Corporate Governance Recruitment

Market Report
Security & Resilience

2017

Barclay Simpson
corporate governance recruitment

Contents

Offices
London
New York
Dubai
Hong Kong
Singapore

Disciplines
Internal Audit
Risk
Compliance
Security & Resilience
Legal
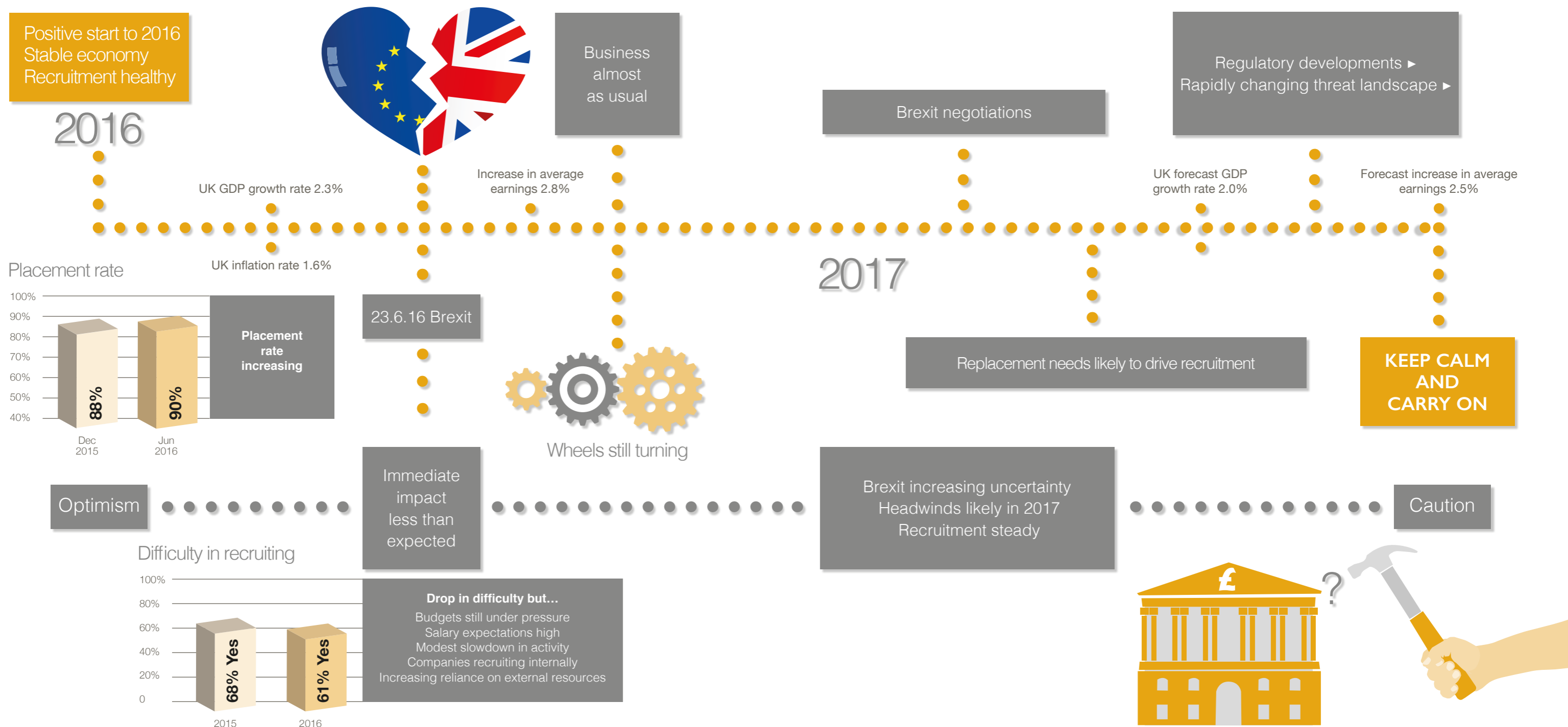Treasury

Introduction 1

Welcome to Barclay Simpson's 2017 Security & Resilience Market Report

Barclay Simpson has been producing corporate governance market reports since 1990. We produce two reports each year. This one, summarising and analysing recruitment trends in the security recruitment market, is supplemented by an employer survey. Later in the year we will be producing our compensation and trends report, which will focus primarily on remuneration and will again be supplemented by a survey of security professionals registered with Barclay Simpson. Comparable reports exist for all other areas of corporate governance. They can be accessed in Section 9 of this report ("About Barclay Simpson") or at **www.barclaysimpson.com**

We place great value on the professional reaction to our reports and would appreciate your comments and any further requests for clarification or information.

Barclay Simpson
corporate governance recruitment

At a glance

2

The Security recruitment market 2016-2017

**Positive start to 2016
Stable economy
Recruitment healthy**

2016

UK GDP growth rate 2.3%

UK inflation rate 1.6%

Increase in average
earnings 2.8%

Business
almost
as usual

Brexit negotiations

Regulatory developments ▶
Rapidly changing threat landscape ▶

UK forecast GDP
growth rate 2.0%

Forecast increase in average
earnings 2.5%

2017

Placement rate

100%
90%
80%
70%
60%
50%
40%

88%

90%

Dec
2015

Jun
2016

**Placement
rate
increasing**

23.6.16 Brexit

Wheels still turning

Replacement needs likely to drive recruitment

**KEEP CALM
AND
CARRY ON**

Optimism

Immediate
impact
less than
expected

Brexit increasing uncertainty
Headwinds likely in 2017
Recruitment steady

Caution

Difficulty in recruiting

100%
80%
60%
40%
20%
0

68% Yes

61% Yes

2015

2016

Drop in difficulty but…
Budgets still under pressure
Salary expectations high
Modest slowdown in activity
Companies recruiting internally
Increasing reliance on external resources

Executive summary

3

Living with Brexit

Our report in July focused on remuneration and was released immediately after the vote to leave the EU. At the time, possibly rashly, we predicted that by the time our 2017 report became available, the consequences of that decision would be better known. Unfortunately, six months later, what might practically be achieved in exit negotiations is no clearer.

This report focuses on employment. Whilst the anticipated Brexit inspired recession has not occurred, the UK is about to start negotiations to leave the EU, an action that even those who support Brexit recognise will do short term damage to the economy. Given this, from our perspective as recruitment consultants, the key to a successful Brexit will be to avoid any serious self-inflicted economic damage.

Economy continues to turn

Brexit has raised the level of uncertainty, which is no friend of the recruitment market. Companies invest and recruit when they feel confident and sit on their hands when they do not. However, outside of a serious economic reverse, as we predicted last year, the security recruitment market, together with the wider economy, will likely learn to live with Brexit. Our experience during the last six months has shown this. Whilst it is not entirely business as usual, the economy is still turning and recruitment decisions continue to be taken.

Recruitment sensitive to the economy

There are very few surveys that do not report how concerned, right up to CEO level, the corporate sector is about security. This is not surprising given the ongoing list of companies that fall foul of security breaches. In terms of cross-border data exchange, third party vendor use, evolving technologies and increased mobile use, there is plenty for CEOs to be concerned about. This leads to the notion that the security recruitment market must be in a constant state of elevated demand with companies throwing money at their security recruitment budgets. Unfortunately, the reality is rather more prosaic. Whilst rising threat levels and well-publicized breaches certainly assist the security recruitment market, the market is in fact more sensitive to trends in the wider economy than the latest security breach. In the immediate aftermath, Brexit temporarily stalled the security recruitment market, but with economic Armageddon seemingly averted, a period of catch up ensued.

