistent factors amongst organisations thought to have handled a breach well.
- Speed of response is also critical – with organisations having solid, comprehensive incident management plans in place.

In addition, respondents note that following established best practice, which can prevent simple mistakes (and possibly the most embarrassing data breaches) is also important. Some issues are unavoidable, but if the industry can collaborate and share information and best practice, it can see the benefits.

Breaches that were handled WELL

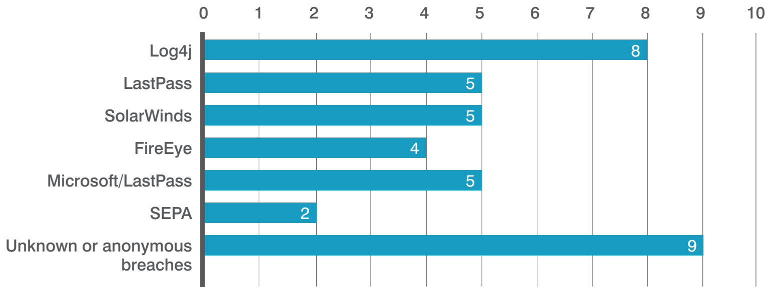


Figure 12 - Summarised – Breaches handled well

As with previous years, we've seen several individual breaches referenced, both in terms of specific organisations, and larger attacks. Figure 12 summarises all breaches that were referenced more than once – and in general, Log4j received the most praise for the response to the issues that arose.

It's also worth noting that a significant number of respondents stated that the best-handled breaches are those you never hear about, because they are solved quickly and do not attract publicity.

We have included these responses in the chart – taken as a whole, they actually represent the largest cohort.

Other cases that respondents commended were (in alphabetical order): Cayman National Bank, CD Projekt Red, Cloudflare, Facebook, Harris Federation Schools, the Irish Health Service, LinkedIn Smart Link, Maersk, Medibank, Microsoft's Exchange 2021 exploit, Mimecast, Okta, Plex, Red Cross, Royal Mail, SCCB, South Staffordshire Water, Ukraine's response to Russian attacks, WannaCry and Zoom's security improvements.

... a significant number of respondents stated that the best-handled breaches are those you never hear about, **because they are solved quickly and do not attract publicity**.

Reasons breaches were handled WELL

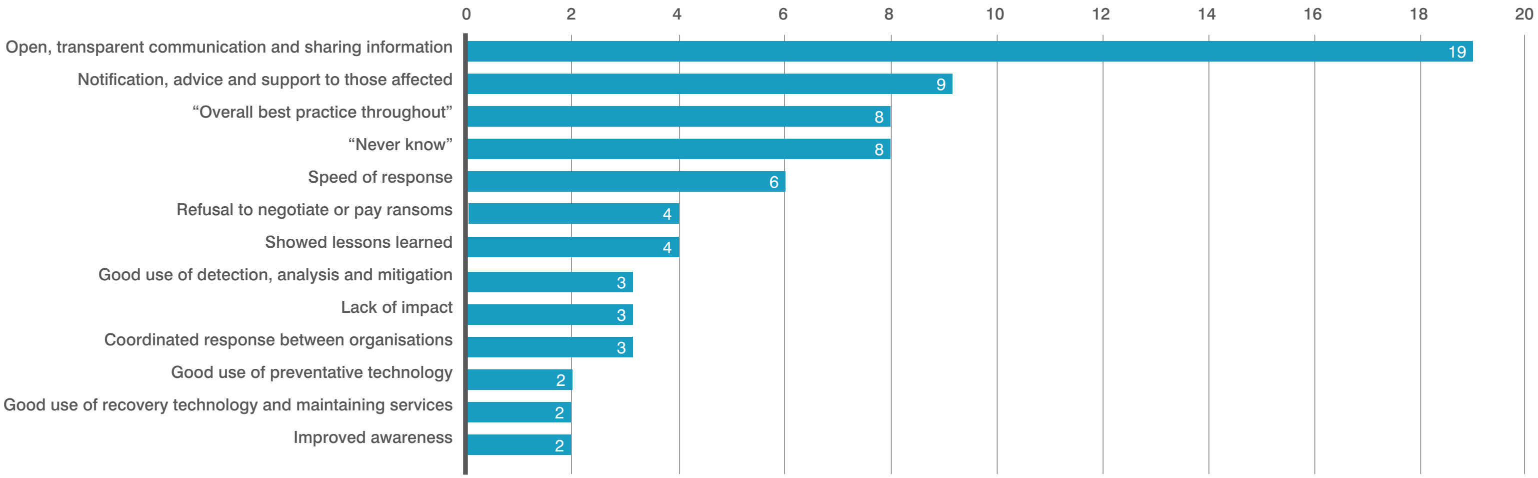


Figure 13 - Summarised – Reasons given for breaches being handled well

As well as identifying the breaches that were well handled, we also wanted to dig into more detail around why they had achieved this perception.

Note that where a breach was listed as having multiple reasons for positive handling, we've included all these in Figure 13.

It's clear that by far the most important ingredient in a good response is communication – being open, responsive, and keeping those affected notified is considered key.

Several factors that didn't make the table – often because they were mentioned once – included the attackers themselves seeing consequences, such as prison time; and the organisation's response influencing later best practices and behaviours.

> It's clear that by far the most important ingredient in a good response is communication – **being open, responsive, and keeping those affected notified is considered key**.

Breaches that were handled BADLY

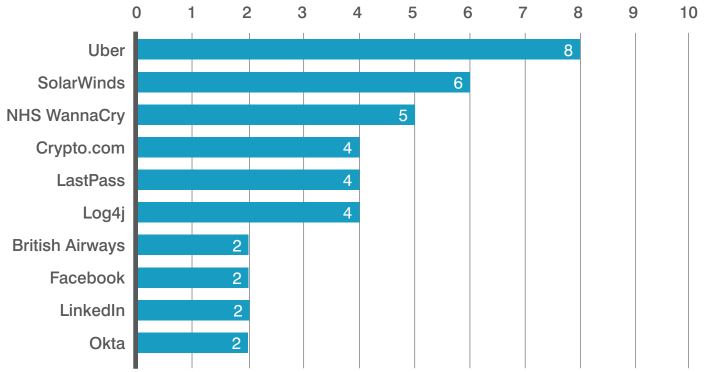


Figure 14 – Summarised – Breaches handled badly

Many breaches were considered to have been handled badly, and to learn lessons we need to look at these alongside those handled well.

It's worth noting that several breaches e.g. Log4j were listed as being handled both well and badly by different respondents, showing that perception of a good or bad response isn't always consistent. For instance, one respondent might praise an organisation's rapid reaction to and clear communication about a breach, while another might lament the lack of security policies that led to the breach in the first place.

There were also a larger number of breaches mentioned by more than one respondent. This suggests that there is more consensus in the industry around what people believe represents a 'bad' breach response.

Other breaches mentioned include: Colonial Pipeline, Costa Rica Government, Davies Group, Electronic Arts, Flexbooker, Garmin, Kaseya, KP Snacks, Marriott, Microsoft BlueBleed and Exchange, the Montenegro Government, Monzo, Open SSL's vulnerability, Optus Telecom, SeeTickets, Sky, Spar, Thales, T-Mobile, Toll Group, Viasat, Ward Hadaway and Yahoo.

Reasons breaches were handled BADLY

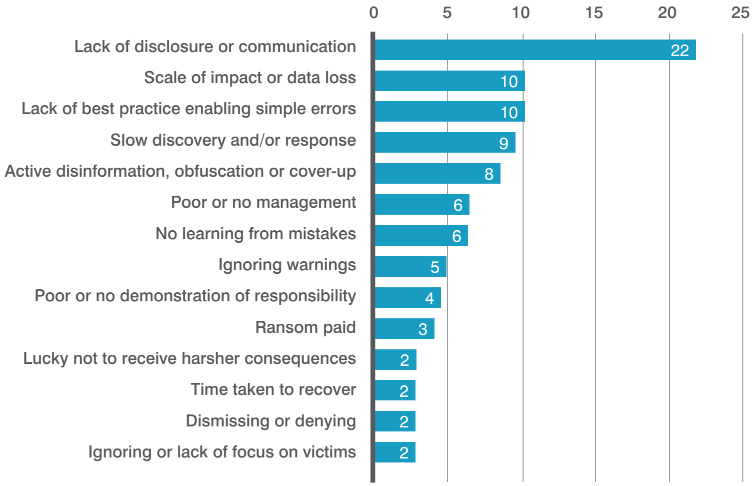


Figure 15 – Summarised – Reasons given for breaches being handled badly

As with well-handled breaches, we wanted to dig into the reasons why people consider these breaches to have been handled badly. Figure 15 shows the reasons that were mentioned more than once, and where multiple reasons were given for a single breach, all of these are included. It will come as no surprise that there's a direct overlap between the reasons people considered one breach to be handled well, and another badly. Communication and following best practices are in the top three in both charts: well done in one, done badly or not at all in the other.

