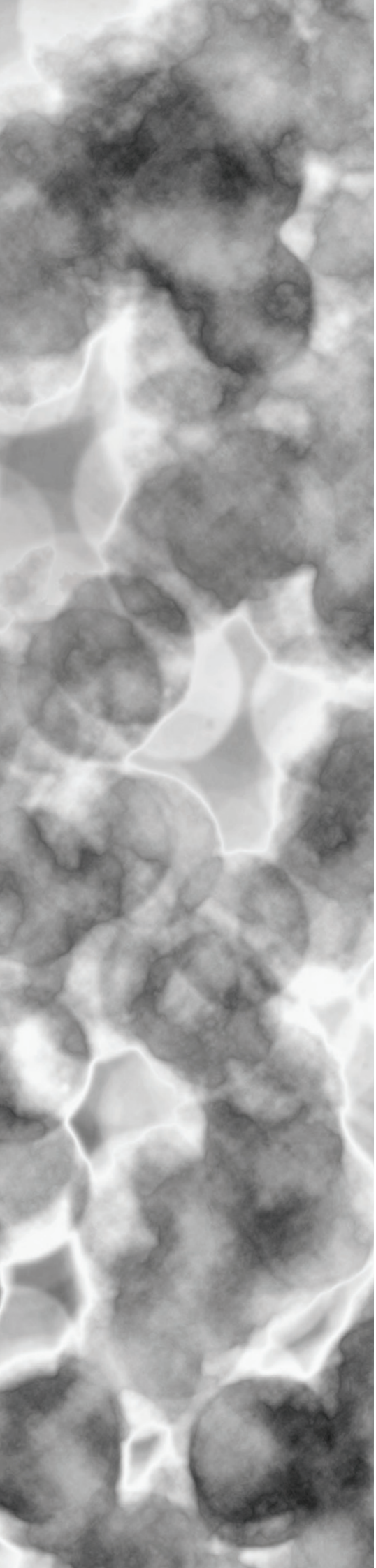
Security Market Report 2019: Data Demands Spur Robust Recruitment

BARCLAY SIMPSON.

www.barclaysimpson.com



FOREWORD

This is the first year Barclay Simpson has combined our candidate and client reports, with over 1,600 governance professionals responding to our global surveys. We are delighted to now share the key security trends with you.

The main theme of our findings is that security currently enjoys a healthy level of immunity to the UK's ongoing economic and political uncertainty. Departments continued to grow in 2018 and talented professionals are more in demand than ever before.

Regulatory changes, such as GDPR and the FCA's drive towards more cyber skills on boards, ensure security and resilience issues are now a priority for many organisations. Major data losses and high-profile hacks also remain a constant fixture of the news cycle and act as a frequent reminder of the perils of poor governance. These factors have delivered an almost recession-proof market for cyber professionals.

Overall, GDPR drove a more data-aware environment throughout 2018, which created a considerable amount of work for security functions. Extra workloads, combined with a well-documented skills shortage and competition from the contract market, created the perfect conditions for rising salaries last year.

However, our surveys revealed priorities may be changing among security practitioners. Career development and a better work-life balance were more important than salary increases for many candidates who were weighing up their options last year. We feel this is a clear sign that many professionals are now already well paid and are focused on other aspects of their jobs.

The future looks bright for the security recruitment market in 2019, with more employers hiring, cyber issues rising up board agendas and candidates increasingly comfortable with salaries. Challenges remain nonetheless, with fewer security departments reporting they are adequately resourced and one-fifth of businesses unhappy with their current recruitment model.

We hope this report will provide useful insight into the security markets. Given the strong ties between all areas of governance, we also encourage you to read our other governance reports, which can be **downloaded here**: https://www.barclaysimpson.com/market-report-2019

Mark Ampleford
Director - Head of Security Division
at Barclay Simpson

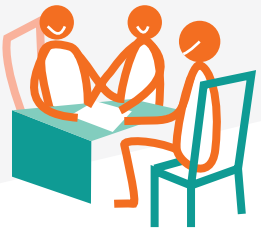
CONTENTS

01

At a Glance

only
43%

of teams
feel adequately resourced



Sourcing interpersonal skills is the biggest hiring hurdle
for **38%** of firms

74%
of employee workloads unaffected by Brexit

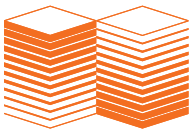
32% of departments hired
10 or more contractors
last year

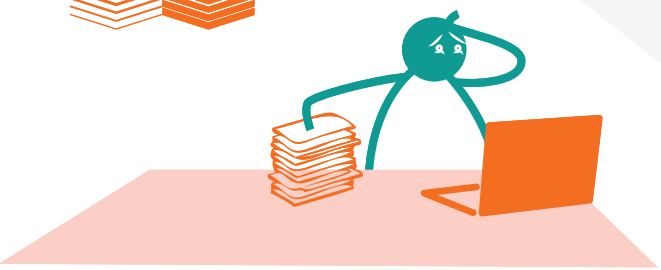
72%
of employers intend to hire
in 2019
up from 67%

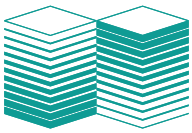
27%
of practitioners
switched jobs, rising from 19% in 2017

Career development
key for
55% **of those who moved**

9%
of companies
felt understaffed
when tackling GDPR



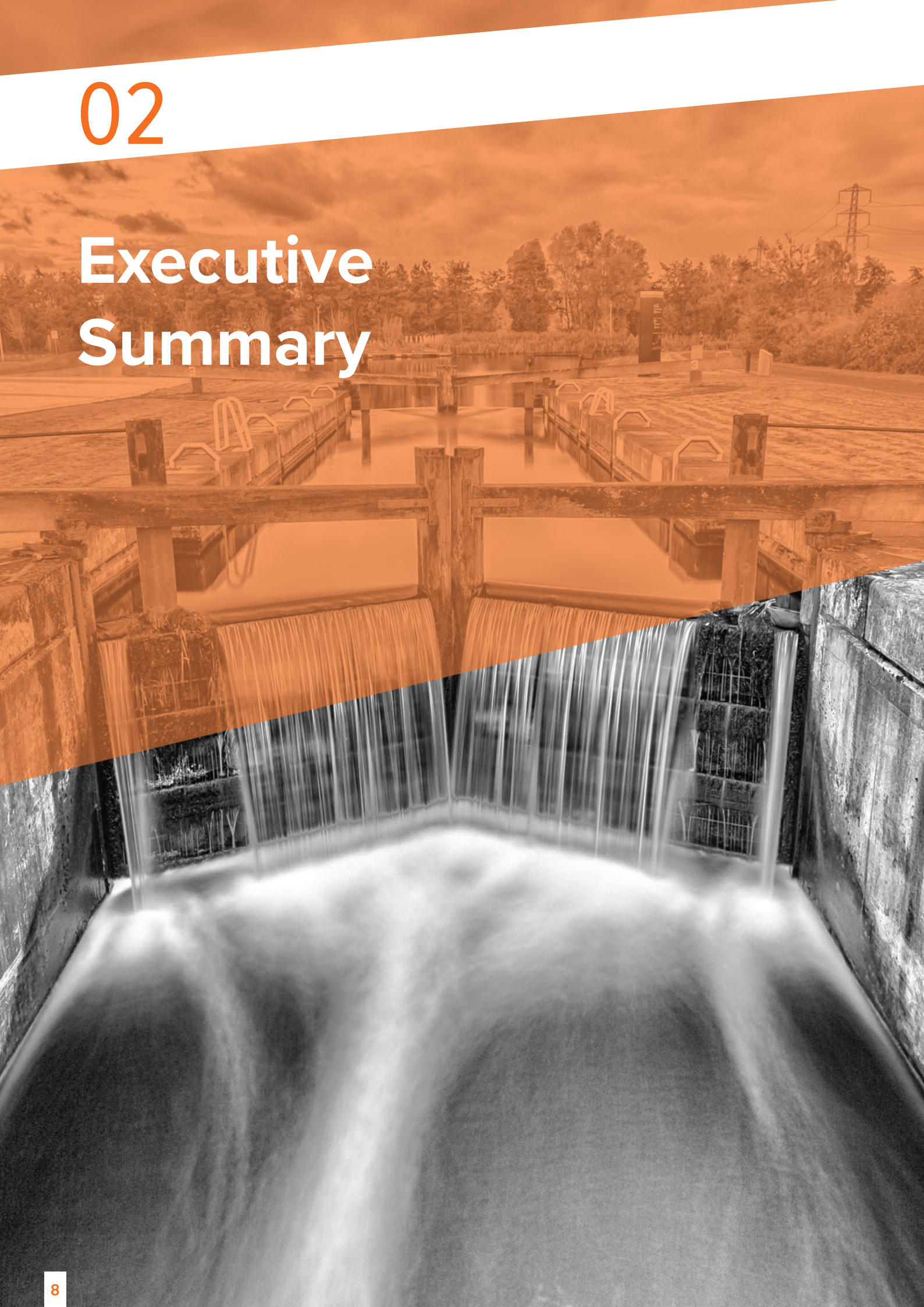




68%
of professionals believe
new technologies
improve efficiency

02

Executive Summary



Recruitment remains robust despite economic uncertainty

GDPR and growing skills shortages within cyber security ensured an active recruitment market in 2018, with two-thirds of departments hiring and 27% of professionals switching jobs. Cyber security is also expected to remain buoyant this year, as the FCA pushes for more cyber skills on boards and organisations tackle the ever-present threat of major data breaches in an increasingly punitive environment.