Recruitment market remains positive

Our survey results, which broadly reflect our own experience, is that whilst the security recruitment market has slowed, recruitment activity and sentiment remain positive. For example: security managers believe they are better resourced to meet the challenges they face with 38% (32% a year ago) reporting their departments are sufficiently resourced; 38% (33% a year ago) have also benefited from an increase in their recruitment budget; and 67% (69% a year ago) report they have recruited or attempted to recruit in the last six months. These are encouragingly resilient findings.

We will avoid predicting that in a further six months all will have become clear. Whilst economic growth and particularly employment have been far stronger post Brexit than all but a few predicted, it is likely that in 2017 the security recruitment market will be facing some steady headwinds. Rising inflation could also have some interesting consequences for security salaries.

" Whilst rising threat levels and well-publicized breaches certainly assist the security recruitment market, the market is in fact more sensitive to trends in the wider economy than the latest security breach. "

Market analysis

4

Vacancies

Vacancy generation quickly recovers from Brexit shock

Prior to the Brexit vote, the rate at which vacancies were being created in information security was broadly consistent with 2015. Demand was notably strong across all sectors for mid-level practitioners, that is "doers" who could quickly deliver. Operational security skills were also in demand as companies looked to bring these skills in-house.

The Brexit vote had an immediate impact on demand. In a knee jerk reaction, vacancies were put on hold, but this hiatus did not last. Within a matter of weeks, the flow of vacancies resumed, together with the added fillip that a number of companies were also looking to recruit against their temporarily delayed recruitment processes. However, by the end of 2016, vacancy generation had eased, perhaps reflecting the headwinds forecast for 2017.

Recruitment drivers in the second half of 2016 included regulation, as sectors outside of banking were subject to increased levels of regulatory attention. Vacancies became more evenly spread across commerce, with smaller companies accounting for a greater proportion of vacancies. Cyber intelligence continues to be a growth area, as do other IT security operational disciplines, such as incident management and monitoring. A number of senior CISO roles emerged with 2nd line security or cyber risk responsibility. Driving improvements from the 2nd line, as opposed to purely providing oversight, is a continuing theme.

Within corporate security, the slowdown we reported in the financial services sector last year has reversed with the adoption of the 3 lines of defence model. Heightened threat levels, particularly across Europe, are helping support demand. Resilience recruitment is steady but down on the recent past. Senior roles are scarce and specific areas of demand include technical areas such as disaster recovery and IT service continuity. Crisis management is a developing area of demand, falling somewhere between corporate security and resilience.

New vacancies   Closing vacancies
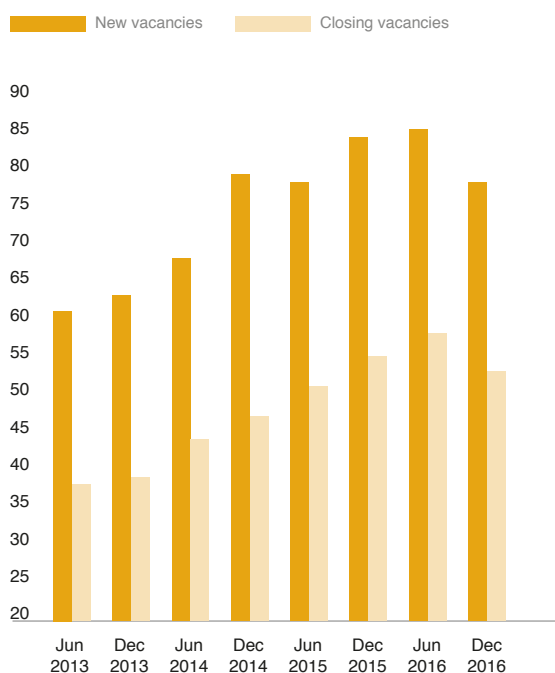
Rate of placements

Rate of placements slows

To provide a better insight into the dynamics of the recruitment market, this graph plots the rate at which placements have been made across the last four years. It reflects the rate at which candidates are accepting offers of employment.

At the beginning of 2016, a sense of urgency was necessary to recruit sought after security practitioners. In response, companies became more flexible, recognising that if they wished to drive recruitment processes forward they needed to be more pragmatic. At the start of 2017, demand had eased. If companies come to the recruitment market with realistic expectations and sensible budgets, they can expect to fill a vacancy. However, recruiting security practitioners with highly specific, in-demand skill sets remains just as challenging.

In-demand skills include roles that require a combination of business facing softer skills and technical understanding, technical risk assessment and application security roles. Operational IT Security roles in SOCs and architect roles are also remaining vacant for longer and are dragging down the overall rate of placements. There is, however, an active supply of contractors in these areas. Given this, employers have tended to move more slowly and be more selective over permanent hires.

Smaller financial services groups have continued to generate vacancies, as they have come under greater regulatory scrutiny. Whilst they are often uncertain about what they can achieve in the recruitment market, they are generally more nimble, completing recruitment processes efficiently and effectively.

Demand for information security expertise is growing in commerce as more companies receive board buy-in. Unfortunately, their expectations can be unrealistic, with hard to achieve requirements and unrealistic recruitment budgets. Many of these vacancies remain open for long periods.

As there is usually a stronger pool of candidates to select from within corporate security, companies usually take longer to make offers. Despite this, the rate of placements has increased across corporate security, with companies in many sectors demonstrating a greater sense of urgency.

Placement rate
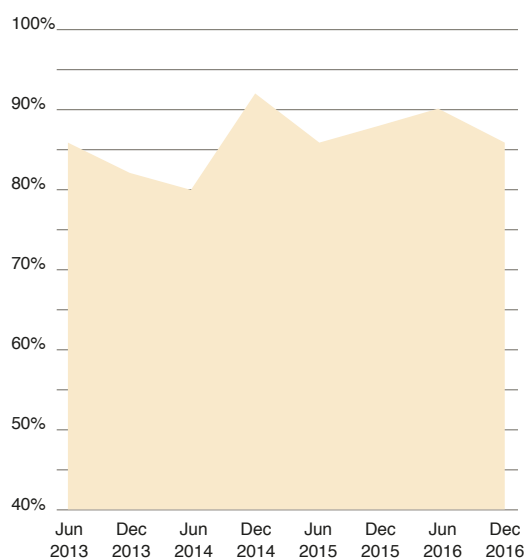
Key conclusions from employer survey

5

The demands on security departments and other areas of corporate governance are without doubt becoming greater. 62% of security departments reported they were not sufficiently resourced to meet the demands made upon them. Encouragingly this was an improvement on the 68% who reported they were insufficiently resourced in 2015. However, more departments report their recruitment budget has fallen at a time when the cost of recruiting security practitioners with the skills and experience required is increasing. The consequences of Brexit are yet to come.

