Articulating your worth to the boardroom

The implications of the annual salary survey from SSR Personnel and ASIS International, where data is collated from more than 12,000 security professionals across 40 business sectors.

Employment, salaries and inflation statistics

The UK Office of National Statistics (ONS) reports that in Q1 2019 UK wage inflation was 3.4%, whilst Consumer Price Index annual inflation (CPI) averaged 1.8 %. In general, mid-management salaries and bonuses increased by 5.4%.

According to Eurostat, the average mid-management salary in the UK was £84,500, the fourth highest in Europe, with Swiss workers at No 1, followed by Germany and Luxembourg. The numbers in employment in the UK, 32.7 million, increased by 300,000 over the past 12 months. Those classified as inactive (people who chose not to work) was just under 7 million. The official UK jobless rate reduced to 3.8 % (1.3 million, the lowest percentage since 1974, whilst UK population has grown by 10 million between 1974 and 2019.

From January to March 2019, there were an estimated 852,000 vacancies in the UK, 32,000 more than a year earlier. These are primarily in the health care sector, 15.6 %, followed by the hospitality and food sector. In the security technology sector, SSR estimates there is a vacancy rate of 1.2 jobs per 100 workers. Many of these are being created in value enhanced roles, implementing and connecting technology, mirroring the surging telecommunications sector.

Skills Shortages

The monthly SSR/Pertemps sponsored CBI Report on Jobs has highlighted skills shortages across the UK which are affecting corporations. The UK is still attracting talented Europeans, but the pool of talent has diminished in the past two years. Home-grown graduates are entering the UK jobs market and being attracted to sectors such as "FinTech", the application of technology to improve financial activities. FinTechs in general are disrupters, changing process to introduce new applications, processes and products. Anti-money laundering and fraud prevention are typically areas that benefit from this technology.

Convergence has benefits and perils

Convergence has immediate effects: reduced costs across almost all industries; merging mechanical engineering and wet services, physical security and IT. The logic is sound until the CEO's greatest nightmare – losing data to a hacktivist; the Board non-executive being associated with an organisation in which the preventable death of an employee results in a corporate manslaughter charge; or the COO paying a ransom demand when the firm's driver booking platform was hacked pre their initial stock exchange listing.

The elements of those corporate crises need a rehearsed solution, and for some firms that experience is not available, as the person at the top does not have the mental agility to keep all the plates spinning or depth of experience within the lean corporation.

We have seen within the Boards of the 1,000 largest corporations in Europe over the past twelve months, an understanding that they cannot be passive in regards to resilience. Shareholder and regulatory authorities will not forgive mistakes, and fines will be levied for persistent miscreants.

Being fined 4% of your global revenues under GDPR has increased the salaries for those that work in the security risk function in the UK who have embraced GDPR, becoming the 'go-to' experts. As looks likely, Facebook may be fined €50bn in the EU for data sharing in Mexico to a third party.

Non-compliant anti-regulatory behaviour can be deep rooted into everyday business practice, only exposed by whistleblowers or hackers. It also highlights the three major differences in data management: China, where they seek to control data; the EU, which seeks to protect personal data; and the Americas, where data has traditionally been there to be commercialised.

We are seeing these concepts clashing by way of fines which will dwarf the banking regulator fines and compensation levied collectively at the twenty largest banks since 2008 of €321bn, the top four UK banks paying €50bn in fines and compensation. Since 2008 the same large banks have made €1 trillion in profit.

Getting a salary increase

This year's salary survey reveals that 44% of participants increased their salary through annual review, 20% by changing their jobs (down from 22% in 2018),18% though increased responsibility and 7.9% through formal job revaluation. On the whole, applicants seeking to change jobs was less than 45%, whilst in 2010-2012 that figure was over 59% of those in the job market. In general, physical security remains cost controlled for many end-user clients. Empathetic gapping is emerging: this occurs where the business wants to devolve non-essential activities, usually to traditional outsourcers, but compliance risks have to be managed by a corporate person.

The risk management function is increasingly attractive as a profession, as there is a high level of qualifications that can be achieved which attracts the Millennial workforce who seek a greater diversity of work experience. Investments in global security operations centres (GSOC) in 2018-19 led to ten major investment programmes.

The diversity of monitoring undertaken (people, assets, regulatory requirements) requires a different skill-set when recruiting project teams where a diversity of experience is in short supply. India and Asia have seen significant investment, but senior management are having to be deployed from other countries to train and mentor local, highly educated applicants. Total packages for a twelve-month deployment are in the region of £200,000 p.a.

Diversity

Diversity is a major factor that companies wish to address in their security teams. With a dominant male presence, many security departments do not reflect their corporation's broader diversity make-up. Across Europe this is very noticeable, with global corporations undertaking detailed attraction projects to understand how they can address this imbalance, which can have a demonstrable effect on performance.

Risk and Resilience roles are being highly rewarded

At a senior level in 2018 and continuing into 2019, salaries have increased for CSO / Risk and Resilience Directors, whilst opportunities have decreased. For over ten years, security structures costs have been tightly controlled, which has led to Security Directors cultivating and investing in home-grown talent and themselves. At a time when new resilience threats were developing, that training investment has been at the cutting edge of threat management. Overall, if you are a global business your spend has increased, as you have convinced the marketing director that having an operational intelligence gathering capability, scalable across your geographical footprint, could help predict disruptive trends; that the FD would benefit from a new cost control system that helpfully monitored employee travel; that HR and Legal Counsel would meet their obligation of employee due care should they invest in a crisis bridge and employee contact centre.