Workloads unburdened by Brexit

Nearly three-quarter of security practitioners said Brexit has had no impact on the work they do. Overall, the function remains resilient to the ongoing uncertainty, although 3 in 10 candidates admitted feeling less secure in their jobs and 53% would be willing to move out of the UK if their career was hampered by Brexit.

Switching jobs continues to reap rewards

Professionals who secured new job opportunities received salary increases of 17% on average in 2018, compared with just 5% for those who chose to stay with their current employer. The number of vacancies increased last year, with employers pricing roles correctly and moving swiftly to fill them.

Career development trumps salary as key motivator

The proportion of candidates who cited career development as their primary reasons for changing jobs increased from 38% in 2017 to 55% last year. There was also a noticeable slump in professionals moving due to salary dissatisfaction (28% versus 20%, respectively). Many people are now already receiving generous pay, so it is likely they are focusing on other benefits when eyeing the job market.

Interpersonal skills in short supply

Finding candidates who have the right soft skills was the greatest recruitment challenge for 38% of employers in 2018, making security the only corporate governance function where interpersonal capabilities topped the list. Technical skills (29%) and sourcing people in the right location (20%) were also key problems.

Professionals divided regarding disruptive technologies

Data analytics, artificial intelligence (AI) and the cloud are already being used or are set to be implemented at 78% of organisations, but security practitioners are split on how innovation will affect their job security. Over half (52%) are either unsure of the impact or think technology will put them at risk, while 48% feel confident their skills will be required even more.

Gender diversity remains a challenge

The gender balance in security departments remains overwhelmingly male-dominated, with an almost 9:1 male-to-female ratio emerging across our surveys. However, the cyber and information security profession shows more ethnic diversity and neurodiversity than most UK industries.

Contractors set to shift into full-time positions

More than 6 in 10 (62%) of security departments used interim staff in 2018, with 32% hiring 10 or more throughout the year. However, upcoming off-payroll legislation in the form of IR35 is likely to result in more contractors moving into full-time roles over the next two years.

03

Security market trends

Various economic, political and regulatory head-winds continue to affect the security and resilience market. Here, we examine the factors that had the biggest impact on hiring last year and predict key trends for 2019.

Economic and regulatory drivers

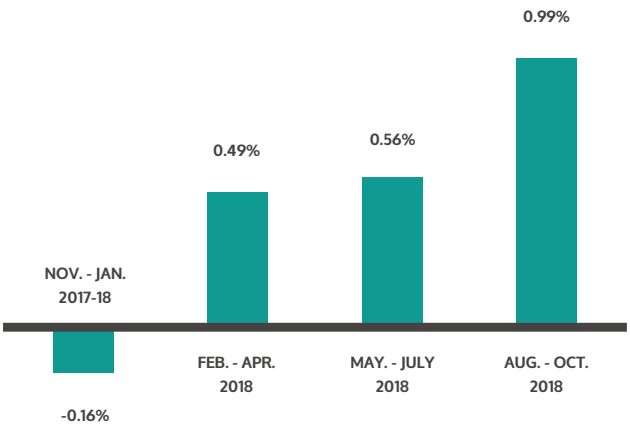
Signs of recovery for UK economy

Uncertainty was perhaps the running theme running through **our last market reports**. In 2017 and 2018, businesses faced massive upheavals as they prepared for regulatory changes such as GDPR, MiFID II and PSD II.

The economy also grew at its weakest rate in five years, during the first six months of 2017.[1] By the end of that year, the country's long-running streak of falling unemployment had faltered[2], real wage growth had stagnated and lingering doubts remained over Brexit.

Uncertainty is still a problem over a year on, particularly regarding Brexit, but there are signs 2018 was a stabilising period and organisations can expect the next 12 months to provide answers to some elusive regulatory questions.

Quarterly UK pay growth (real)



Source: ONS

Pay growth revival

Unemployment stood at just 4% in the three months to August 2018, which was the lowest rate in 40 years.[3] This figure had crept up to 4.1% by the September quarter[4] but still remained significantly below the 8.1% peak seen in 2011.[5] A subsequent skills shortage helped pay growth hit 3.3% at the time of writing.[6] This is the biggest increase since the country plunged into recession in 2008.

Real wage growth, which accounts for inflation, is also steadily increasing. Between April and June, regular pay edged forward just 0.34% in real terms.[7] However, this had climbed to nearly 1% for the three months leading to October[8], as the annual inflation rate stabilised at 2.3% in November.[9] Sluggish productivity remains a problem for businesses, but the results nevertheless suggest salary growth showed a strong upward trajectory throughout 2018.

The data legislation revolution

Data protection and privacy concerns have increased in recent years, as the media spotlight continues to shine on massive cyber security breaches and alleged commercial misuse of consumer information.

Suffice it to say, 2018 was a year in which UK and EU regulators sought to significantly strengthen existing laws by introducing several pieces of key legislation. GDPR came into force on May 25th last year, just two days after the UK's Data Protection Act 2018 received royal assent. The Act is designed to modernise the country's data laws in an increasingly digital age and ensure the UK remains aligned with GDPR standards after Brexit.

The Network Information Systems (NIS) Directive also applied from May last year. Whilst not specifically targeting data protection, the directive aims to protect the integrity of IT systems that are critical to national infrastructure across EU member states. As such, overlap with data protection and privacy issues are unavoidable.

Security remains calm amid Brexit storm

Predicting the future is always difficult, but even the best analysts have found it impossible to forecast what will happen next with Brexit.

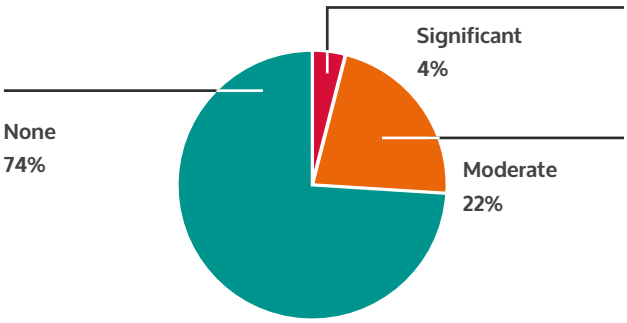
The tension surrounding the UK's exit from the EU was palpable in our previous market reports and not much has improved since then. However, the cyber and information security market has remained resilient in the face of continuing uncertainty.

Workloads see minimal Brexit impact

Many security professionals appear to be taking a pragmatic approach to the UK's separation from the EU, particularly as the wider political and economic picture remains unclear.

Nearly three-quarters (74%) of security professionals claimed Brexit had no effect on their workloads in 2018, which is significantly higher than other corporate governance functions. Meanwhile, 54% of departments had not begun contingency planning, although 16% of employers had opened or were planning to open offices outside of the UK in preparation for Brexit.

What impact has Brexit had on workloads?



One eye on the future

Despite a generally bullish attitude, professionals still appreciate the negative impact a UK-EU split could have on their career, with 30% feeling less secure in their job due to Brexit. More than half (53%) of candidates also admitted they would be willing to relocate to an EU country if Brexit harmed their career.

A sizeable proportion of security professionals are already from overseas, meaning they are often open to moving outside the UK if the country's economy weakens. Further weakening of the pound could encourage more practitioners to examine opportunities abroad.

Professionals are flexible regarding location

Security professionals are more flexible regarding their preferred employment location than any other corporate governance department. Amsterdam and Zurich were cited as acceptable relocation options by 59% and 57% of candidates, respectively, but at least half were also willing to move to Dublin, Frankfurt or Paris.

Among employers that had opened (or were planning to open) a new office, Germany and Benelux were the most popular destinations with 38% of the vote apiece. Candidates hoping to relocate to Zurich may be disappointed to hear that none of our respondents had plans to open Swiss branches.

Disruptive forces affecting security departments

GDPR compliance

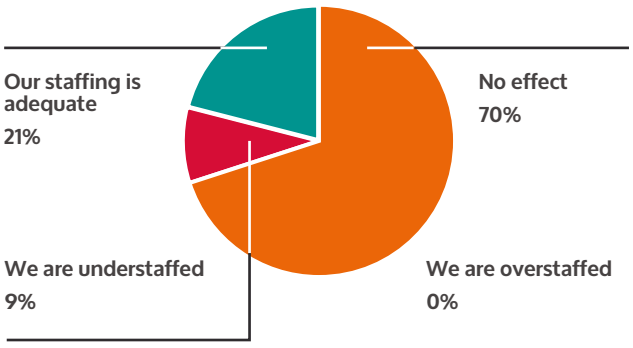
Significant resources went into preparing for GDPR in 2017 and 2018, with the regulation's introduction marking the most comprehensive modernisation of Britain's data protection and privacy laws since the Data Protection Act 1998.

GDPR heralds a new era of potentially eye-watering fines for mishandling data. The maximum penalty for serious breaches is €20 million or 4% of an organisation's annual revenues, whichever is higher. This is seen as an improvement from previous guidelines as the Information Commissioner's Office (ICO) had only been able to hand out fines of up to £500,000.

Security professionals may have breathed a sigh of relief when the implementation deadline passed, but the job is far from over for many departments. A TrustArc survey showed 26% of organisations didn't expect to be compliant with GDPR by the end of 2018, while 7% won't even be ready when this year comes to a close.[10]

Our research found nearly 1 in 10 (9%) security departments said they were understaffed in the lead-up to GDPR's implementation. However, a large majority (70%) claimed the regulation had no impact on staffing levels, suggesting employers felt confident of their ability to protect sensitive data.

What impact has GDPR implementation had on staffing?



It remains to be seen whether confidence in GDPR compliance is well placed. As I write this, the first GDPR fines ***are already beginning to trickle through*** *but the extent to which regulators will punish flagrant data protection and privacy breaches is uncertain.*

In 2019, we expect the technological implementation of GDPR controls, the post-Brexit data-sharing deal and the introduction of the e-Privacy regulation to all play a part in driving up demand in a market where hiring is already tough.