Departments remain under-resourced

- Only 38% of managers believe their security department is "sufficiently resourced for the demands made upon it" (32% in 2015)

Pressure on recruitment budgets remains

- Increase from 33% to 38% in 2016 of security departments reporting an increase in their recruitment budget. 10% now reporting a fall

- Increase in information security budgets (58%) more common than in corporate security (27%)

- Increases now more likely in commerce than in banking and financial services
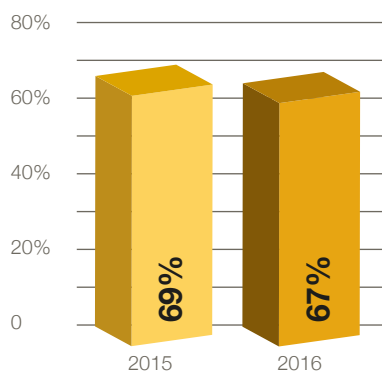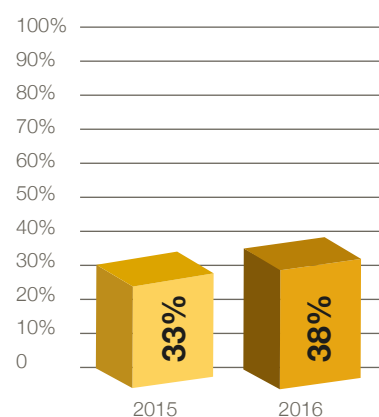
Modest slowdown in recruitment activity

- 67% of security departments have recruited or attempted to recruit in the last 6 months, down from 69% in 2015 and 78% in 2014

- Split between information security at 85% and corporate security at 60%


Fall in departments reporting recruitment difficulties

- 61% of managers report they are finding it difficult to recruit (68% in 2015)

- Split between information security at 74% and corporate security at 48%

## Recruitment of security practitioners not getting any easier

Salary expectations remain high

- 80% of managers (86% in 2015) report candidate salary expectations to be either excessive, beyond their budget or more than expected

- 20% consider salary expectations to be reasonable (14% in 2015)
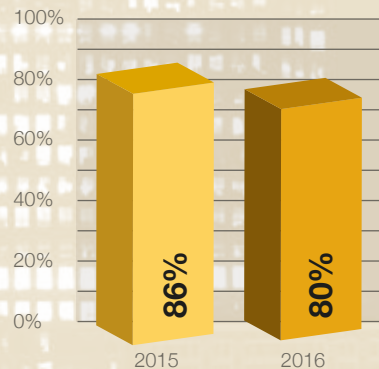
External resources widely utilised

- Only 23% of departments report they never or only on a very limited basis use external resources

- 37% report they routinely use external resources and 40% do so to cover specialist skills

- Contractors still most likely to be used for project specific purposes although becoming more widely used as subject matter experts
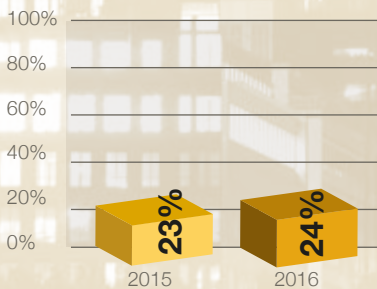
Internal recruitment a significant source of candidates

- 24% (23% in 2015) of managers using internal recruitment as principal source of candidates

- At 39%, external preferred suppliers remain the principal source of recruitment

Replacement recruitment to be main recruitment driver in 2017

- 42% of security departments report replacement recruitment to be their key driver

- At 19% regulation is the second most important

Demand set to continue in 2017

- Only 11% (9% in 2015) of managers report they are unlikely to recruit in 2017

- 61% (59% in 2015) report they are likely to recruit

Brexit yet to have a meaningful impact

- Only 16% of information security managers report that Brexit is influencing the work they undertake (only 7% in corporate security)

- Just 12% of departments are likely to require additional resource as a result of Brexit

Market commentary

6

Our survey suggests that, despite Brexit and the prospect of a weaker economy, the demand for security practitioners is holding up. Companies seem to recognise the importance of security and recruitment budgets are marginally up. Heads of Security report their departments are better resourced and able to meet the demands made on them. However, it remains a tough market to recruit in with 61% of departments still finding it difficult to recruit. This may explain why security departments are coming to rely on internal recruits and the use of contractors.

More security practitioners appointed internally

The percentage of security practitioners recruited internally has increased in each of the last four years.

Where skills are in short supply, internal recruits can be the solution. There is a breadth of areas covered in information and IT security departments including: change, operations, review, policy, strategy, risk assessment and compliance. As such, there is a wide range of disciplines and people employed outside of security, but within companies, that can potentially bring relevant skills to a role in security. It also helps that an increasing number of people are getting involved as stakeholders and subsequently becoming interested in information security; increasing the potential pool of applicants.

Audit and risk departments have always been a source of recruits and many have valuable transferable skills. Given the importance of cyber risk, it is not unusual for an operational risk practitioners to gain knowledge and even qualifications in cyber or information security. Likewise, computer auditors often routinely take an interest in cyber security and their responsibilities are not that far removed from review focused information security roles. They too often see the benefit of gaining an information security qualification. Larger banks have regularly recruited information security practitioners into their internal audit departments to ensure their third line of defence has suitable expertise. Some of these auditors are now returning to security and, having focused on cyber threats, already have a relationship with the CISO.

Internal recruitment can also be reactive to a specific need. Security Operations Centres regularly recruit from Network Operations Centres. As one would expect, security functions going through major transformations recruit internally from programme management or business change functions.

It is also not uncommon for a CISO or senior cyber leader to be recruited internally for their leadership rather than their subject matter expertise. They are usually recruited from corporate security, audit, risk and programme management.

" It remains a tough market to recruit in with 61% of departments still finding it difficult to recruit. This may explain why security departments are coming to rely on internal recruits and the use of contractors. "

Market commentary

6

Brexit's modest impact

Although early in the process, our survey asked if Brexit was influencing the work that security departments were undertaking or was likely to impact on the resources their departments required. We were not surprised by the modest impact reported, particularly from security departments within industry and commerce. However, the implications that Brexit could have on freedom of movement may bring into focus the reliance UK based security departments place on European recruits.

What's currently driving the recruitment market?

There are two main drivers.

1. Regulatory developments

General Data Protection Regulation (GDPR) is looming and companies are reacting by pushing privacy changes towards information security departments. They are encompassed as part of wider information security policies and to drive change in the business. This increased workload is creating vacancies and is likely to continue to do so.

Regulators are also increasing the demands made on the financial services industry. Whilst their focus was previously on banking, the wider financial services sector is now having to respond and demonstrate the necessary enhancements and improvement programmes. Recruitment is often focused on creating the capacity for companies to produce the required management information. Regulatory influence is not confined to financial

services. For example, telecom groups have actively recruited from the financial services sector as they adjust to becoming more heavily regulated. Recruits must have the skills and experience to put the processes in place to ensure regulatory requests are handled effectively.

2. Rapidly changing threat landscape

Companies are conducting more business digitally. Previously off-line businesses are facing major risks and have had to invest to understand and mitigate these risks. These changes in the way businesses operate present multiple threats. The Internet of Things (IoT) and cloud computing are the most obvious ways in which businesses are changing and need to invest to counter the new level of threats they face.