Other reasons given were a lack of training, poor or no incentives to stop using the service and fix the issue, and organisations falling victim to a known threat.

As an aside, if organisations were to improve on some of these factors, there would be a knock-on effect on others. For instance, following best practices would reduce the scale of an attack, which is another factor that affects people's view of a breach.

Innovations in cyber security

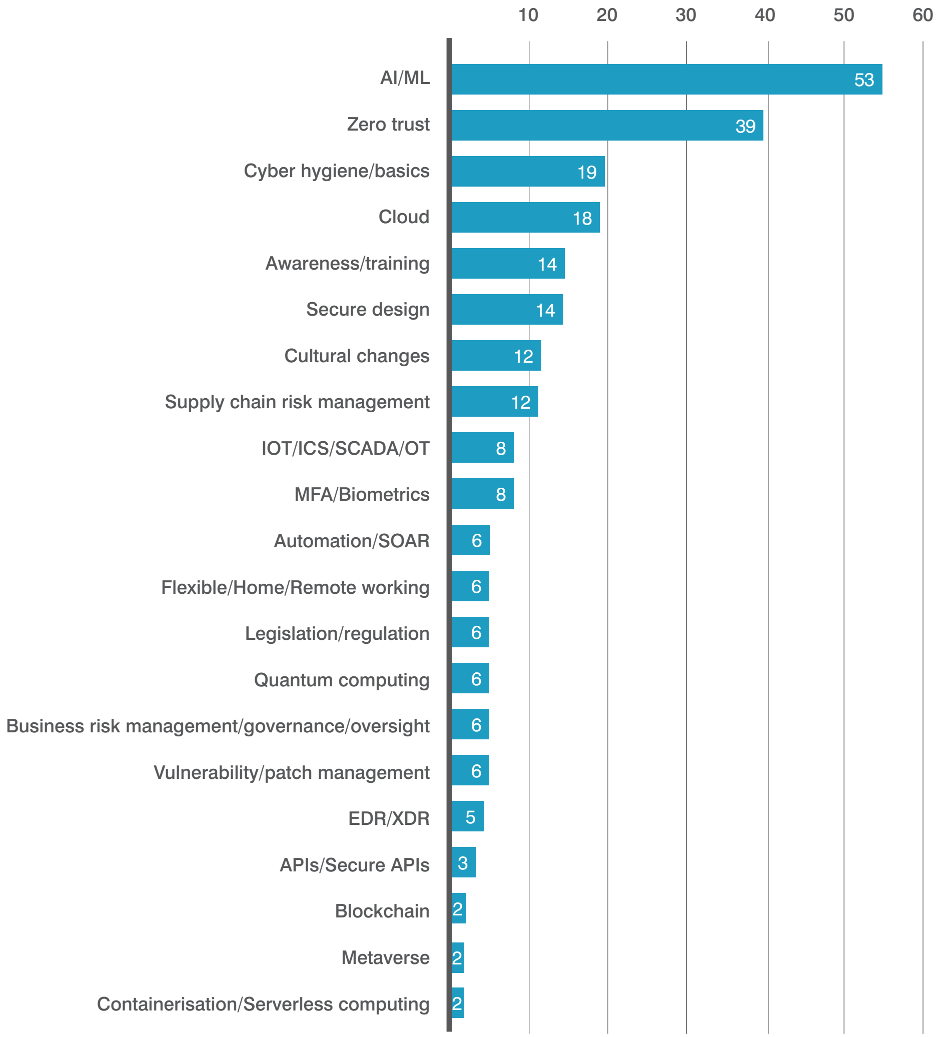


Figure 16 - What innovation will have the biggest effect on cyber security? 2022/2023 – number of mentions (responses with multiple mentions only)

With so much change and innovation in the cyber security sector, we're always interested to see what our respondents view as the most impactful.

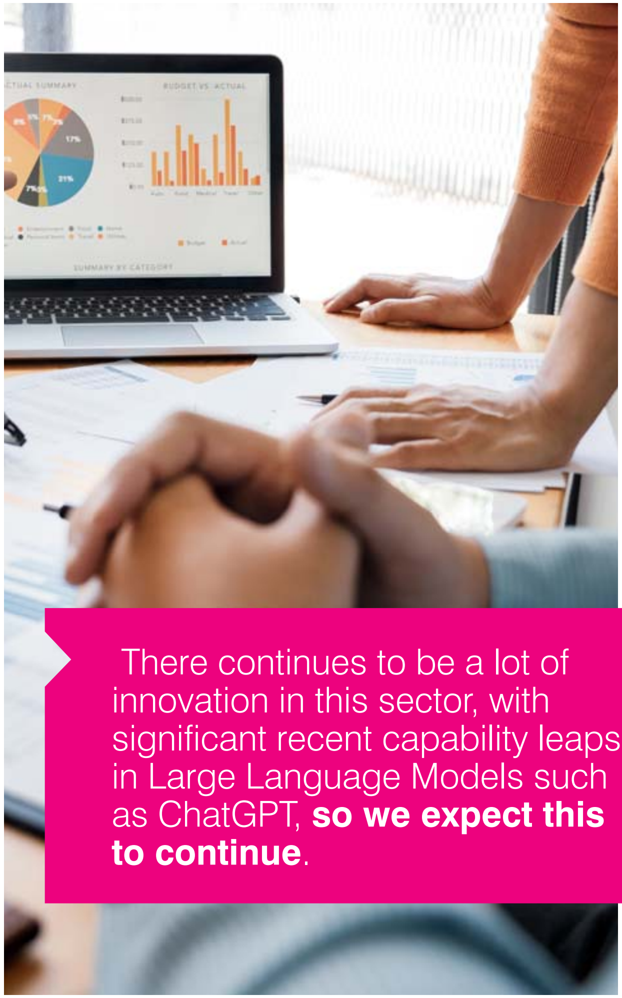
Unsurprisingly, artificial intelligence (AI) / machine learning (ML) holds the top place, where it has consistently been for the last few years. There continues to be a lot of innovation in this sector, with significant recent capability leaps in Large Language Models such as ChatGPT, so we expect this to continue.

But apart from AI, it's notable that many of the other higher-placed innovations are not so much technologies, but processes and approaches. There are two likely reasons for this:

- Our survey respondents place significant importance on people as the greatest security challenge (and we cover this later in the report).
- Security needs change, as the use and importance of specific technologies fluctuates, but best practice and awareness can provide a consistent level of protection regardless of the current technology favourites.

We can see that remote, flexible and home working remains low in expected impact again this year, in line with the fact that the innovations needed to enable remote and hybrid working in 2020 are in place and seen as normal.

Note that Figure 16 only shows those areas of innovation that were identified by multiple respondents. SASE and cyber insurance were only chosen by one person each, while – despite being presented as options – no respondents chose SIEM / Security Analytics or 5G/Networking.



There continues to be a lot of innovation in this sector, with significant recent capability leaps in Large Language Models such as ChatGPT, **so we expect this to continue**.

People, process and technology

What is the biggest challenge we face in security?