Andrew McNamara
DATA PROTECTION AND PRIVACY RECRUITMENT

Technology: A double-edged sword?

The move towards cloud computing, AI, data analytics and machine learning enables organisations to streamline the front line of security operations, delivering efficiency and cost reductions.

There is greater emphasis on SOAR (Security Orchestration, Automation and Response) models that automate threat detection and level 1 security analysis. Less than 1% of businesses that had security teams containing more than five people used SOAR technologies in 2017, but Gartner predicts this figure will jump to 15% by 2021.[11]

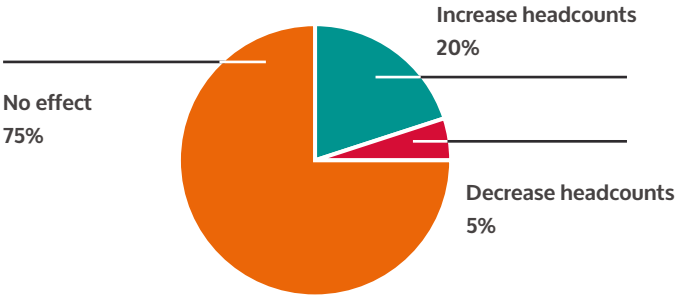
This innovation creates both challenges and opportunities for different segments of the market. For example, the adoption of disruptive technologies could reduce headcounts in front-line areas but lead to an increase of roles at the more technically capable end of the market. Technological advances also mean security professionals face new and evolving threats from cyber criminals every day.

These competing factors appear to be reflected in our research results, which indicated a broad spectrum of views on disruptive technologies. Data analytics, AI and the cloud are already being used by 58% of employers, with a further 20% planning to introduce them. Three-quarters of respondents believe these technologies won't affect their recruitment needs, although 20% expect to increase headcounts to optimise their approach to innovative platforms.

Among candidates, 68% were confident adopting data analytics and the cloud would increase security department efficiency but 21% disagreed. Similarly, professionals were divided on whether or not new technologies would affect their job security. While 48% of respondents said their employment would be more secure, 52% were either unsure of the impact on their jobs or felt they would be less secure.

How will AI, data science and cloud computing affect your job security?

What effect will technology have on staffing?



There is already a technology drive towards the cloud, which means organisations will begin investing more in cloud-based security. Some roles will naturally become less important as a result, including infrastructure security positions.

Candidates with experience of managing complex cloud implementation projects will be highly sought-after. However, these opportunities are likely to stagnate once the majority of organisations have finished transitioning.

Sophie Jdouri

CYBER AND INFORMATION SECURITY RECRUITMENT

Diversity and inclusion

Diversity is a hot topic, and rightly so, with businesses worldwide keen to be more inclusive during their recruitment processes. Countless studies have emphasised the benefits of diverse workforces, which include:

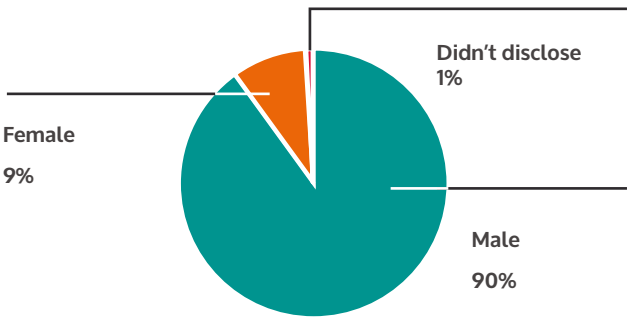
- Enhanced profitability;[12]
- Improved decision-making;[13]
- Better innovation[14]; and
- Improved customer experiences.[15]

Security departments are often a mixed bag when it comes to diversity and inclusion. For example, there is notable neurodiversity in areas such as cyber security, with some experts believing individuals with Asperger Syndrome and associated conditions can bring unique insight and skills to cyber-crime prevention.[16]

The IT sector overall also has better ethnic diversity than other industries. The proportion of non-white IT workers stood at 17% in 2017, compared with 12% across all UK employees.[17] Just under one-third (31%) of London-based IT specialists are from an ethnic minority background.

However, cyber and information security has a well-established gender diversity gap. Research shows just 7% of cyber security professionals across Europe in 2016 were women, and men were nine times as likely to hold managerial positions.[18] Our results showed a similar pattern, with a male-to-female ratio of approximately 9:1 among candidates.

Gender balance in security departments



The challenges of diversity-led recruitment

Organisations are taking important strides towards better diversity and inclusion within security teams. Indeed, 16% of clients told us diversity and inclusion targets directly affected their recruitment decisions in 2018, indicating firms are making proactive attempts to tackle gender gaps.

The UK government is also trying to encourage more women into the industry through gender-focused initiatives as part of the National Cyber Security Skills Strategy.[19] Deloitte is just one of a number of major businesses to launch a Women in Cyber scheme in recent years.[20]

Nevertheless, securing top talent in the security and resilience recruitment market is often hard enough for employers. LinkedIn research has revealed that finding enough applicants to interview is the main hurdle for most diversity-focused businesses, let alone employers operating in industries with severe skills shortages.[21] Our findings reflected similar concerns, with 43% of hiring managers reporting that recruitment efforts prioritising diversity were unsuccessful.

Cyber and information security remains a male-dominated field, particularly at the top. This is going to take some time to change, but there are a number of encouraging initiatives — both at the national and organisational level — that are working to address gender diversity within the profession.

With corporate security traditionally being a second career for many people after government service, those transitioning into the space are often male due to a lack of diversity in the police, military and intelligence services.

Sophie Jdouri

CYBER AND INFORMATION SECURITY RECRUITMENT

04

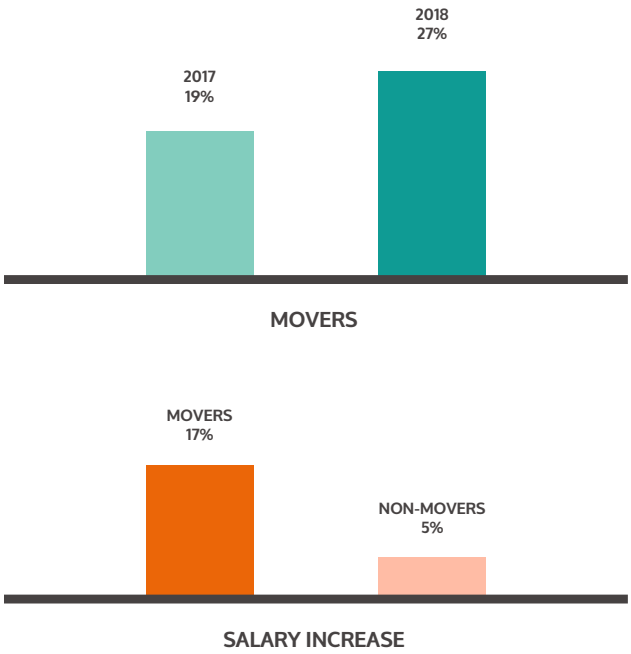
Recruitment, salary and compensation trends

We have discussed the major factors influencing the market, but what impact are they having? This section examines key client and candidate insights from our global surveys along with salary trends.

How active is the security recruitment market?

More than one-quarter (27%) of security practitioners moved jobs last year, which is a significant increase compared to the 19% who switched roles in 2017. This matched our own experiences, with consultants reporting a more buoyant market overall.

A snapshot of security recruitment in 2018



Vacancies increased but, more importantly, the roles advertised were often priced correctly and companies moved swiftly to fill them. Top-shelf talent is rarely on the market for long and employers risk losing out on quality candidates if they persist with slow-moving, bureaucratic recruitment processes.

Cyber and information security skills shortages helped create upward pressure on remuneration, meaning candidates who changed employers saw an average salary increase of 17% in 2018, compared with a 5% rise for non-movers. Of those that moved, 45% admitted it was more difficult than they expected. This is perhaps surprising given ongoing skills gaps and the fact just 33% said the same in 2017 - a year in which the market was less active.

The number of data protection officer roles increased rapidly in the months before and after GDPR's implementation. Many organisations are legally required to assign individuals to these positions, so businesses lacking the appropriate capabilities in-house have actively sought these skills on the market.

In the latter half of 2018, a shift towards more junior and mid-level hires occurred. Many organisations are experiencing increases in operational privacy activities, such as answering subject access requests, conducting privacy impact assessments and re-writing data protection policies.

This has meant historically flat privacy functions, comprising of one or two professionals, have grown to teams of five or six in order to handle the increased workload. We have also seen a surge in the market for privacy lawyers, with many firms creating separate privacy legal counsels or adding privacy-focused experts to existing General Counsels.

Andrew McNamara

DATA PROTECTION AND PRIVACY RECRUITMENT

The CISO market enjoyed solid growth in 2018, with businesses across all sectors investing in transformation programmes and recruiting their first security leaders. Demand for CISOs who have a history of successful transformation projects therefore continues to be strong. While these candidates are generally in short supply, the market has a healthy churn rate because individuals often get itchy feet once a newly transformed department approaches BAU functionality.

Many CISOs are attracted to innovative sectors or the size of an organisation rather than salaries or packages, but remuneration at the upper end is on the rise nonetheless. The international nature of the CISO market has contributed to salary inflation in Britain, and a drop in the value of pound sterling typically works well for professionals who have always been UK based.

Although the resilience market has remained stable, there has been a significant amount of job creation within the corporate security space, from lower-level analysts through to senior-level strategic hires. Some surprisingly large firms also hired their first strategic-level CSO, resulting in subsequent trickle-down effects as they then built out a suitable team.