"Companies are conducting more business digitally. Previously off-line businesses are facing major risks and have had to invest to understand and mitigate these risks. These changes in the way businesses operate present multiple threats. "
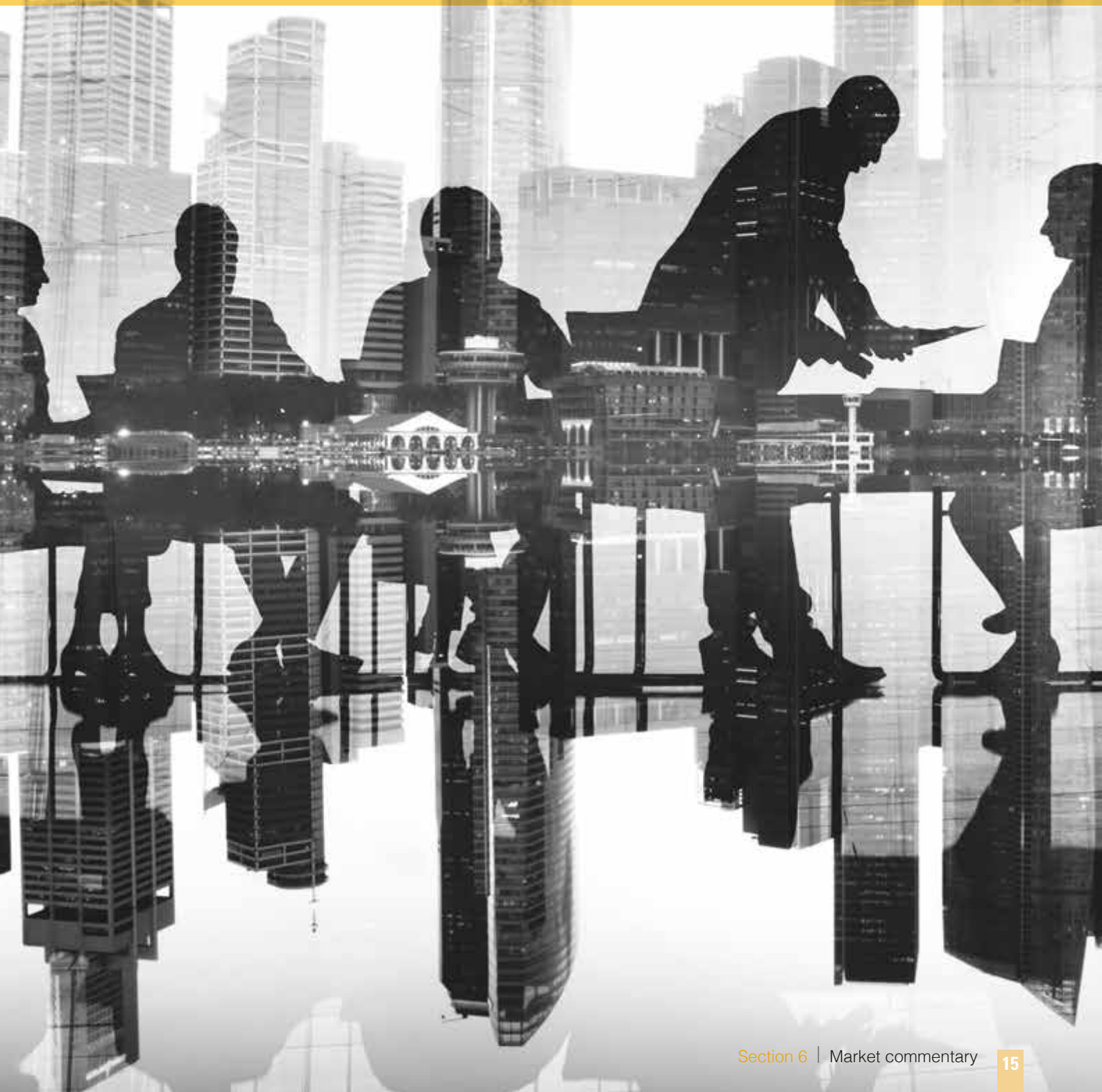
Market commentary

Some further observations

Information security practitioners least likely to be in demand are those who do not have a good technical understanding. Whilst information security is not necessarily a technical discipline, it interacts with technical experts. Purely policy focussed practitioners are struggling in the recruitment market. Many consider their best option is to move into data privacy or data protection.

We have already written that security staff are more likely to be recruited internally and commented on the effort companies will make to retain their staff. One effect of this is that security practitioners are more likely to be promoted earlier. This is resulting in more junior security practitioners being sought at the expense of managers.

Many security practitioners looking for new positions are sensitive about their potential job title and, perhaps not unreasonably, look for titles that reflect greater responsibility. Given the plethora of more junior positions, it is not unusual for companies to inflate a job title with a reference to management where such responsibilities do not exist. Many security practitioners are now sensitive to this and will only settle for a role and a job title that meets their expectations.

Sector observations

Financial Services

The mainstay of a significant proportion of demand in information security - the top tier investment and retail banks – recruited at much lower volumes in 2016. Notwithstanding a tougher operating environment, these banks are under siege from a myriad of smaller competitors and the explosion of Fintech groups operating in niche and sometimes completely novel service lines. As already discussed, many of these banks are under pressure to recruit internally. In their absence, their smaller rivals are creating or enhancing their information security and cyber security capability. These greenfield opportunities often require different skills to longer term BAU roles. For those seeking a new challenge this is generally positive as demand is displaced to these smaller groups offering more interesting and broadly based roles.

During 2016, the insurance sector was buoyant with almost unprecedented demand. Clients commented that they: "were playing catch-up with the banking sector" and "recruitment was necessary just to be able to provide the management information required by the regulator". Others in the sector highlighted a need to be as secure as possible, given the risk to their reputations as providers of cyber insurance. Whilst we are expecting demand to wane from larger groups in 2017, smaller, niche groups should remain active.

Security operations continues to be an area of investment as groups look to enhance their outsourced SOCs with internal points of contact. We have seen a range of roles including security operations management, incident response and monitoring analysts. Whilst financial services groups would have seen an external SOC as a satisfactory solution there is now more in-house resource to complement their external SOC.

> "Many more companies are now open to attack. With the development of the Internet of Things and heavy reliance on applications, commercial groups across many sectors are experiencing a massive change in their risk profile."

The broader physical security requirements within the industry have remained steady as financial services groups have traditionally invested in them. However, a focus on intelligence led security is leading to enhanced demand for intelligence focused security professionals.

Resilience is currently on the regulatory agenda, providing a steady flow of what are usually replacement rather than newly established positions.

Commerce

Within commerce, information and cyber security now has a significant level of 'buy in' at board level. This is being reflected in a higher volume and diversity of roles.

Many more companies are now open to attack. With the development of the Internet of Things and heavy reliance on applications, commercial groups across many sectors are experiencing a massive change in their risk profile.

Whilst the telecoms, pharmaceutical and utilities sectors are, in information security terms, relatively mature sectors, even in these regulated sectors, new CISOs are being appointed with enhanced reporting lines and budgets.

Sectors where information security has historically seen little investment, such as manufacturing and a number of service industries, are now expanding or creating new functions. This is providing security practitioners with greater opportunities to shape their own careers as they develop security roadmaps from embryonic stages.

Salaries remain an issue for many companies. They often have no experience of recruiting security practitioners and come to the recruitment market with unrealistic expectations. This can result in extended recruitment exercises as they exhaust the recruitment market seeking a candidate within their budget.

Many smaller companies establishing information security functions for the first time look for a virtual CISO service or a freelancer to take the lead on a part time basis. Given they will often report to an executive with limited security expertise, this can be sensible and allows greater clarity of what is needed before a permanent appointment is made. It also helps with the formation of realistic job descriptions given the frequent disparity between what a company expects the recruitment market to deliver and what is realistically available.

There is currently less demand for cyber type roles compared to the financial services and consultancy sectors and more broadly based IT / Information Security roles where candidates are expected to be competent across a wider range of areas.

The telecoms sector currently remains the largest recruiter of information and cyber security skills, with the travel and retail sectors expanding. Law firms, no doubt shocked by the Panama Papers, are investing heavily but embedding the changes CISOs advise in a partnership environment is challenging.

Although corporate security does not have the same profile at executive level enjoyed by information security, it is taken seriously. However, along with resilience, this does not always translate into external recruitment.