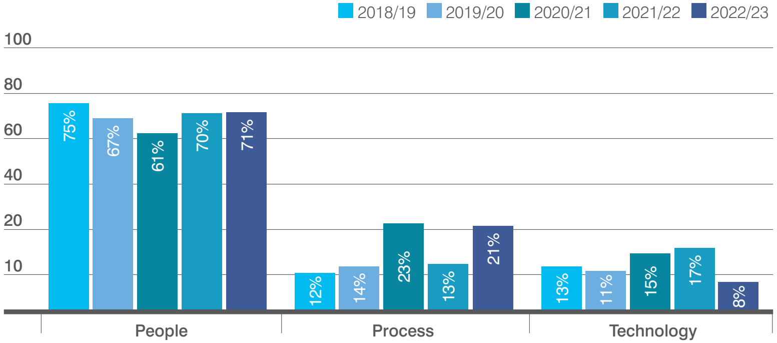


Figure 17 - Is the biggest challenge people, processes or technology? (Note percentages do not always add to 100 as skipped responses are omitted).

Every year we ask our survey respondents where they feel the biggest challenge for security comes from: people, processes or technology, and every year, the area of greatest challenge is identified as people.

This won't come as a surprise to anyone – even as individuals, we're faced with an increasing number of person-based security attacks, from targeting with scam links, to full-blown corporate phishing attempts. It's how some of the biggest breaches of last year were started.

This year, we're also seeing the lowest figure for 'Technology' since the survey began. With all this taken together, it's clear that investing in skills foremost, followed by processes and best practices that will minimise threats, are the best way to reduce risk.

Skills, resources, jobs and the market

Skills and resources

A shortage of quantity (resources) or quality (skills)?

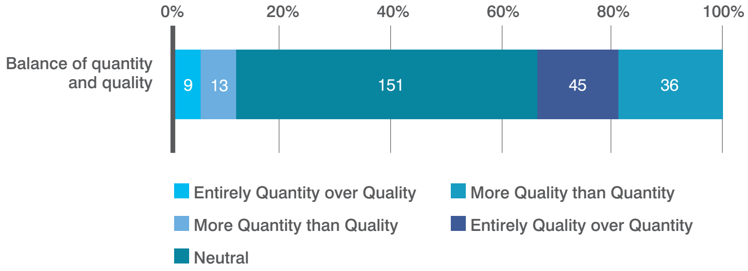


Figure 18 - Is the industry short of resources or skills?

A shortage of experienced personnel or new entrants?

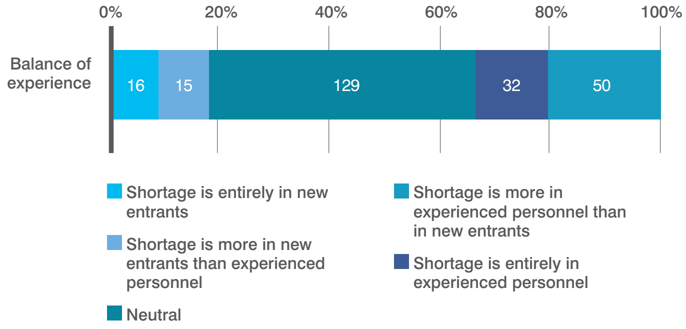


Figure 19 - Is the industry short of experience or new blood?

As in our previous surveys, we wanted to investigate where respondents think the (undeniable) cyber skills shortage originates.

Is it a shortage of people, or a shortage of the specific skills needed to perform tasks? Does the profession need more experienced, skilled personnel, or more fresh entrants?

Unlike previous years, we have taken a less binary view of the data. Compared to last year there has been little change, but splitting by degrees allows a more nuanced insight.

The results? We can see that while most respondents are neutral on both subjects, there is a clear trend: far more respondents believe that the industry is facing a shortage of skills, rather than people, and they believe this needs to be remedied with more skilled personnel than simply fresh recruits.

In practice, this means that attracting people with relevant experience, but from different backgrounds, will be crucial.

Is it a shortage of people, or a shortage of the specific skills needed to perform tasks? **Does the profession need more experienced, skilled personnel, or more fresh entrants?**

Job prospects

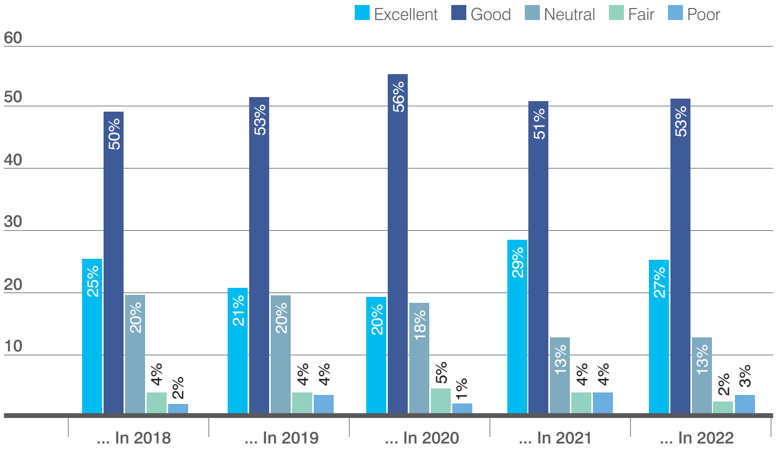


Figure 20 - Current job prospects...

Once again, the outlook on job prospects remains positive year-on-year: the relatively high number of ‘Excellent’ responses from 2021 continued into 2022.

This is despite economic concerns that would have been on respondents’ minds, and it points to cyber being to some extent a recession-proof business function. Regardless of the economic climate, organisations always need to reduce risk and protect themselves from threats that prove catastrophic if not identified and addressed.

The growth of the security market

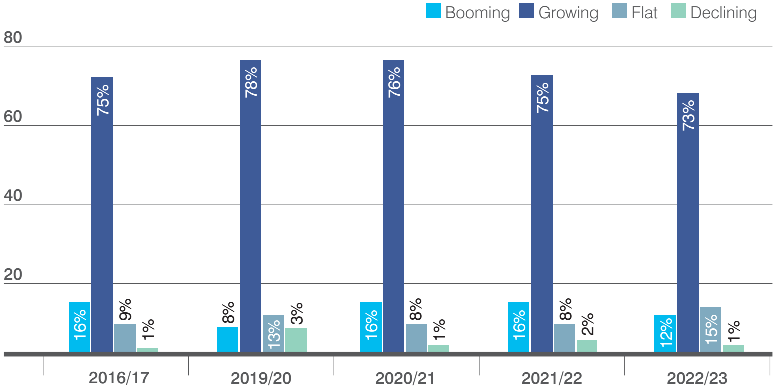
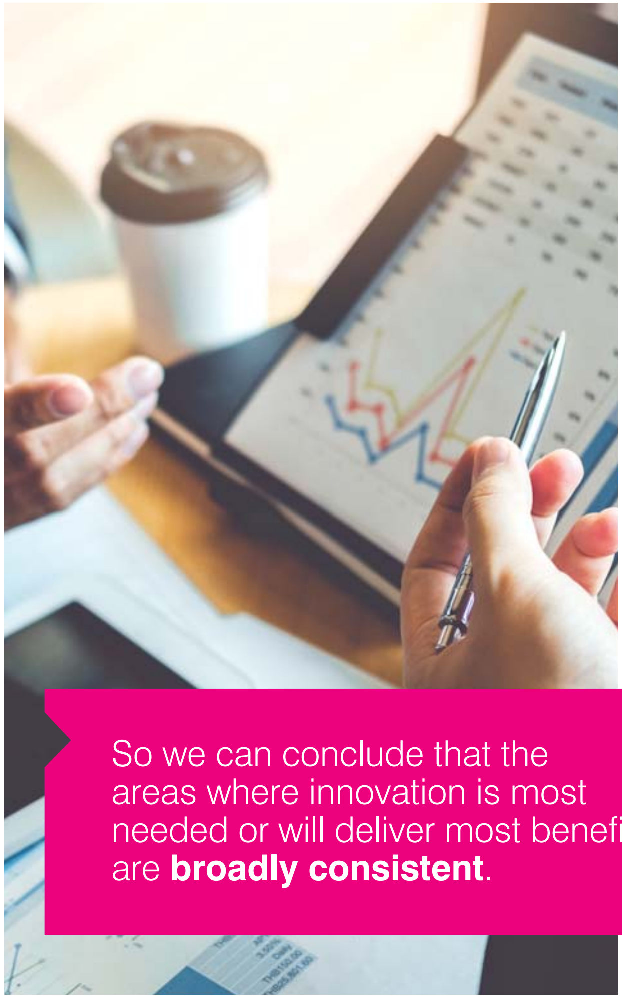


Figure 21 - How is the security market changing?