What drivers are affecting candidate choices?

People move jobs for a variety of reasons, but 2018 marked a significant shift in priorities for many security practitioners.

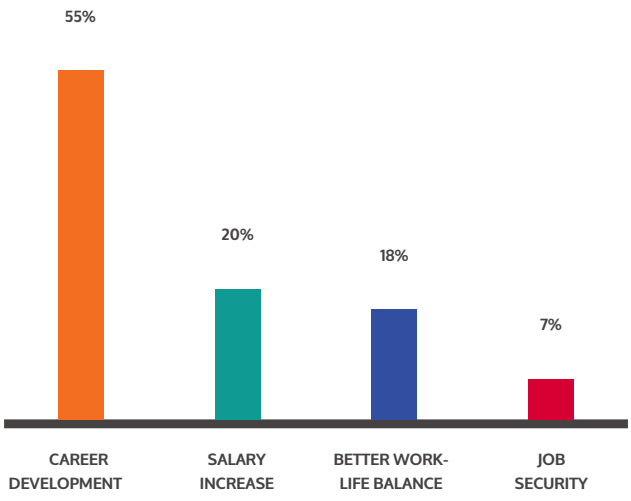
Career ambitions on the rise

Candidates showed a renewed interest in career development last year, with 55% citing this as the primary reason for switching jobs. The figure is a considerable increase from the 38% who said the same in 2017. This contrasted with a fall in the proportion of respondents who moved due to salary dissatisfaction from 28% to 20%.

The most obvious explanation for this trend is that many security practitioners are already generously paid. Those who felt they were lagging behind the market have now enjoyed a few years of solid industry growth, allowing them to secure new roles or land a pay rise to address salary shortfalls. Indeed, 62% of respondents felt they were adequately compensated, which was up from 56% in 2017 and 58% the previous year.

Employers in security work hard to ensure remuneration is at the right level, but CISOs this year and beyond must be able to match candidates' career ambitions. As departments continue to grow across the board, professionals will favour roles that provide clear paths of progression, opportunities to upskill and the chance to work on interesting projects.

Why did you move jobs?



Data protection skills needed

Recruitment within the data protection market has historically been relatively steady, but regulatory changes significantly increased activity across all industries in 2018. Experienced candidates who have the relevant privacy skills remain in short supply, which has caused rapid salary rises. Organisations are either approving pay increases to retain their existing data professionals or stretching their budgets to attract the right talent in an extremely competitive market.

The data protection market has been given a new lease of life due to the introduction of GDPR and the Data Protection Act 2018. Indeed, many non-technical security professionals are now reskilling in order to move into lucrative privacy policy roles or risk-based data protection positions.

However, this migration into data protection has not been exclusively for non-technical security professionals. We have also seen more candidates using their control implementation skills to assist privacy programmes in achieving GDPR compliance.

Tom Woods

DATA PROTECTION AND PRIVACY CONTRACT RECRUITMENT

Salary demands make way for other benefits

With most professionals feeling comfortable with remuneration, hiring managers and candidates are able to have sensible conversations about pay. Other job perks became more important for applicants weighing up offers last year.

For example, 79% of survey respondents said their employer provides flexible working, yet 72% would like even more opportunities of this nature. Nearly one-fifth (19%) admitted a better work-life balance would be the main reason for considering another job or going to an interview.

Security practitioners rarely apply for multiple roles unless they are highly motivated to leave their current job, so employers must be shrewd when advertising vacancies to ensure they appeal to an increasingly discerning candidate pool. Access to big budgets, best-of-breed technologies and ambitious transformation projects often attract top talent who want to work for a company that takes security seriously.

What recruitment challenges did employers face?

Two-thirds (66%) of departments recruited or attempted to recruit security and resilience professionals in 2018. However, 33% said hiring was more difficult than expected. Here are some of the reasons why:

A global skills shortage

The cyber and information security skills shortage remains an ongoing concern. Analysts have predicted there will be 3.5 million unfilled cyber security job openings worldwide by 2021.[22] In Europe, the profession is predicted to have a shortfall of 350,000 skilled workers within the next three years.[23]

The UK's National Cyber Security Skills Strategy aims to bridge the country's growing talent gaps. Currently, 54% of all British businesses are unable to confidently perform basic technical cyber-related tasks, such as detecting and removing malware, setting up and configuring firewalls and storing or transferring data in a secure way.[24]

The cyber skills shortage has led to an exceptionally candidate-driven market. Last year, 94% of recruiters polled by the Recruitment and Employment Confederation predicted cyber salaries would rise due to 'significant' increases in demand for security staff.[25] This forecast appears accurate; 55% of candidates in our research said finding a new role was easier than expected last year, and one-quarter of those who switched jobs enjoyed a salary increase of more than 30%.

Talking the talk ...

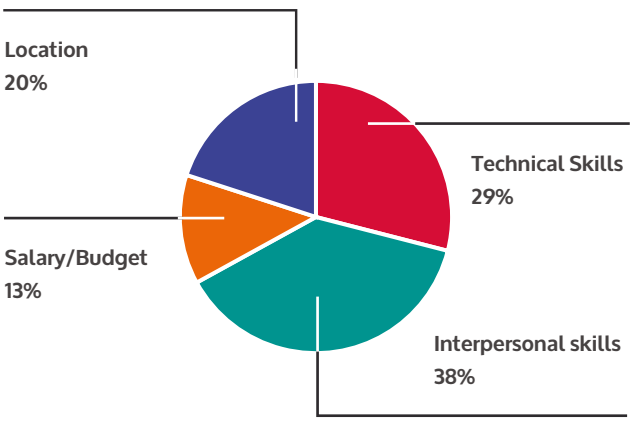
Security and resilience was the only corporate governance function where finding people with strong interpersonal capabilities was the greatest recruitment challenge for employers last year. Nearly 38% of respondents cited soft skills, although technical skills (29%) and securing candidates in the right location (20%) were also notable problems.

Excellent communication is becoming a key trait for security professionals as cyber issues continue to climb up the boardroom agenda. The ability to deliver complex technical information and concepts to the C-suite, many of whom lack a technical background, is already highly valued.

Communication and influencing skills are also vital within corporate security. Without the regulatory requirements of some fields and being somewhat under the radar compared to cyber, corporate security professionals have to 'sell' the function to show its value.

Only 13% of employers cited restrained budgets and unrealistic salary expectations as their main hiring hurdle, indicating an impressive level of buy-in at senior levels for top talent. Given this, we're surprised at how much candidates invest in their technical qualifications and training when a business coach or mentor to improve their people skills could pay higher dividends.

What is your greatest recruitment challenge?



... And walking the walk.

Interpersonal skills may be the main focus but securing candidates with technical aptitude remains a struggle for a sizeable proportion of firms. Ultimately, employers want security practitioners who have a combination of hard and soft skills, as well as leadership capabilities.

Policy-focused, non-technical candidates have either moved into allied professions, such as privacy, or become more technical as a result. Even at a distance within the second or third line of defence, anyone looking at cyber controls must have technical depth and know-how to compete.

Security leaders and CISOs are now key hires to organisations with board visibility. When organisations break their security budget, it's usually to land a talented CISO who has emerged as the leading candidate from a competitive field of applicants during an executive search process.

Engineers and analysts are also seeing strong demand for their skills. These positions have not enjoyed the salary increases of other security disciplines, which is why many are instead attracted to the contractor sector.

Mark Ampleford

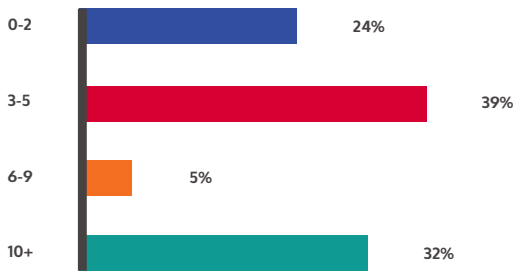
DIRECTOR - HEAD OF SECURITY DIVISION

Contractors help fill security skills gaps

The contractor market saw a steady stream of opportunities last year, particularly during the first three quarters. Our survey showed 62% of security and resilience departments used interim staff in 2018, with nearly one-third (32%) hiring 10 or more contractors.

These figures, which are higher than all other corporate governance functions we surveyed, highlight the importance of contractors in a discipline where skills shortages are especially prevalent. The majority of security departments (46%) cited a desire to keep headcounts low as their primary reason for using contractors, while project work (25%) and subject matter experts (24%) were also popular requirements.

How many contractors do you hire a year?



Contractor recruitment remains relatively balanced across both technical roles and GRC (governance, risk and compliance) roles. Indications point to a heavier reliance on contractors for incident response, architectural and SecDevOps roles.

Initial media reports suggested the introduction of off-payroll legislation (IR35) to the private sector could appear as early as April 2019. As a result, we saw organisations push aggressively to convert a percentage of their contractors to permanent employees.

According to the 2018 Budget, IR35 will now be delayed until 2020, but we expect the trend of interim staff shifting into full-time positions to continue. The rules will bring private firms in line with public organisations, and HM Treasury claimed the reform has already raised £550 million in income taxes and NICs for the exchequer.[26]

Owanate Bestman

MANAGER - HEAD OF SECURITY CONTRACT RECRUITMENT

Unsurprisingly, the number of data protection contract roles has dropped since the GDPR implementation date passed. Data protection remains a key governance focus point for businesses, but a lack of skills within the market has led to employers seeking fixed-term contractors rather than daily rate consultants. This decision is often driven by budget limitations and the fact data protection often straddles the border between legal and security teams, rarely having its own department.