Consultancies and Systems Integrators

Last year we reported that there was a chronic shortage of candidates available to meet increasing demand from the consulting sector. This has not changed.

Despite this, consultancies have not relaxed their recruitment criteria. They remain committed to attracting recruits who are not only able to deliver a service, but also able to help build market share. These are security consultants with

Market commentary

strong commercial skills and a level of technical understanding or consultants who have expertise in areas of technical security, such as SIEM, Penetration Testing, Incident Response and Identity & Access Management.

Salaries are rising as some consultancies are beginning to offer above market rate salaries to attract candidates away from in-house lower travel roles. Some consultancies, who could previously rely on their brand and career development potential to attract candidates, in addition to higher salaries, are offering other benefits such as flexible working hours, home working and fast track progression.

For the first time, salaries in the consulting sector are consistently above those in commerce. However, consultancies are losing candidates to the contract market which is an obvious attraction to consultants already familiar with an assignment based work culture.

With GDPR coming into effect in 2018, there is already high demand for candidates with relevant experience. We expect this to continue as pressure grows on consultancies to ensure their clients are GDPR ready.

Other drivers in the sector are the number of clients looking to move to the Cloud and Digital Transformation projects. Candidates with experience of successfully delivering these types of projects are increasingly sought after.

Demand from corporate security consultancies continues to be hit by the travails in the energy and extractive sectors. There is no shortage of candidates interested in these sectors. Protective security operations are a short step from government service. It is also an obvious move into geopolitical/security analysis for those with relevant Masters Degree programmes. However, the number of potential candidates at junior levels continue to outweigh the number of opportunities.

Whilst resilience consultancies continue to grow, particularly within the Big 4, recruiting candidates with the ability to consult as well as sell remains a challenge. Although UK practitioners are viewed as market leaders, it remains to be seen if high demand from overseas markets will continue.

The contract market

Demand for contractors in 2016 was steady and driven by regulatory pressures, the Internet of Things (IoT) and cloud migration programmes. A trend from our survey is that contractors are becoming increasingly likely to be used as subject matter experts rather than for project specific purposes. It is also notable how the routine use of contractors is increasing.

The increase in demand for IoT experience skills is particularly evident within the manufacturing, retail and telecom sectors. With companies under pressure to manufacture and release new products, security is not the afterthought it once was. Demand is often driven by a failure to recruit on a permanent basis, together with the acknowledgement that security specialists who have worked in a number of different environments are more likely to be contractors.

Many of the new roles released at the end of 2016 were regulatory and, in particular, GDPR driven, which we expect to continue throughout 2017 as the May 2018 deadline looms. Replicating the demand for contractors with PCI DSS compliance experience, an uplift of up to 30% is potentially available for contractors with strong Data Protection experience. This is encouraging otherwise permanently employed Data Protection practitioners to become contractors, which in turn creates vacancies that are often filled by contractors!

We anticipate the demand for contractors to be buoyant in 2017 and to be led by regulatory demands.

Salary guide

7

We reported in our main Compensation and Market Trends Report six months ago that the average salary increase achieved by security practitioners changing jobs was 16%, down from 17% in 2015. The increase for those staying with their existing employer rose from 4.9% in 2015 to 5.6% in 2016.

Despite the uncertainty caused by the Brexit vote and a low inflation environment, salary pressures remained in 2016. The response to our survey suggests that salary expectations remain high although marginally down on 2015. 80% of security departments felt that candidate salary expectations were either more than expected or excessive, down from 86% in 2015. This pressure is more keenly felt in information security than corporate security.

Going forward, after a period when the UK economy flirted with deflation, inflation is likely to have a greater influence on the recruitment market than recently. We have been surprised at the number of security practitioners who reported to have received no salary increase for staying with their existing employer or only a marginal one. In 2016, 25% of security practitioners reported their salary had not increased and 23% reported that their increase was below 2.5%. In a low inflation environment, this is possibly understandable, however given that inflation is likely to exceed 2% in 2017, many of these departments will need to offer their security practitioners salary increases at least in line with inflation or their real earnings could materially fall. Whilst many of those who have received no increase will have already concluded that given their poor marketability there is little they can do in terms of changing employer, inflation is likely to have an unsettling effect on the wider security recruitment market. Clearly amongst more marketable security practitioners there is an expectation that their salary will increase, not only in nominal, but also in real terms. If it does not, entering the recruitment market is the obvious solution.

Given the competition for security expertise, particularly for those practitioners with in demand skills and experience, we anticipate the pressure on security salaries will continue. Even for those companies that are creative and efficient in their recruitment processes and are able to offer good career development opportunities and possibly flexible working, when it comes to salaries, it is difficult to successfully recruit without offering at least close to market rates. Market rates are likely to rise further during 2017.

Salary guidance

Barclay Simpson analyses the salary data that accumulates from the placements we make in the UK. This provides a guide to salaries for security practitioners.

The salary ranges quoted are for good rather than exceptional individuals and take no account of other benefits in addition to salary that usually accrue to security practitioners, such as bonuses, profit sharing arrangements and pension benefits.

Barclay Simpson will release a Compensation and Market Trends Report in July that will include detailed information on salaries.

Selected profiles - permanent

Salary £000

Profile	Description	London (£000)	Regional (£000)
Senior Data Protection Analyst	Team member in a small DP department for a large mobile telecommunications group. Proven experience in a similar role and ISEB qualified.	~48–53	~40–47
Security Analyst	Generic information and IT security consulting and project delivery in a large retail financial services company.	~50–60	~43–52
Senior Security Consultant	Working for an SI, undertaking security consultancy and delivering on security projects for a large-scale client. Senior person also involved in bid/proposal work and mentoring.	~55–73	~50–67
CCP	Senior level in a security practice of a large consultancy or SI. Skills in security architecture, security policy formulation and review, and risk assessment. Also undertakes business development activities.	~60–95	~53–85
Senior Business Continuity Consultant	Working for a large consultancy firm, delivering and managing consulting engagements and in some cases managing junior staff. Some sales and business development responsibility.	~67–75	~53–63
PCI QSA	Practicing QSA working with external clients and managing their entire PCI compliance programme.	~67–78	~57–67
SIEM Consultant	Technical specialist with strong skills with a leading SIEM solution such as ArcSight or RSA envision. Design, implementation and integration experience. Client facing consultative role.	~72–87	~63–80
Identity & Access Management Consultant	Solid skills in identity and access management design and architecture. Background of working in consultancy, with good client-facing skills and bid work experience.	~67–80	~57–67
Security & Compliance Manager	Security Manager responsible for the business meeting compliance standards such as ISO27001 and PCI.	~73–85	~63–72
Security Manager	Security background in a small financial services company. Demonstrable management experience. No permanent reports. Will utilise consulting firms and contractors on an ad-hoc basis.	~83–92	~72–82
EMEA Manager of Data Protection	Medium to large insurance group. No direct reports. EU Data Privacy legislation experience.	~78–88	~67–73
Network Security Team Leader	Working in a FTSE 100 group leading a team of 6-8 network security specialists, reporting directly to the Head of Security. 10 years' experience.	~83–92	~72–82
Head of Business Continuity	Major financial services group, a large team to manage/supervise. Established career history within BCM.	~105–145	~95–115
Head of Security	Managing a team of 8 security professionals in a financial services company, assisted by 2 more junior managers. Significant management experience and wide security experience.	~125–150	~95–113