Similarly, our respondents' view of the security market as a whole is broadly consistent with previous years. While the number saying the market is 'growing' is lower than other years, it is only by two percentage points.

In comparison, almost double the proportion of respondents in the two previous surveys have said that the market is 'flat' – even more than in 2019/20. However, a larger proportion than that year still believe it is 'booming'.

It will be interesting to see if these proportions return to the norm next year, or whether parts of the industry are in for an extended period of low or no growth.



So we can conclude that the areas where innovation is most needed or will deliver most benefit are **broadly consistent**.

Learning, development and career progression

Training and development

This shows people’s preferences for how they grow, learn and develop:

	2018	2019	2020	2021	2022	5-year Average
On-the-job learning	65%	66%	75%	63%	75%	69%
Attending courses	59%	70%	55%	59%	56%	60%
Events/seminars	55%	45%	48%	51%	48%	49%
Reading	54%	48%	46%	44%	46%	48%
Online courses	32%	35%	46%	45%	43%	40%
1-to-1 mentoring	21%	27%	33%	30%	39%	30%
Conferences / shows	25%	20%	23%	19%	19%	21%

Table 1 - How do people prefer to learn, grow and develop? (Multiple answers accepted)

On-the-job learning remains the number one preference for training. The percentage point value has even grown, at the slight expense of online courses and attending events.

It makes clear that the most effective way for employees to learn is still on the job, followed in second place by properly designed, accredited courses.

The popularity of online courses has fallen a little, perhaps as employees return to in-person training in the wake of the pandemic, but it is still notably higher than in the 2010s.

Similarly, one-to-one mentoring is showing a consistent rise – and as a good complement to on-the-job learning, this is encouraging.

The most important skills

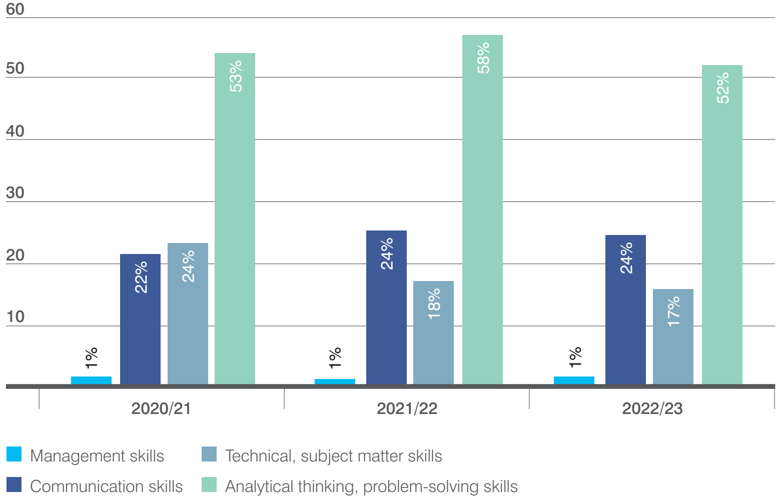


Figure 22 – What are the most important skills for people entering the profession?

It's only a few years since we started asking respondents what families of skill are most important in cyber security: analytical and problem-solving skills needed to address potential risks; technical and subject matter skills; the communication skills needed to cooperate with the security team and the wider business; or the management skills needed to support the business and team.

As we can see, the responses have remained reasonably consistent year-on-year. Analytical and problem-solving skills are seen as by far the most important, although there is growing recognition of communication skills above technical skills.

Also worth noting is that most of our respondents still do not value management skills. This may change as security becomes more of a strategic business function but, at present, the figure remains very low. The results distribution for this question may also change as the industry attracts more new entrants from different backgrounds and who, as a result, may value different skill areas more highly.

Career planning

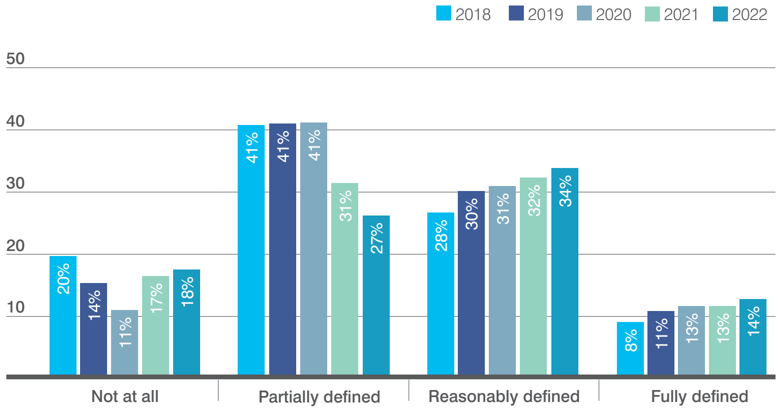


Figure 23 – Do you have a defined career plan?

A defined career plan is an important asset for people in any industry, including security professionals. Knowing your end goal, and the skills you need to achieve it, can help people achieve their full potential.

From our survey, we can see that there has been a steady growth in the proportion of respondents who have a career plan in place that is reasonably, or fully, defined. Almost half (48%) have now met this goal.

Interestingly, the number of respondents with no defined plan has crept back up almost to its previous high, after dropping to half only a few years later, in 2020.

What we seem to be seeing, is an increasingly all-or-nothing approach to career planning, with fewer people than ever having only a partially defined plan.

Growing your security team - recruitment and retention

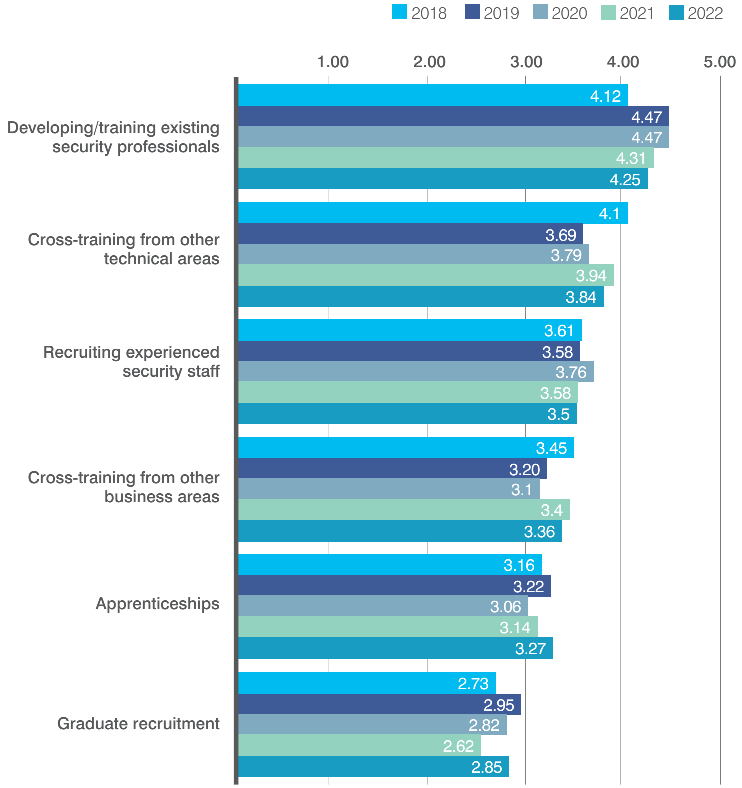


Figure 24 - How should businesses grow or develop their security capabilities?

This is a question we ask every year – how do you, as a security professional, feel organisations should best grow their security capability?

The leading answer is by developing and training existing security professionals. As we can see from the results (showing as weightings) respondents have been generally consistent over the years about this having the greatest impact.

However, while graduate recruitment is still the least commonly chosen option, it has noticeably become more popular since 2018 – so there is increasing recognition that the industry needs fresh blood.

As we can see from the results (showing as weightings) respondents have been **generally consistent over the years** about this having the greatest impact.

Security and career motivations

To aid corporate members and those seeking to attract and retain security staff, we ask survey respondents what attracts people to jobs and causes them to leave.