Overall, firms are showing a propensity to recruit interim staff, which is readily available, while they search for a permanent hire. The contractor candidate base is also growing, particularly on the technical side, although salary expectations among cyber and information security professionals can be unrealistic.

Looking ahead to 2019

The proportion of security departments that felt adequately resourced slumped from 48% to 43% last year, emphasising the growing skills shortage and strong demand for quality candidates. But what recruitment trends are expected in 2019?

A snapshot of security recruitment for 2019

Hiring to hit new heights

In 2017, just over two-thirds (67%) of security professionals believed they would need to hire last year. These predictions turned out to be accurate, with this exact proportion recruiting or trying to recruit across the 12-month period.

Security recruitment is likely to be even more buoyant in 2019, as 72% of employers confirmed they intended to hire. Departmental expansions appear to be the largest driver of demand; 62% of respondents are adding to existing headcounts through growth hires, compared with 38% who said they would be mainly replacing outgoing staff.

However, skills shortages may be fuelling dissatisfaction with existing recruitment models among CISOs. One in five organisations said they weren't happy with their current hiring methods, with nearly half (49%) using direct sourcing. Will 2019 be the year more employers seek specialist support when recruiting for security and resilience roles?

Data protection and privacy remain key concerns

GDPR and other important cyber security legislation are now in place, which means demand for data protection and privacy professionals will continue this year as firms get to grips with greater scrutiny of their processes. We have already seen a growing number of candidates strengthen their technical capabilities to compete for privacy policy roles and risk-based data protection positions. This will be an ongoing trend driving recruitment within the market in 2019.

Automation will also be a central feature of data protection over the coming years, and any processes involving consumer data must have privacy by design built into them. The ICO has recently hired its first automation specialist to cope with the expected increase in AI data privacy misuse investigations.

The proposed ePrivacy Regulation is unlikely to be finalised until 2020 at the earliest[27], but talks are likely to recommence after the European Parliament elections in May this year. The regulation's impact on UK security and resilience roles will depend on whether or not the government chooses to implement the changes after Brexit.

A push for boardroom cyber skills

Asset management firms and wholesale banking institutions are putting their clients at risk of serious harm due to cyber security failings at the board level, a recent FCA review suggested.[28] The regulator highlighted that firms "generally lacked board members with strong familiarity or special technical cyber expertise".

Financial services isn't the only industry where cyber skills are missing at the senior executive level. The National Cyber Security Centre has continually highlighted the importance of encouraging better boardroom discussions regarding these issues.[29]

The drive to ensure boards of directors are more cyber savvy is exciting for many senior leaders in the security world. Few professionals could have foreseen the potential of cyber security growth when they first entered the industry.

In 2019, we don't expect a widespread trend of CISO promotions into executive boards, but a paradigm shift is occurring and leaders who have cyber skills could find themselves offered non-executive directorships. This will open up portfolio career options.

05

Security recruitment: a sector analysis

Every industry had unique challenges and opportunities for security practitioners in 2018. This analysis drills down into the data to draw out key insights for various sectors and career streams.

Corporate security

CHRIS MEAGER

Head of Corporate Security and Resilience Recruitment

The corporate security market remains buoyant after an encouraging performance last year. Many firms hired for new positions, while also upgrading existing teams in both size and strategic focus. However, the number of large firms who have little or no in-house corporate security expertise is surprising, even among those operating in high-risk locations or having senior executives travelling the world.

Although roles that combine the cyber/corporate security skillsets still seem limited, there appears to be increased focus on intelligence-driven security functions. This has resulted in more firms hiring both analytical resources and corporate security practitioners who come from an intelligence background. We have seen anecdotal evidence supporting this, as numerous clients have hired more senior, strategic corporate security professionals to try and get ahead of the curve, moving away from tactical or reactive functions.

Although PAS:3001 was launched in 2016, there seems to be a more noticeable recent focus on supporting staff travelling overseas. As such, a growing number of firms are recruiting specific travel security-focused professionals, rather than leaving these tasks as part of a more generalist responsibility.

Financial services

MARK AMPLEFORD

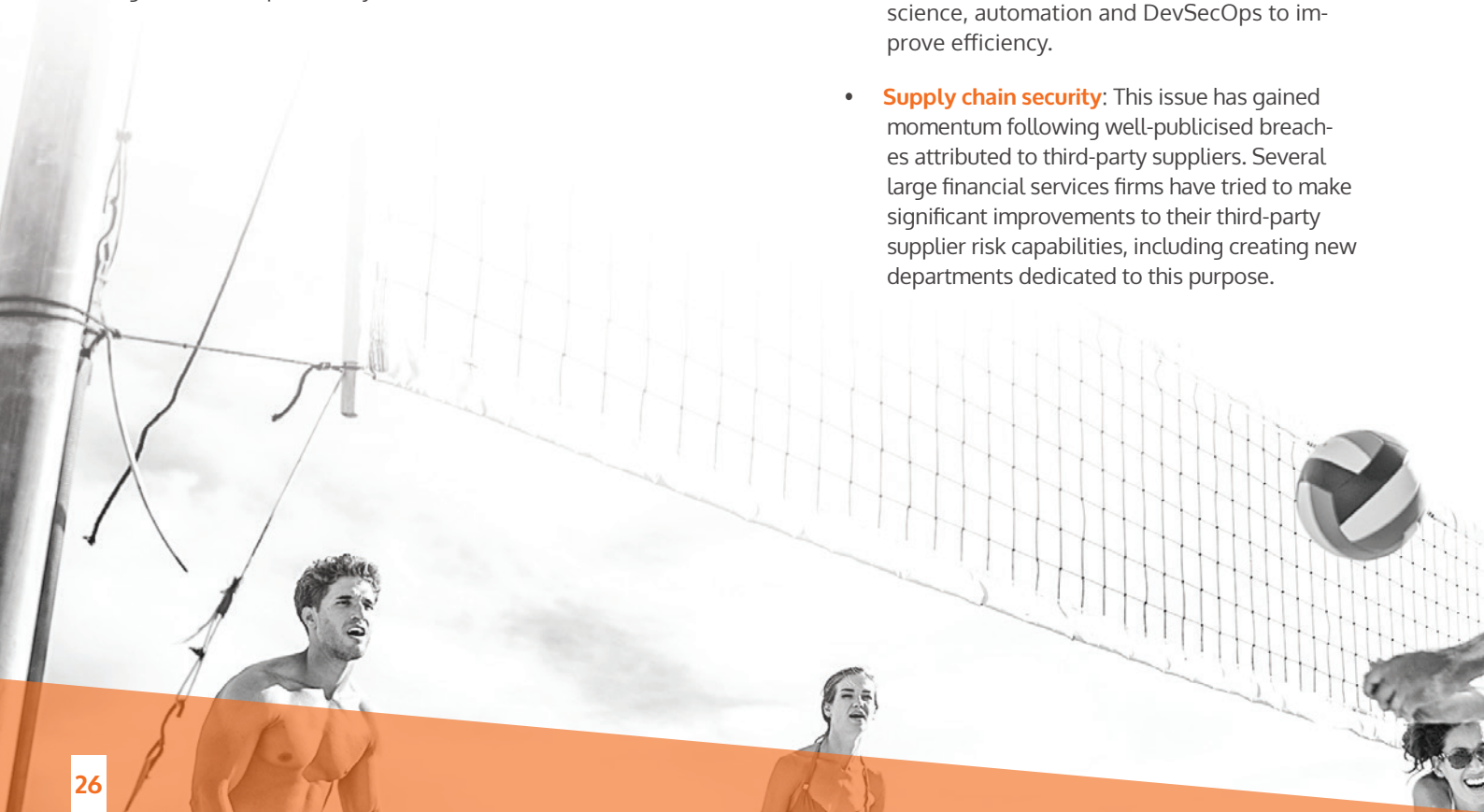
Director - Head of Security Division

Security recruitment within financial services has become extremely diverse, with a wide range of sought-after disciplines. Organisations with established security departments continue to evolve, and we have seen numerous smaller businesses recognise the need to increase security investment and appoint their first dedicated resource to build and run a function.

Smaller trading firms and fintechs have historically prioritised other major governance hires over security due to confidence in their IT and resilience processes. However, industry and regulatory pressures demand a greater focus on cyber security once companies reach a certain size. We're starting to see more appetite to develop in-house security expertise in order to reduce dependence on third-party outsourced security solutions.

Priorities and strategies vary significantly among larger banks and insurers, so it's difficult to identify unifying trends. Nevertheless, key areas of focus have emerged:

- **Disruptive technology**: Security professionals with cloud, AI and blockchain skills are in high demand. These new technologies create unique security challenges, with a growing number of security departments using data science, automation and DevSecOps to improve efficiency.
- **Supply chain security**: This issue has gained momentum following well-publicised breaches attributed to third-party suppliers. Several large financial services firms have tried to make significant improvements to their third-party supplier risk capabilities, including creating new departments dedicated to this purpose.



- **Risk and security grow closer**: An increased focus on enhancing technical knowledge within risk in 2017 continued into last year. The second line of defence is now keen to maximise their effectiveness in checking and challenging the first line of defence. A move towards a hybrid line 1.5 model has created demand for candidates who combine strong technical understanding with excellent communication skills and the ability to look at how technology can affect risk at an organisational level.

Commerce and industry

MARK AMPLEFORD

Director - Head of Security Division

The size, scale and seniority of reporting lines for departments within large corporates continued to grow in 2018. As reliance on technology and commitments to consumer data safety increase, it's fair to say that security practitioners outside financial services have had to upskill and larger corporates are investing heavily.