Legend: London | Regional

Salary guide

Selected profiles - contract

Per day £	300	350	400	450	500	550	600	650	700	750

Security Architect
Review and creation of technical security designs. Deployment of Security solutions and architecture, exposure to mobile/cloud/network solutions. Holds CISSP/TOGAF/SABSA/ knowledge of OWASP.
London: 650–720; Regional: 650–710

Data Privacy Officer/Lead
Experienced in the security and regulatory implications of Data Protection compliance with emphasis on EU General Data Protection Regulation. Holds ISEB/ PDP/CIPP/E.
London: 700–750; Regional: 600–700

Data Privacy Analyst
Experience of DPA 98 and EU Privacy Directive 95/46/EC, required to provide specialist privacy knowledge and support.
London: 430–480; Regional: 350–400

Security Consultant
Providing security advice across the business, ranging from policy review and development, to information risk reviews. Holds CISSP or CISM.
London: 540–600; Regional: 500–550

Technology Risk Consultant
Good technical understanding with the ability to identify, assess, manage and report risk. Working with different projects within the organisation on varying technologies.
London: 550–600; Regional: 530–550

SOC Consultant
Technical specialist with strong skills in leading SIEM solutions such as design, implementation and integration. Often also involved in elements of policy oversight and review.
London: 550–580; Regional: 500–550

PCI Consultant
PCI Consultant who can work with the client to ensure compliance to PCI-DSS standards.
London: 550–600; Regional: 550–600

Penetration Tester
SME in application security, code reviews and vulnerabilities, attacks and countermeasures with a deep knowledge of hacking and penetration testing techniques, methodologies and tools across web application and infrastructure.
London: 530–580; Regional: 480–550

Business Continuity Consultant
Managing a team of 8 security professionals in a financial services company, assisted by 2 more junior.
London: 500–520; Regional: 400–450

Legend: London Regional

Salary chart - end users

| Salary £000 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 | 110 | 120 | 130 | 140 | 150 | 160 | 170 |

Business Continuity Analyst (2 yrs+)
Info Security Analyst (3 yrs)
Info Security Analyst (4 yrs+)
Data Protection Manager (5 yrs+ no team)
Business Continuity Manager (4 yrs+ no team)
Info Security Manager (team under 5)
Info Security Manager (team 5+)
Head of Info Security (dept under 10)
Head of Info Security (dept 10+)

Banking | Non-banking FS | Commercial FTSE 100 equivalent | Commercial FTSE 250 or smaller

Salary chart - consultancies and SIS

| Salary £000 | 30 | 40 | 50 | 60 | 70 | 80 | 90 | 100 | 110 | 120 | 130 | 140 | 150 | 160 | 170 |

Penetration Tester (under 4 yrs exp)
Consultant
CHECK Team Member
Senior Consultant
Manager
CHECK Team Leader
Senior Manager
Director (Practice Lead)

Big 4 | Systems integrator | Large consultancy | Boutique consultancy

Employer survey results

8

The key conclusions from our employer survey results are contained in Section 5 of this report. Here are the survey results from which the conclusions were drawn.

Respondents to our survey were individuals with responsibility for recruitment who were asked questions designed to elicit their perspective on the recruitment market.

Demand

Pressure on resources easing

Q Do you feel your department is sufficiently resourced for the demands that are made on it?

Sector analysis 2016

Yes		No	
35%		65%	Information Security
46%		54%	Corporate Security
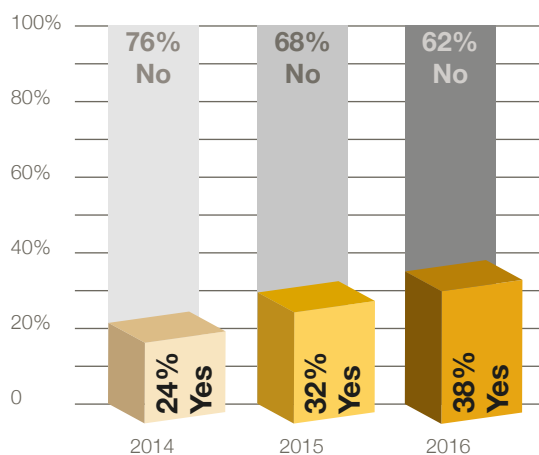
Level of activity down, but remains high

Q Have you recruited, or attempted to recruit, externally in the last 6 months?

Sector analysis 2016

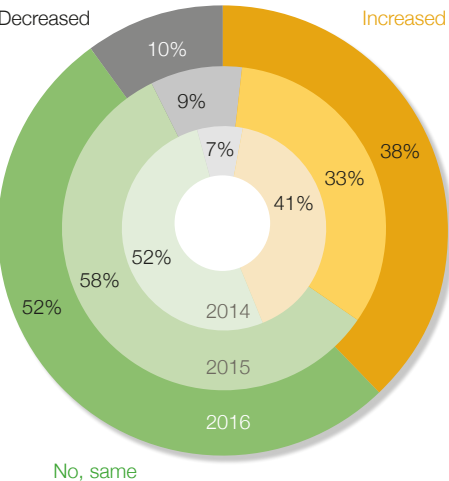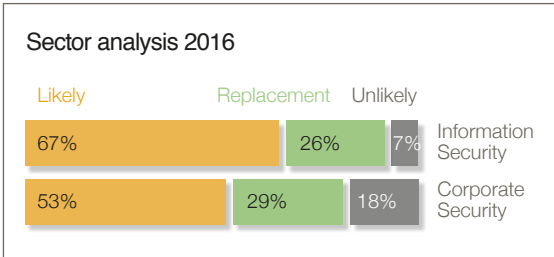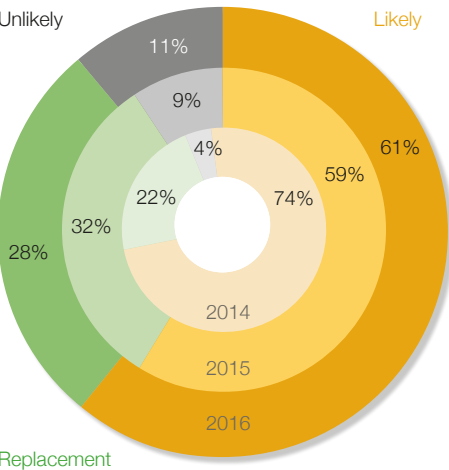| Yes		No	
85%		15%	Information Security
60%		40%	Corporate Security
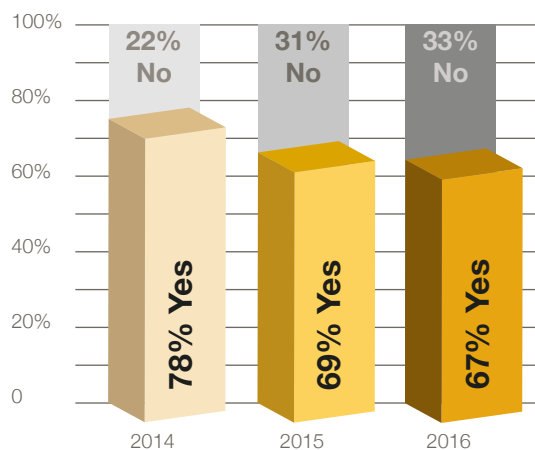
Information security budgets increasing over corporate security

Q Has your recruitment budget increased in the last year?