Top 5 factors that attract people to TAKE security jobs	Position 2021/22	Position 2022/23
Money/remuneration	1	→ 1 (7.65)
Opportunity/scope for progression	2	→ 2 (6.95)
Variety of work	3	→ 3 (6.10)
Training opportunities	4	→ 4 (5.10)
Autonomy/scope for initiative	5	→ 5 (4.58)

Table 2 – What attracts people to take new jobs?

Top 5 factors that cause people to LEAVE security jobs	Position 2021/22	Position 2022/23
Money/remuneration	2	↑ 1 (7.02)
Opportunity/scope for progression	1	↓ 2 (6.85)
Bad/ineffectual management	3	→ 3 (6.80)
Boring work/lack of variety	5	↑ 4 (4.88)
Atmosphere or issues with teams/ colleagues	N/A	↑ 5 (4.88)

Table 3 – What makes people leave jobs?

The factors that cause people to take security jobs tend to remain consistent year-on-year and in the same order for the last two years.

There has been a notable change in the factors that cause people to leave roles. Remuneration is more important, now in the top slot, while opportunities for progression have fallen.

The work environment is increasingly important, with boring or monotonous work, and a poor atmosphere or other issues with colleagues (position 5) causing people to leave. Bad or ineffectual management (position 3) also is a factor and forms part of this environment.

Interestingly, last year's fourth-most-common reason for leaving – insufficient training – has dropped out of the top five completely this year.

There has been a notable change in the factors that cause people to leave roles. **Remuneration is more important**, now in the top slot, while opportunities for progression have fallen.

Remuneration – Year-on-year

Once again, we have compared salary bands in two ways: year-on-year and comparing the first year of our survey (2016) with the most recent.

While the first graph gives us a more granular view, the second makes it obvious where changes are happening. In particular, the number of respondents on a mid-range (£50-75K) salary has dropped sharply, while there has been a significant climb in the two bands on either side.

Given that it is now seven years since our first survey, this suggests a natural progression of respondents – similar to the earlier question on respondents' ages. Many of those who were originally in that £50-75K band are likely to have moved to higher-paid roles, while newer entrants to the industry are still in the lower brackets.

It may also be that, with the advent of apprenticeships and greater recognition of the importance of security, there are fewer roles with this lower level of remuneration. What the statistics do tell us is that cyber security continues to be a profession that provides excellent opportunities for remuneration and advancement.

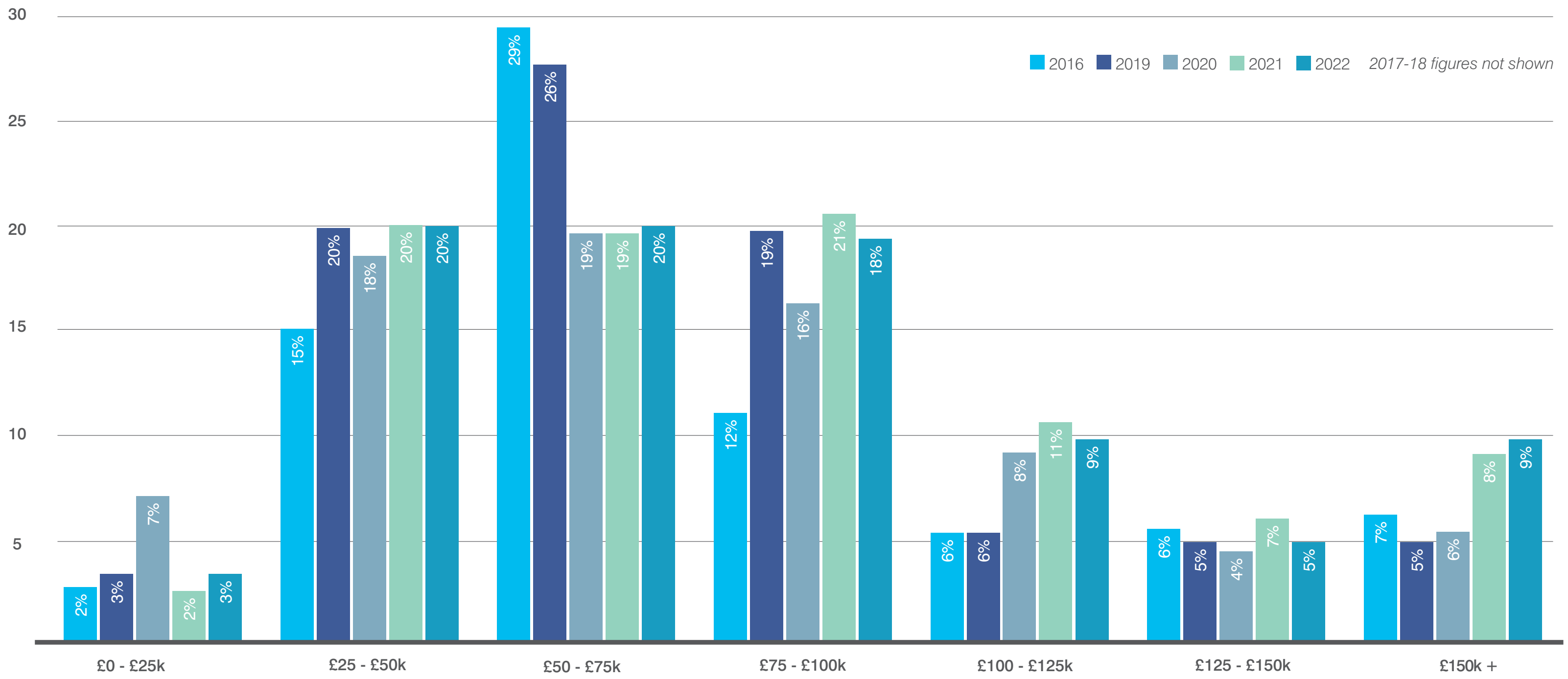


Figure 25 - Salary range – showing data back to 2016 and most recent 4 years

Remuneration – oldest and newest figures

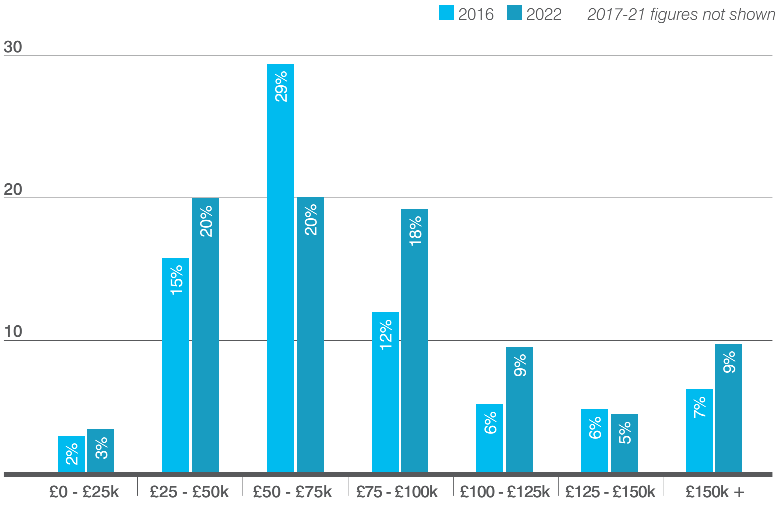


Figure 26 - Salary range – first and last years' data sets only

While the first graph gives us a more granular view, the second makes it obvious where changes are happening. In particular, **the number of respondents on a mid-range (£50-75K) salary has dropped sharply**, while there has been a significant climb in the two bands on either side.

How long do people stay in jobs?