Leadership in security is not restricted by sector, so we have seen regular movement from those in financial services into commerce and back into financial services. Vacancy numbers in the oil and gas, utilities, travel, retail and gaming industries remain healthy and increased between 2017 and 2018. App-heavy start-ups and software companies are also fuelling market demand, with many of these businesses budgeting for security personnel from an early stage.

The seniority of CISOs in major corporates has crept up year on year, which has a knock-on effect for the layer below. As the structures have grown, we have seen more Heads of GRC, Heads of Cyber Operations and Heads of Architecture hit the market at a corporate level where we would previously only have seen CISOs.

Consultancies and systems integrators

HARISH PARMAR

Manager - Head of Commerce and Consultancies Recruitment

Recruitment has been a high priority in 2018 for the consultancies and systems integrators that offer cyber security services. As the number of clients seeking these services continues to grow, so does the need to have sufficient resources to meet demand. With immense competition and an ever-present skills shortage, many consultancies and systems integrators have been much more accommodating in order to attract candidates.

Many consultancies and systems integrators are hiring contractors as a way to fill these skill gaps while they look to secure additional permanent staff. The types of skills employers seek remain the same, particularly strong commercial capabilities and a solid level of technical understanding. Security Architects, especially those with cloud security experience, are among the highest in demand. Firms are also keen to hire consultants who have technical security expertise, such as SIEM, penetration testing, incident response and identity and access management.

Overall, there are two key factors that determine the level of success consultancies have in securing candidates:

- **Salary**: The increase in demand and competition has resulted in offers being pushed up. On average, salaries increased by 16% for people who switched roles between 2017 and 2018.

- **Flexible working**: Employers recognise candidates want flexibility and while it is accepted that travelling is part of the job, many consultancies are providing assurances of limited travel. Firms that still require candidates to travel 75-100% of the time often struggle to hire.

06
Conclusion

The security market remained resilient in the face of economic, political and regulatory headwinds in 2018. GDPR raised the stakes for organisations that mismanage data and boardroom buy-in for cyber security continues to climb.

As a result, the recent buoyancy seen in security recruitment is unlikely to falter anytime soon. However, hiring managers face significant skills shortages, with employers struggling to source candidates with the right mix of interpersonal and technical capabilities.

Looking ahead to 2019, organisations must be aware of shifting priorities among candidates if they want to attract and retain top talent. Many professionals are already well paid, so career development and flexible working opportunities are becoming more prevalent.

The security landscape is constantly evolving, which is why employers and practitioners often benefit from working with a partner who understands the market and can navigate choppy waters.

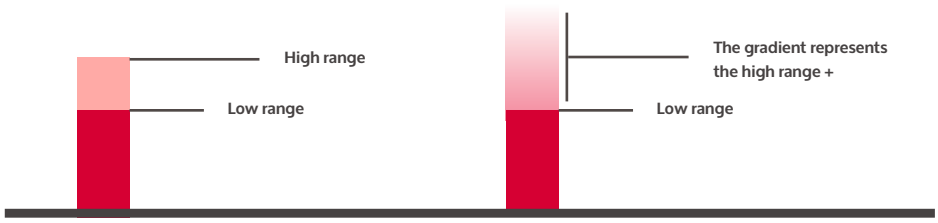
07 Salary guide

Barclay Simpson analyses the salary data that accumulates from our UK security and resilience placements. The salary ranges are industry averages and don't account for other benefits such as bonuses, profit-sharing arrangements and pension benefits.

For further information about salaries in the compliance market contact Mark Ampleford at **ma@barclaysimpson.com**

Key

Each bar shows the low and high salary range:

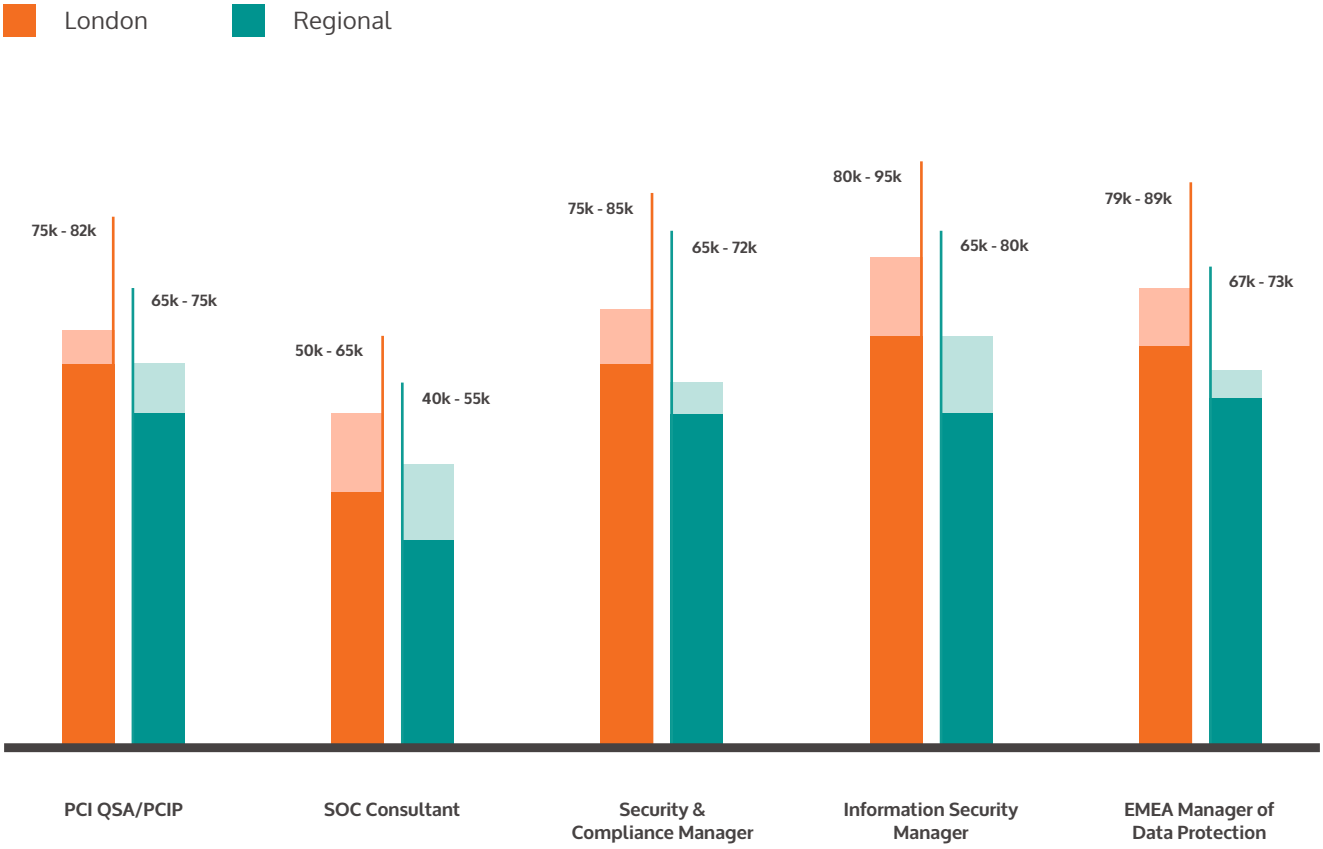


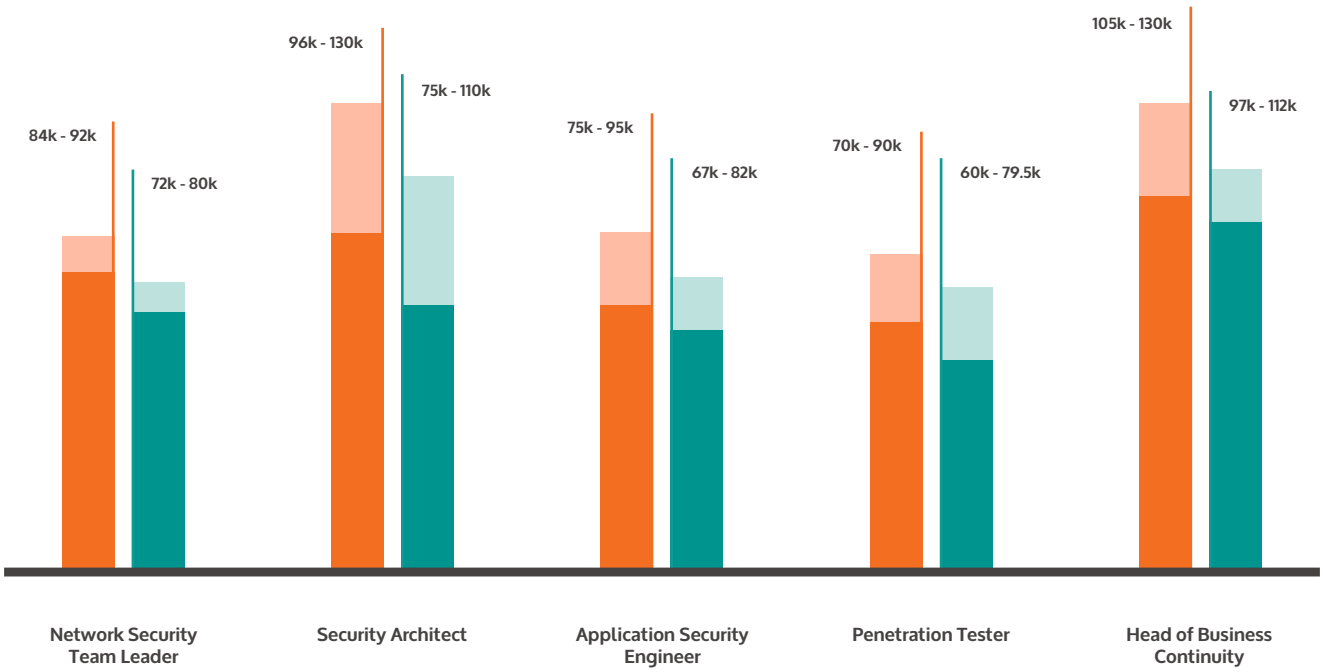
Permanent

Gross annual salary in GBP

Permanent (continued)