Decreased
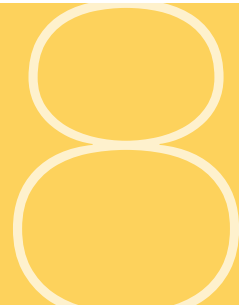
Increased

10%

9%

7%

38%

33%

41%

52%

58%

52%

2014

2015

2016

No, same

Sector analysis 2016

Increased   No, same   Decreased

58%	34%	8%	Information Security
27%	60%	13%	Corporate Security
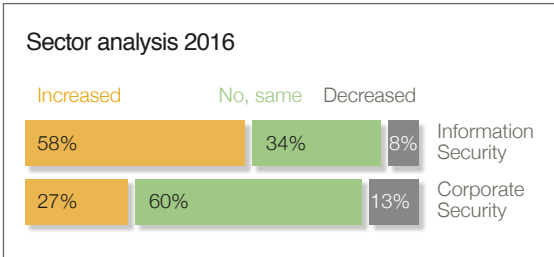
Just 11% unlikely to recruit in 2017

Q What are your recruitment plans for 2017?

Unlikely

Likely

11%

9%

4%

61%

59%

74%

22%

32%

28%

2014

2015

2016

Replacement

Sector analysis 2016

Likely   Replacement   Unlikely

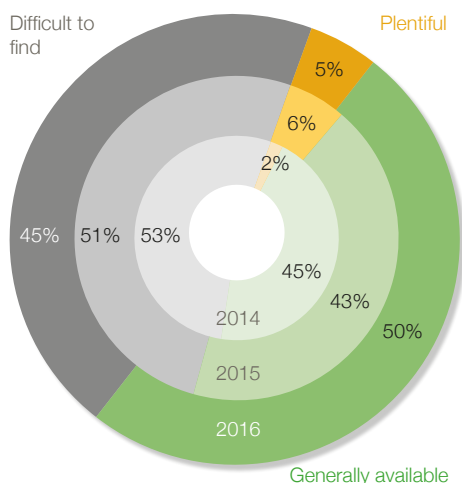|			
67%	26%	7%	Information Security
53%	29%	18%	Corporate Security

Employer survey results

8

Candidate availability

Good candidates remain hard to find
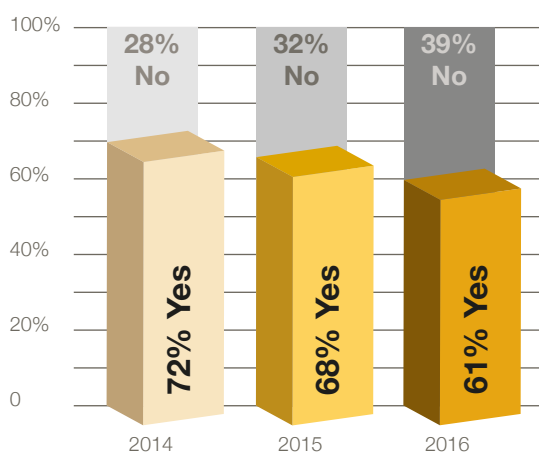
Q How would you rate the availability of candidates?

Difficult to find

Plentiful

5%

6%

2%

45% 51% 53%

45%

43%

50%

2014

2015

2016

Generally available

Sector analysis 2016

Plentiful   Generally available   Difficult to find

3%	34%	63%	Information Security
6%	63%	31%	Corporate Security
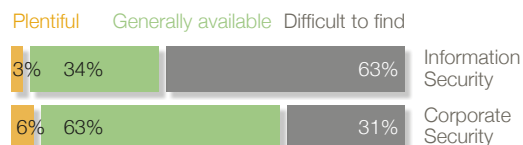
Recruitment remains a challenge

Q Overall, have you found it difficult to recruit?

28% No	32% No	39% No
72% Yes	68% Yes	61% Yes
2014	2015	2016

Sector analysis 2016

Yes   No

74%	26%	Information Security
48%	52%	Corporate Security

Interpersonal skills hardest to find

Q What has been the greatest challenge?

	2014	2015	2016
Interpersonal skills	44%	47%	58%
Technical skills	56%	53%	42%
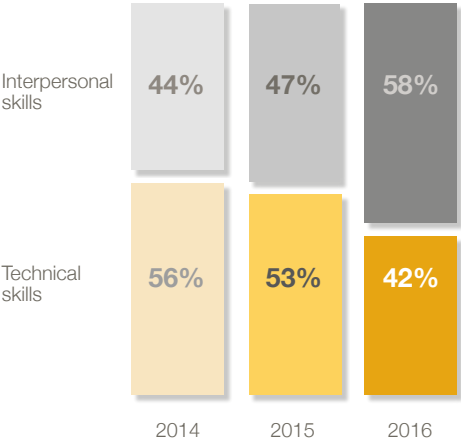
Use of contractors

Subject matter expertise becoming more important

Q What is your main reason for using contractors?

Subject matter specific

Project specific

30%
18%
5%
62% 2014
52% 2015
39%

33%
30%
31% 2016

BAU
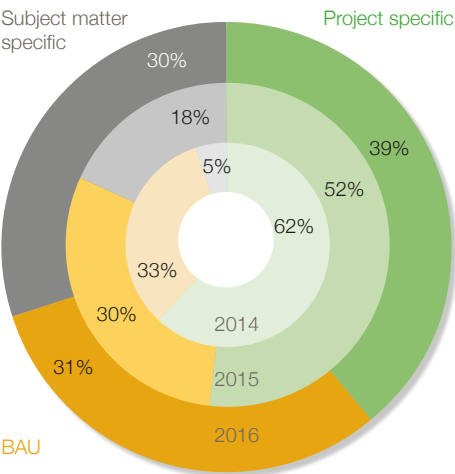
Contractors widely used

Q To what extent do you rely on contractors?

Routinely

Very limited

37%
18%
15%
25%
23%
30%

60% 2014
52% 2015
40% 2016

Specialist skills

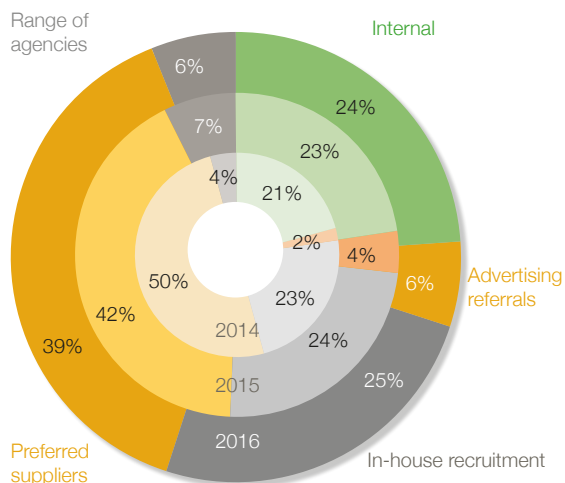# Employer survey results

8
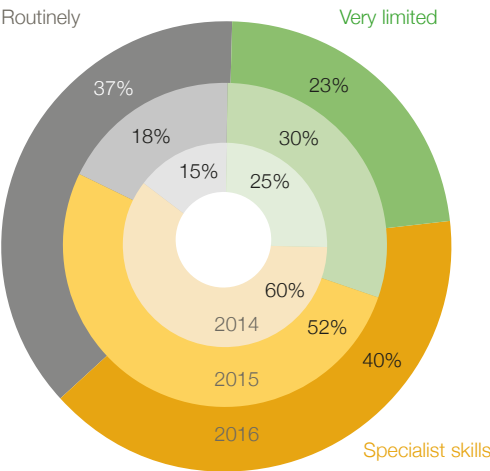
Other findings

Little change in sources of candidates

Q What is your principal source of candidates?