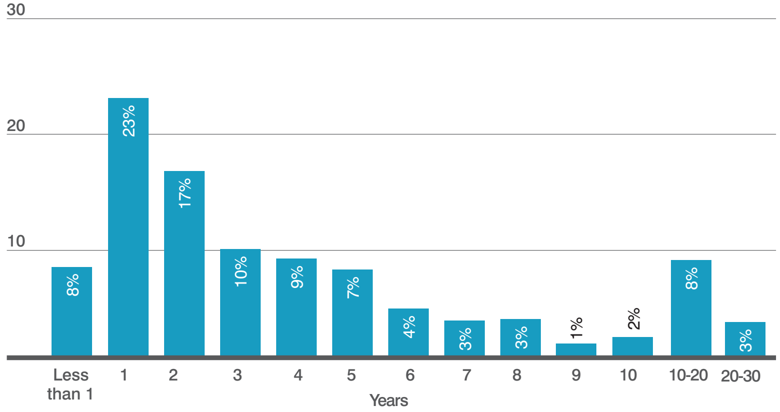


Figure 27 – How long have people been in their current job (years)

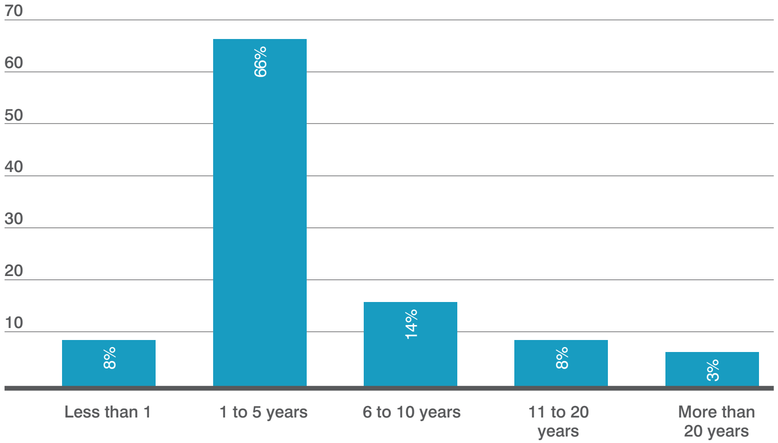


Figure 28 – How long have people been in their current job (years) – by band

To understand how long people stay in cyber security positions, we asked how long they had been in their current job.

The mean tenure has remained consistent – from 4.63 years in 2020, to 5 in 2021, to 4.69 in 2022. As you can see, most people have spent between one and five years in their current jobs – with one being the mode.

It all shows that, on average, people are still staying with their employers for long enough to reward any investment in training and progression.

What we can't tell from this data, is how uncertain economic times could affect these figures – whether from employees being more or less willing to move jobs, or from employers making redundancies in the event that security becomes less recession-proof.

One possibility is that retention will improve. No one likes taking a chance with their livelihood when living costs and mortgage payments are climbing. Next year's data may shed more of a light on this, as at the time of writing mortgage rates have reached a new high, even as utility bills are starting to fall.

Do people see themselves staying in their jobs?

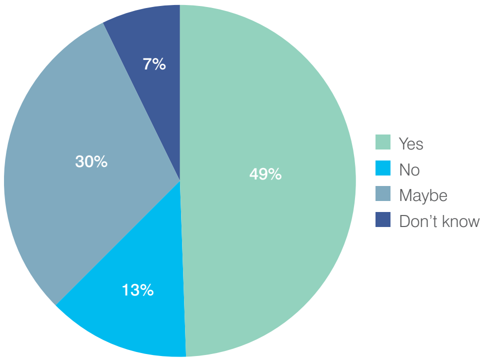


Figure 29 – Do people see themselves working for the same employer in a security role in the next two years?

This year, we also wanted to understand how likely people were to move jobs, so we asked them to talk about their plans over the next two years.

In short, the majority of respondents don't see themselves at another employer in the next two years, although a significant number are unsure.

This may be because security is a well-remunerated, interesting profession, but may also have to do with the economic uncertainty mentioned above. Revisiting this question in years to come will also help us paint a fuller picture.

How long do people stay in the security profession?

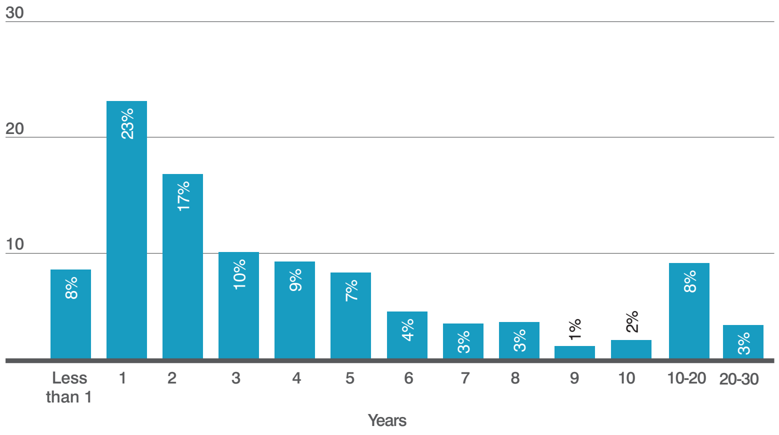


Figure 30 – How long have people worked in security (years)

Looking at the security profession as a whole, we can see it rewards long careers. On average, our respondents have been working in the profession for 15.5 years.

But it's interesting to see that the two most common career lengths are 5-9 years and, at the other end of the scale, 20-24 years.

It's also notable how many people have seen significant technology change during their time working. For instance, more than half of respondents were already working in security when the iPhone was launched in 2007.

Career stress and patterns of work

Working hours

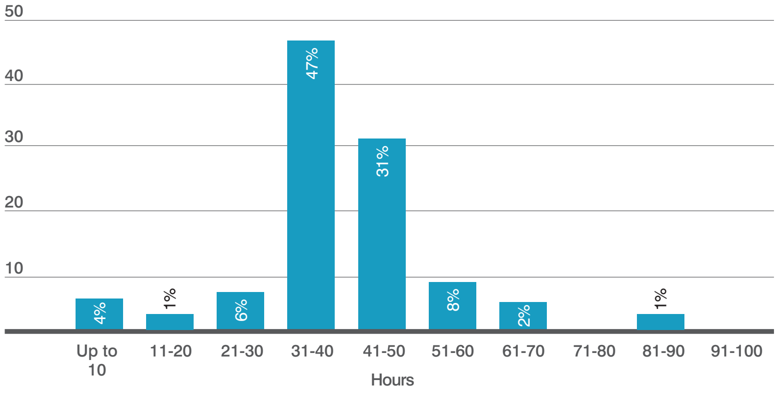


Figure 31– Weekly hours worked

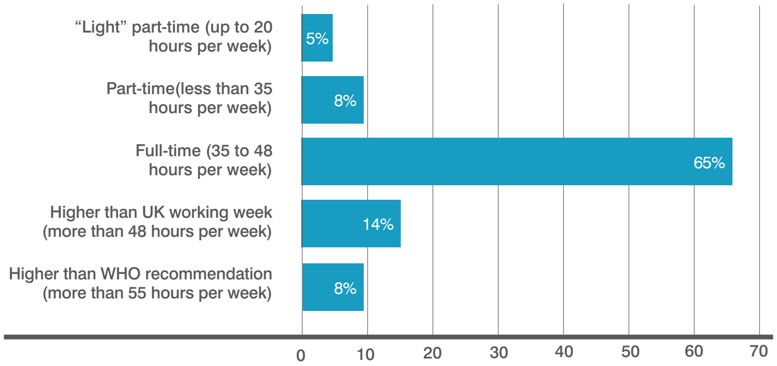


Figure 32 – Weekly hours worked by full / part-time

This is the third year that we have asked about the time cyber security professionals spend working.

Clearly, the vast majority are working full-time, i.e., between 35 and 48 hours a week, with a mean working week of 41.3 hours. This doesn't differ significantly from previous years.

But there's a significant number of professionals working part-time (i.e., below 35 hours a week), equivalent to almost 1 in 8 professionals. As many as 5% of respondents work less than 20 hours a week.

At the other end of the scale, it's concerning to see that more than a fifth (22%) of respondents are working more than the UK's mandated 48 hours a week. Most troubling, 8% say they're working more than 55 hours a week. This is above the level at which the World Health Organization claims is the upper limit to prevent harmful effects from overwork.

Employers and employees alike should pay attention to these figures and prioritise understanding whether security professionals are doing their jobs at the expense of their health.

But there's a significant number of professionals working part-time (i.e., below 35 hours a week), **equivalent to almost 1 in 8 professionals**.