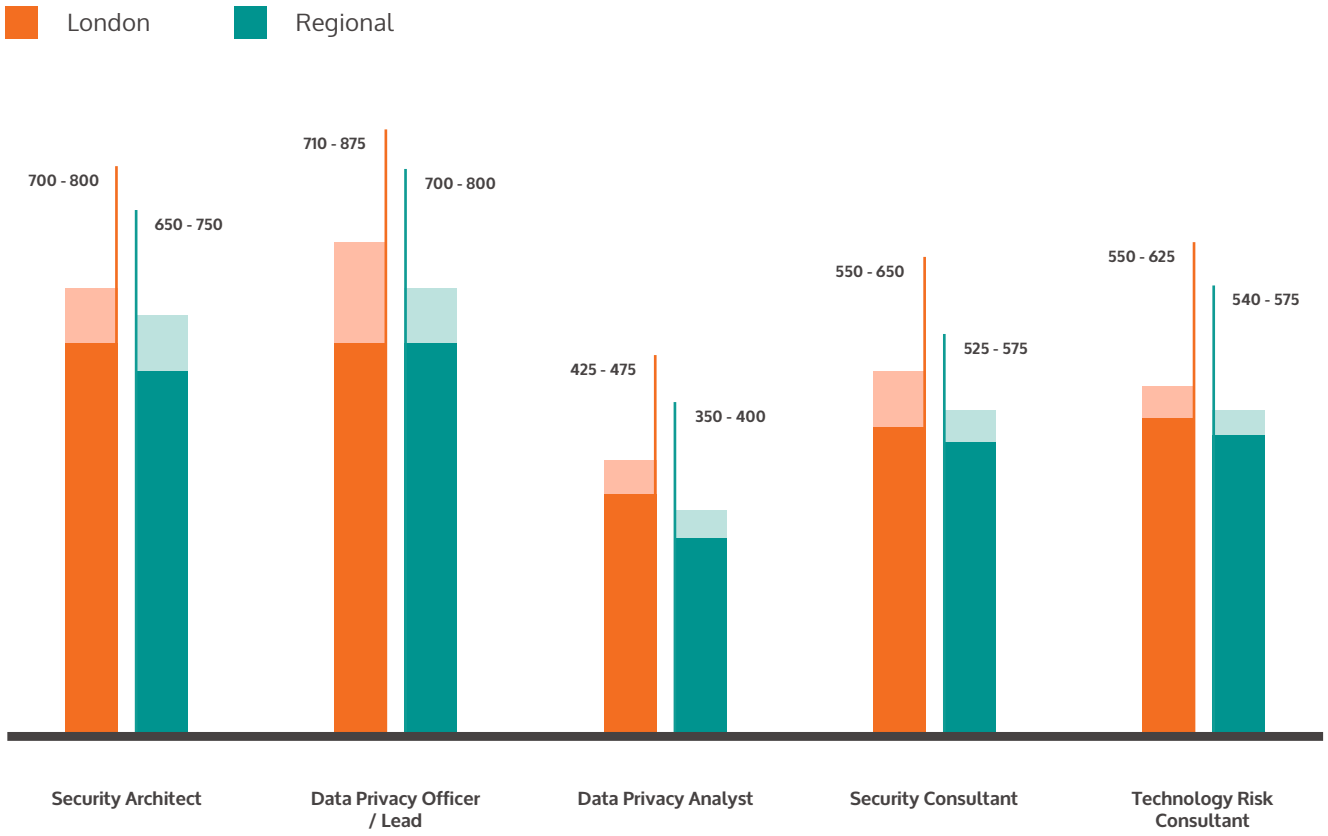
Gross annual salary in GBP

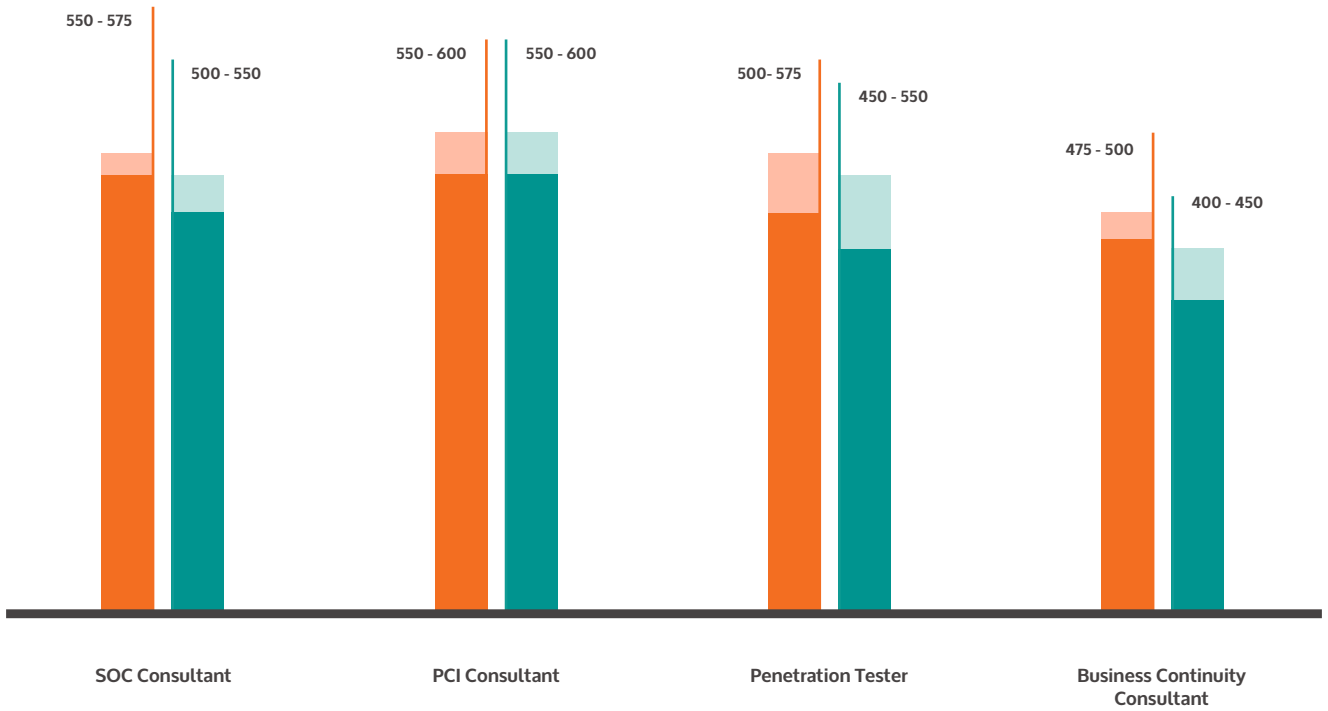




Contract

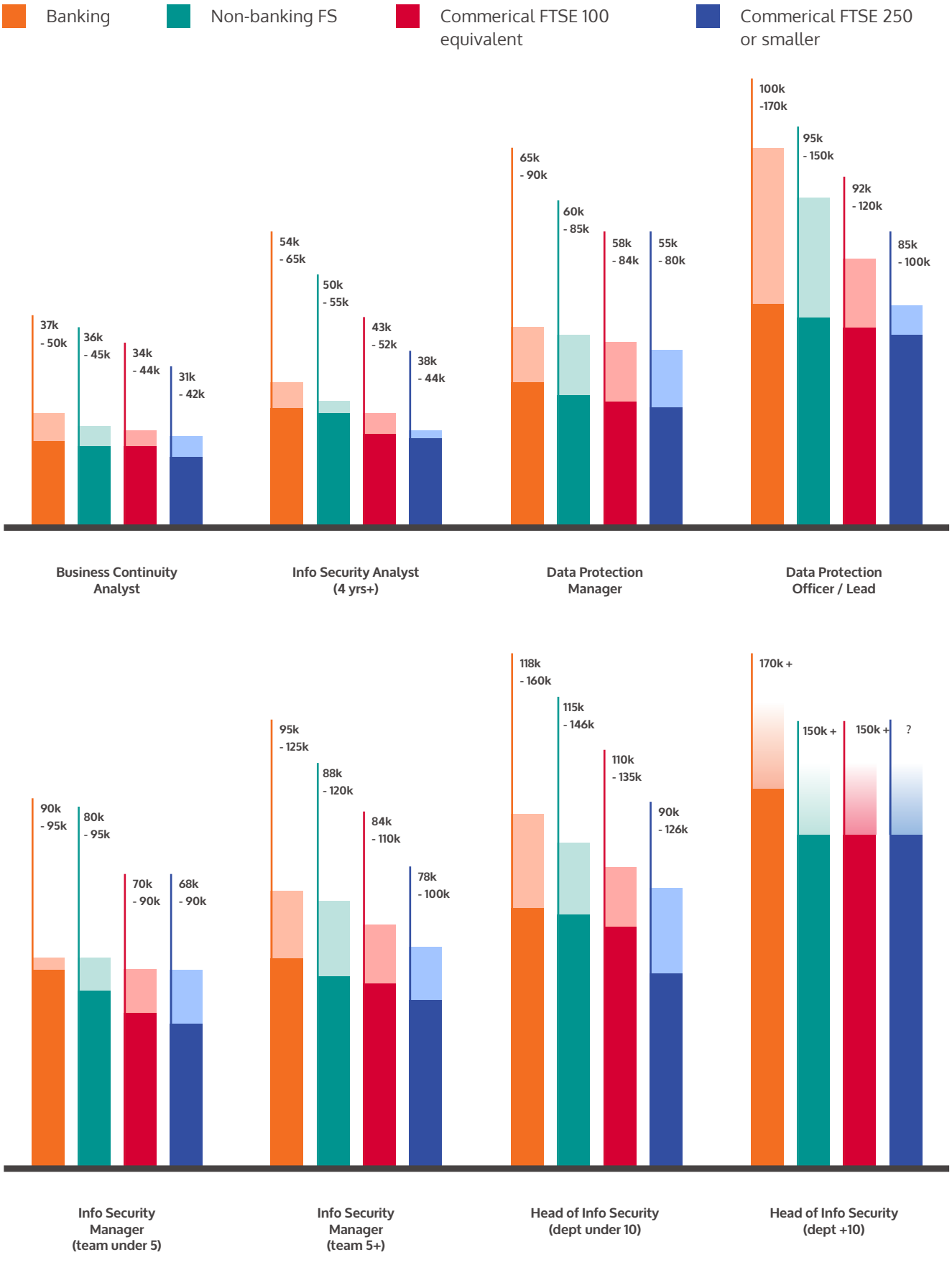
Daily rate in GBP





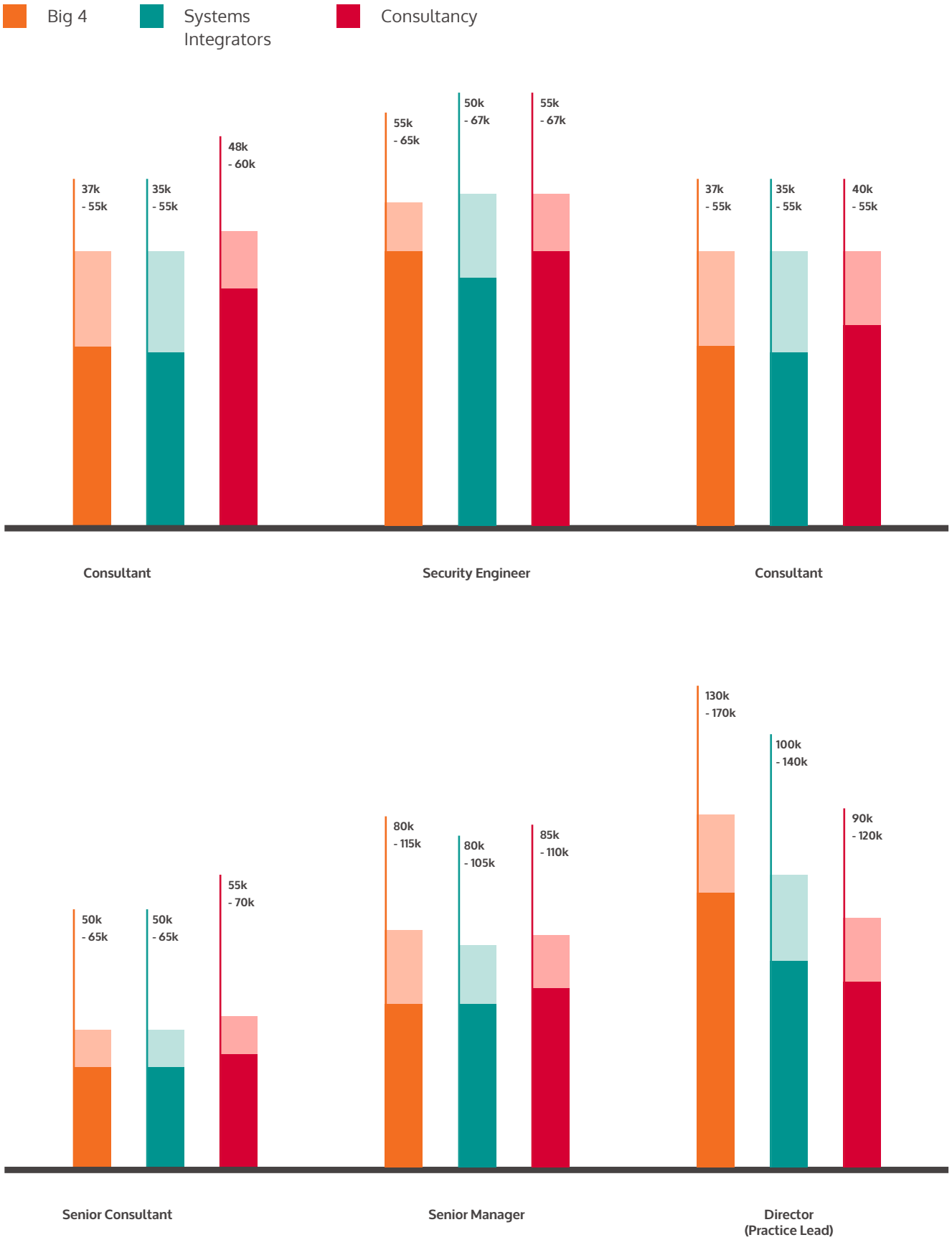
In-house

Gross annual salary in GBP



Consultancies and SIS

Gross annual salary in GBP



Bibliography

1 https://www.pwc.co.uk/economic-services/ukeo/pwcukeo-section4-nowcasting-july-2017.pdf

2 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/november2017

3 https://www.theguardian.com/money/2018/sep/11/unexpected-rise-uk-pay-growth-jobless-total-40-year-low

4 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/labourmarketeconomiccommentary/november2018

5 https://www.ons.gov.uk/employmentandlabourmarket/peoplenotinwork/unemployment/timeseries/mgsx/lms

6 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours

7 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/november2018

8 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/december2018

9 https://www.ons.gov.uk/economy/inflationandpriceindices/bulletins/consumerpriceinflation/november2018

10 https://www.trustarc.com/blog/2018/07/13/trustarc-research-74-of-companies-expect-to-be-gdpr-compliant-by-the-end-of-2018/

11 https://www.gartner.com/doc/reprints?id=1-4O4VC17&ct=180109&st=sb

12 https://www.mckinsey.com/~/media/mckinsey/business functions/organization/our insights/delivering through diversity/delivering-through-diversity_full-report.ashx

13 https://cdn2.hubspot.net/hubfs/2095545/Whitepapers/Cloverpop_Hacking_Diversity_Inclusive_Decision_Making_White_Paper.pdf

14 https://www2.deloitte.com/content/dam/Deloitte/au/Documents/human-capital/deloitte-au-hc-diversity-inclusion-soup-0513.pdf

15 https://www.uta.edu/news/releases/2013/12/briggs-ethnicity-marketing.php

16 https://www.csoonline.com/article/3221606/it-careers/cybersecurity-help-wanted-asperger-people.html

17 https://www.bcs.org/upload/pdf/diversity-report-2017.pdf

18 https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/03/15/2017-03-15-Women-European-Cybersecurity-Workforce

19 https://www.gov.uk/government/publications/cyber-security-skills-strategy/initial-national-cyber-security-skills-strategy-increasing-the-uks-cyber-security-capability-a-call-for-views

20 https://www2.deloitte.com/ch/en/pages/press-releases/articles/women-in-cyber-initiative-press-release.html