Messaging to the top

The top quartile of Security Directors have always been game changers and mobilisers, diffident to the approach of "we have always done it like this". They have developed a culture of "develop and exceed". Typically, in the area of cyber incidents there is a need to de-mystify and categorise the nature of the threats, when nearly 30% of CEOs consider their organisations could be attacked in the next twelve months. That affords them great influence and messages to the Board.

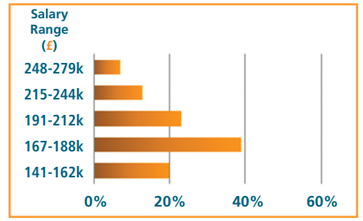
Across the 2019 survey, building up from 2018, roles / people engaging in cyber resilience are experiencing the most significant salary increases. £30–40,000 top-up increase for taking over the leadership and management of cyber incidents, making it a hostile environment for attackers to operate within; entry level analysts, with a coding capability, £35–45,000 starting salary, white hats / hunters £60–70,000 p.a; for managing a team, £90–110,000 p.a; and your salary in today's candidate-driven market may be reviewed every six months.

Arguably, in this changing world where the tech giants of today have replaced Coca-Cola, GE and IBM in the top five most valued brands in the world, politicians are calling for them to be broken up as they are too powerful because they own the access to our data. Yet they have all, at the senior manager level, employed consistently the word 'Trust'. Trust is now considered an important and tangible asset by businesses today – so that has to be a good thing for the risk and resilience professional.

Peter French MBE
SSR Personnel

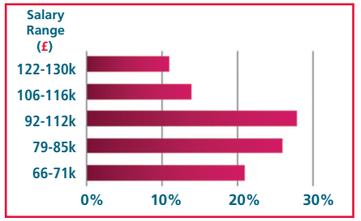
www.ssr-personnel.com

UK SALARY SURVEY 2018 – 2019



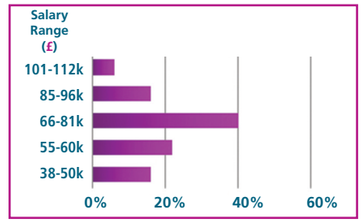
CSO / Global Resilience & Risk Director

The land grab for corporate responsibility should be within the realm of resilience and the threads for business continuity, cyber preparedness and crisis management. Responsible for policy, Executive board briefings. Dotted line or direct responsibilty for Cyber & Resilience should see pay increase €30-60k p.a.



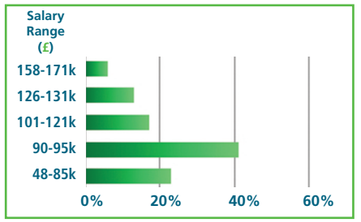
Cyber Resilience Manager / Head of Cyber

A role that is developing across a range of sectors as organisations elevate their response to cyber attacks. The rapid controls of insider users that organisations need to have requires a robust cyber policy against perennial and growth risk.



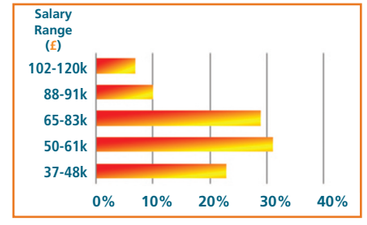
Senior Investigator

Responsibility for more than one country's operations. Active across all security breaches, due diligence, product diversion, counterfeit and auditing functions for the corporation. Provides the forensic function in company.



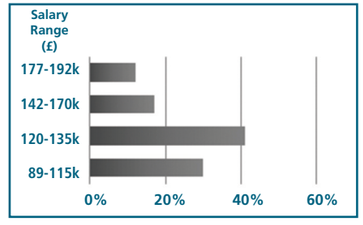
EMEA Security Head

Regional policy development, executive reporting, promulgating corporate policy overview of physical and intellectual protection. Taking responsibility for cyber hunting, risk alert programmes, business continuity and crisis management should have increased basic salary by 20-30%.



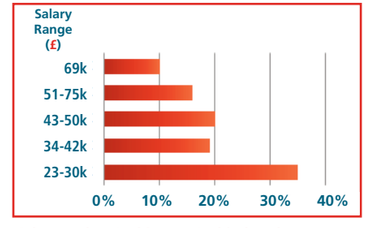
National Security Head

Responsible for all aspects of corporate security and maintaining standards across an estate. Developing an estate programme for internet connected devices and plant that has been overlooked by IT departments. GDPR has been and remains a major part of this role oversight.



Director, Risk & Resilience / Head of Security

Responsible for delivering localised policy and executive board briefings. They are a driver for change and service expansion. Responsibility for cyber hunting, risk alert programmes, business continuity and crisis management should have increased basic salary by 20-30%.



Cyber Analyst / White Hat / Ethical Hacker

As organisations go on the attack against cyber resistant intruders, the skills for this role are stretched across the UK and Europe. Certification will not help; like law enforcement you are seeking technicians who have an exploring nature, 'in harmony with machine code'.

Cost of a Cappuccino across the UK

Anchoring the UK Salary Survey through comparing the cost of a cup of cappuccino provides more indicators as to the regional variance we find in salaries. In these indices we see the cost difference between London and Bradford is £2.78 to £2.38, 15.5% higher.