Sources of stress

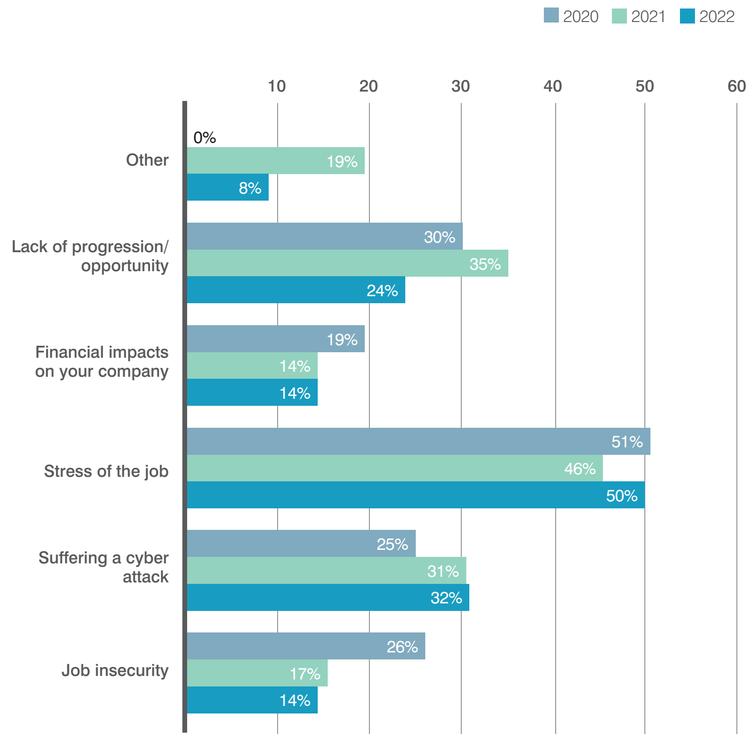


Figure 33 – What keeps you up at night? (Multiple answers allowed)

What keeps professionals up at night? Overwork may be a source of stress for cyber security employees – particularly the 22% working long hours – but we also want to explore other sources. A lucky 4% of respondents reported that nothing caused them stress.

For everyone else, the stresses that have become most common relate to the job in general – including suffering a cyber-attack. In particular, the worry around attacks seems to be showing a steady year-on-year increase, suggesting increased awareness of threats is having an equal impact on professionals' level of stress as it is their ability to cope.

Conversely, there's been a drop in the number of people worrying about a lack of career progression or opportunity. This could be because professionals currently feel better recognised and remunerated, or because they welcome a steady position in tough economic times.

One notable statistic is that, despite offering it as an option, nobody in this year's survey said the effects of the pandemic were a worry. It suggests that many respondents either believe the danger is over, or have accepted it, at least in cyber security.

> ... there's been a drop in the number of people worrying about a **lack of career progression or opportunity**.

The state of the economy

In each year's survey, we identify a theme and ask specific questions on it. This is a good way to identify current trends or to answer specific questions about aspects of the profession, the way we all work, or the challenges and events that are shaping the cyber security industry.

This year, we chose to seek views on the economy. What effects do security professionals fear? What are they seeing already? Who do they think will be most affected?

There are clear economic issues influencing our industry:

- Rising inflation is affecting costs for both businesses and employees.
- Ongoing upheaval in supply chains due to factors, such as the war in Ukraine, and the effects of climate change which is making products and services more expensive or harder to obtain.
- Businesses are expected to react quickly in uncertain marketplaces, often meaning spending more in order to succeed.
- The economic slowdown means that customers in both private and public sectors have less to spend.

As a result of these factors, there are particular risks to cyber security teams including:

- An increased threat to jobs, whether for security professionals working for vendors, or in end-user organisations.
- Less organisational resources, resulting in security teams who are stretched further and so less able to identify and react to threats.
- Organisations that are cost cutting also demanding a more rigorous approach to risk reduction – further increasing the demand on security teams.
- Individuals with financial concerns, who in themselves create a greater organisational security risk either because they are distracted by financial worries to work as effectively or carefully, or because they become open to enabling or committing cyber crime or fraud for financial gain.

Impacts of the weakened economy

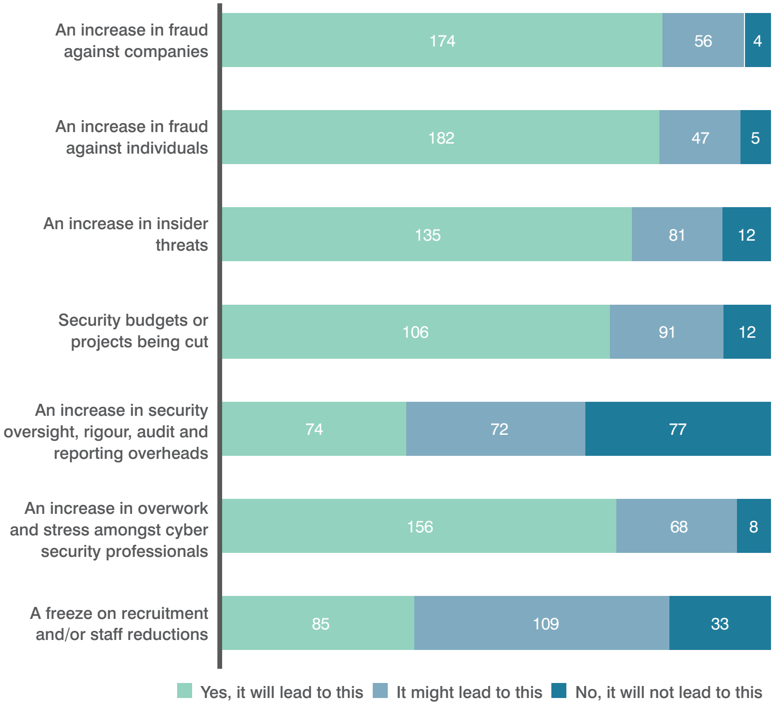


Figure 34 – Potential impacts of the current economic headwinds

We asked security professionals what they thought were the most likely consequences of a weakened economy. It's very clear that fraud, against both companies and individuals, is the threat that most concerns them.

We see this as being likely due to two issues: financially desperate individuals turning to fraud as a last resort, increasing the resources criminals have open to them; plus opportunistic fraudsters seeing this as the perfect opportunity to take advantage of individuals and organisations who are likely to also be dealing with the economic climate.

It's also a likely cause of the predicted increase in insider threats, as employees either knowingly or unknowingly allow hostile actors access.

There is clear concern about overwork and stress – understandable as security teams will need to be on the frontline of preventing fraud and insider threats, with the additional worry about their own economic circumstances.

At present, respondents have less concern around freezes in recruitment or increased security oversight, presumably as security is already seen as a crucial and to some extent recession-proof function. However, there is also currently a lot of uncertainty in these areas, so that may change.

The next question is: which of these potential impacts are we already seeing?

Current economic impacts

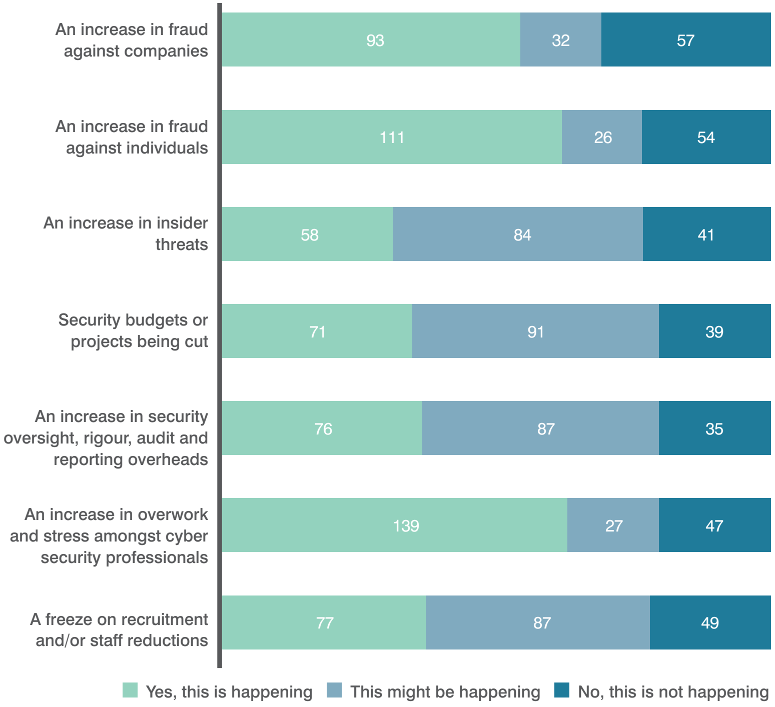


Figure 35 – What effects are respondents are already seeing?