21 https://business.linkedin.com/content/dam/me/business/en-us/talent-solutions/resources/pdfs/linkedin-global-recruiting-trends-2018-en-us.pdf

22 https://cybersecurityventures.com/jobs/

23 https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

24 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf

25 https://www.rec.uk.com/news-and-policy/press-releases/demand-for-cyber-security-staff-to-surge-next-year-rec

26 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752074/IR35_web.pdf

27 https://dma.org.uk/article/eprivacy-hold-ups-could-delay-introduction-until-2020

28 https://www.fca.org.uk/publications/multi-firm-reviews/wholesale-banks-asset-management-cyber-multi-firm-review-findings

29 http://www.cbi.org.uk/news/full-speech-ciaran-martin-on-the-national-cyber-security-centre/

About Barclay Simpson

Barclay Simpson is an international recruitment consultancy specialising in internal audit, risk, compliance, cyber and information security, business continuity, legal, company secretarial, and treasury appointments.

Our strength lies in our ability to understand client and candidate needs and then use this insight to ensure our candidates are introduced to positions they want and our clients to the candidates they wish to recruit.

We also provide comprehensive reports and compensation guides for the internal audit, risk, in-house legal, compliance and treasury recruitment markets. All our specialist reports can be **accessed for free on our website**: https://www.barclaysimpson.com/market-report-2019

If you'd like hard copies of any of the reports, or would like to discuss any aspect of them, please contact the following divisional heads:

Company Secretarial	Ian Coyle	ic@barclaysimpson.com
Corporate, Cyber & Information Security	Mark Ampleford	ma@barclaysimpson.com
Legal, Compliance & Financial Crime	Tom Boulderstone	tgb@barclaysimpson.com
Interim Solutions	Andrew Whyte	aw@barclaysimpson.com
Internal Audit	Russell Bunker	rb@barclaysimpson.com
Risk	Josh Lawson	jl@barclaysimpson.com
Treasury	Sophie Spencer	ss@barclaysimpson.com

To discuss our international services, please contact:

Europe	Daniel Close	dc@barclaysimpson.com
Middle East	Tim Sandwell	ts@barclaysimpson.com
North America	Greg Anderson	ga@barclaysimpson.com

BARCLAY SIMPSON.

Barclay Simpson

Bridewell Gate, 9 Bridewell Place
London EC4V 6AW
Tel: 44 (0)20 7936 2601
Email: bs@barclaysimpson.com