Range of
agencies

Internal

6%

7%

24%

4%

23%

21%

2%

4%

50%

23%

6%

42%

Advertising
referrals

39%

2014

24%

2015

25%

2016

In-house recruitment

Preferred
suppliers

Salary expectations high but generally affordable

Q What has been your perception of candidate salary expectations?

Reasonable

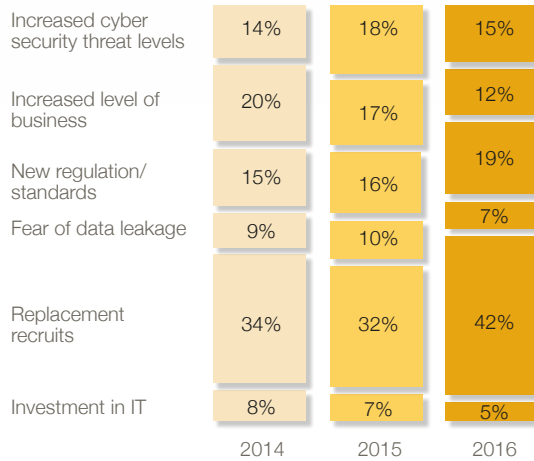Excessive

20%

18%

14%

20%

11%

22%

67%

66%

62%

2014

2015

2016

More than expected

Sector analysis 2016

Excessive   More than expected   Reasonable

Excessive	More than expected	Reasonable	
26%	58%	16%	Information Security
13%	64%	23%	Corporate Security
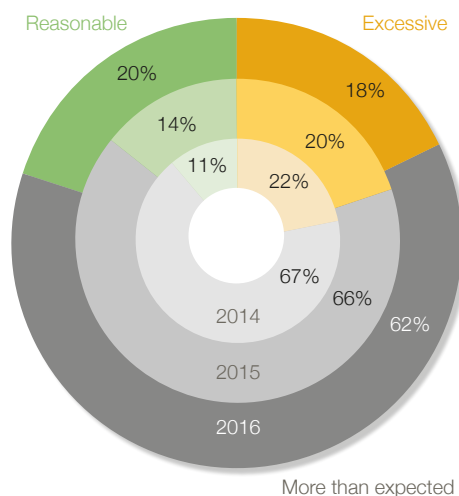
Replacement likely to be biggest recruitment driver

Q Which will be the most important recruitment driver in 2017?

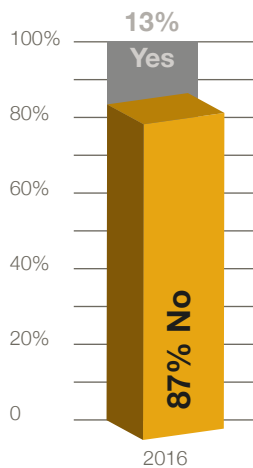|	2014	2015	2016
Increased cyber security threat levels	14%	18%	15%
Increased level of business	20%	17%	12%
New regulation/ standards	15%	16%	19%
Fear of data leakage	9%	10%	7%
Replacement recruits	34%	32%	42%
Investment in IT	8%	7%	5%

Minimal change in diversity and inclusion targets

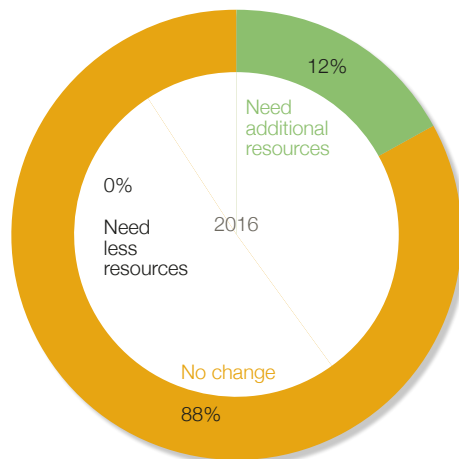Q Do you have any diversity and inclusion targets that may influence your recruitment decisions?

	2014	2015	2016
Yes	40%	37%	38%
No	60%	63%	62%
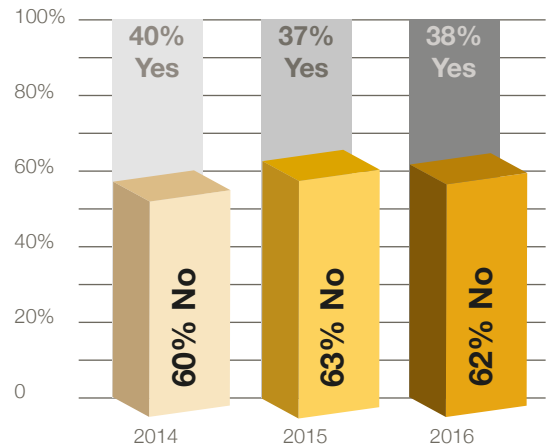
Brexit having a bigger impact in financial services

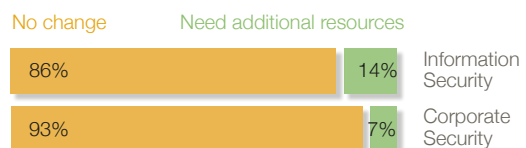Q Is Brexit already influencing the work undertaken by your department?

13% Yes
87% No
2016

Sector analysis 2016

	Yes	No	
	16%	84%	Information Security
	7%	93%	Corporate Security

Q How is Brexit likely to impact the resources your department requires?

12% Need additional resources
0% Need less resources
2016
No change 88%

Sector analysis 2016

No change	Need additional resources	
86%	14%	Information Security
93%	7%	Corporate Security

About Barclay Simpson

9

Barclay Simpson is an international corporate governance recruitment consultancy specialising in internal audit, risk, compliance, security & resilience, business continuity, legal and treasury appointments.

Established in 1989, Barclay Simpson works with clients in all sectors throughout the UK, Europe, Middle East, North America and Asia-Pacific from our offices in London, New York, Dubai, Hong Kong and Singapore.

We add value by using our unique focus on corporate governance, our highly-experienced specialist consultants and access to both the local and international pools of corporate governance talent.

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

For more in-depth coverage, comprehensive reports and compensation guides exist for the Internal Audit, Risk, Security & Resilience, Compliance and Legal recruitment markets. These can be accessed from the links below.

We also produce other specialist reports, each of which can be accessed for free on our website: **www.barclaysimpson.com**

www.barclaysimpson.com/internal-audit-market-report-2017

www.barclaysimpson.com/risk-management-market-report-2017

www.barclaysimpson.com/compliance-market-report-2017

www.barclaysimpson.com/security-and-resilience-market-report-2017

www.barclaysimpson.com/legal-market-report-2017

Barclay Simpson

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

If you would like to discuss any aspect of the reports please contact the following divisional heads:

Corporate Governance	Adrian Simpson	as@barclaysimpson.com
Internal & IT Audit	Tim Sandwell	ts@barclaysimpson.com
Risk	Dean Spencer	ds@barclaysimpson.com
Compliance	Tom Boulderstone	tgb@barclaysimpson.com
Security	Mark Ampleford	ma@barclaysimpson.com
Legal	Jane Fry	jf@barclaysimpson.com
Interim	Andrew Whyte	aw@barclaysimpson.com

To discuss our international services, please contact:

Europe/Middle East	Tim Sandwell	ts@barclaysimpson.com
Asia Pacific	Russell Bunker	rb@barclaysimpson.com
North America	Daniel Close	dc@barclaysimpson.com

Barclay Simpson
corporate governance recruitment