Current economic impacts

Our survey found that cyber security professionals are already seeing the predicted increase in fraud. They're also seeing a significant increase in overwork and stress – which backs up claims about what keeps people awake at night.

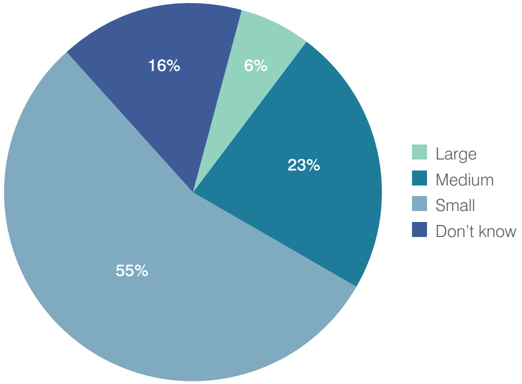
The data also shows there's still quite a lot of uncertainty in many of these areas, meaning it is quite possible that the eventual outcome will differ from the professionals' predictions.

Whether these challenges turn out to be better or worse than expected, it is essential that the industry can deal with them before they turn into real problems. For instance, security teams should be proactively given the support and training they need to reduce work pressure. Meanwhile, organisations should continue hiring new blood from all backgrounds, so that teams don't end up struggling to keep pace with all the current threats.

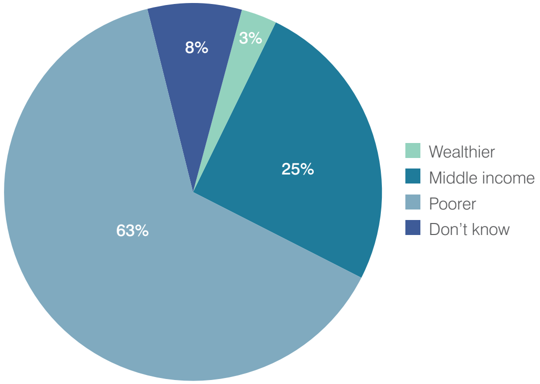
> Whether these challenges turn out to be better or worse than expected, it is essential that the industry can **deal with them before they turn into real problems**.

The victims of the economic impacts

Businesses



Individuals



Figures 36 & 37 – Who will feel the effects of the economy more acutely?

Finally, we wanted to know who will feel these economic impacts the most, both in terms of businesses and individuals.

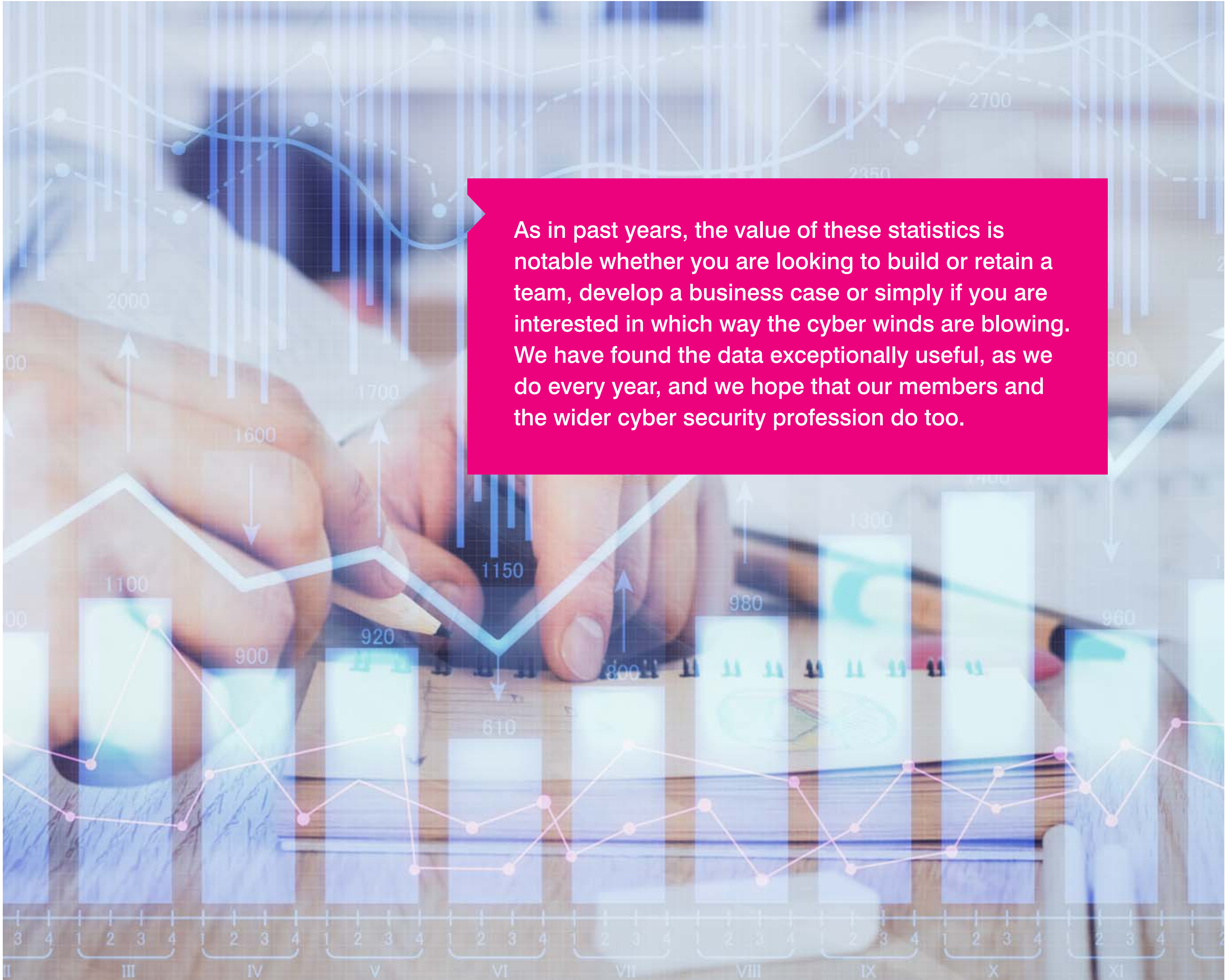
Our respondents are clear those most at risk are people and organisations that do not have the resources to protect themselves.

For instance, smaller companies may not have the resources to develop a strong security strategy that will protect them from major risks. As a result, they may not be able to absorb the damage from a major attack, so a breach that might only trouble a large business (e.g. through reputational damage or upending supply chains) could permanently cripple a smaller one.

Similarly, poorer individuals are likely to be feeling economic impacts more strongly, making them more stressed, and they may not have the training and support that those in higher-paid positions will.

What it all shows is that protecting against the economic impacts on security is a societal challenge. Like vaccination, the more people and businesses that are protected, the less opportunity there is for threats to breed or break out.

> Our respondents are clear - those most at risk are people and organisations that **do not have the resources to protect themselves**.



As in past years, the value of these statistics is notable whether you are looking to build or retain a team, develop a business case or simply if you are interested in which way the cyber winds are blowing. We have found the data exceptionally useful, as we do every year, and we hope that our members and the wider cyber security profession do too.

About The Chartered Institute of Information Security

The Chartered Institute of Information Security (CIISec) is the only pure-play cyber and information security institution to have been granted Royal Charter status and is dedicated to raising the standard of professionalism in cyber and information security.

CIISec was formed in 2006 to advance the professionalism of information security practitioners and thereby the professionalism of the industry. CIISec provides a universally-accepted focal point for the information cyber security profession, it is an independent not-for-profit body governed by its members, ensuring standards of professionalism for practitioners, qualifications, operating practices, training and individuals.

CIISec has a growing membership that represents over 15,000 individuals in the information and cyber security industry.

ciisec.org

Offenham Office
Haddonsacre Station Road
Offenham WR11 8JJ

London Office
CAN Mezzanine Borough 7-14 Great Dover Street
London SE1 4YR

Chartered Institute of
Information Security