



outsources

Cyber Security - Market Insights
January 2019

Market Update 2019

- Gartner forecasts that worldwide spending on information security products and services will exceed \$124bn in 2018, up 8.7% from last year, with the biggest area of demand in security services (so good news for the consultancies!) Security as a Service is predicted to make up 50% of security services by 2020.
- Reports now show the global shortage of skilled cyber security workers is at 3 million (up from 1.8 million in our last report), with an ISC2 report showing 63% of companies surveyed claiming a lack of skilled cyber workers directly result in cyber security breaches, which is up from 43% from our last report. However businesses need to train and grow their own talent, as if we only look to hire experienced resources, there is a risk that these numbers won't reduce, as we just move the top tier of talent around.
- 2018 has been a great year for Outsorce, with a suite of products and services launched to complement our full recruitment services. These include IR35 & Compliance Audits, Inclusion & Diversity Consultancy, Bench Resource and Talent Pooling. If you have a workforce challenge that you need a fresh perspective on, we enjoy working in partnership with our customers to help you solve your challenges.
- Our Cyber team held a number of events this year, to attract the highest calibre of candidates, including candidate advancement workshops, the development of our ex-forces network and our extremely popular M1Con event thrown by our Cyber team quarterly which is a free platform for candidates interested in Cyber Security to learn, develop and network. We also co-hosted a Diversity in Cyber event with NCSC (National Cyber Security Centre) as well as co-hosted our M1con events with clients. This is a great way for client's to advertise their brand and find passive talent. If you are interested in attending our meetups, speaking at our events or co-hosting with us, do let us know.



Rosie Anderson
Cyber Security - Manager
randerson@outsorce-uk.co.uk
Tel: 07854 072480



Meet the #CyberSquad



Rosie Anderson Cyber Management, Risk & Resilience

- 15 years recruitment experience
- Focussed on Cyber Security Directors, Heads of Cyber Function, Cyber Risk Managers & CISOs both on a permanent, interim and contract basis
- D&I Lead for Outsource Cyber, hosting our own Diversity events and upskilling programmes for military veterans
- AFCEA Member
- [Spoke at CyberUK](#) in 2018 on the Importance of Diversity within Cyber Teams, and [hosted an event with NCSC](#) promoting Cyber as a career choice
- CERIS Approved

Rebecca Jane SOC, SIEM & Incident Response

- Over 7 years recruitment experience
- Focusses on Senior SOC, SIEM & Incident Response on both a permanent and contract basis
- CERIS Approved



Shirin Fahri Pen Test & App Sec

- Over 5 years recruitment experience
- Focusses on Pen Test & App Sec recruitment
- Created own event [M1Con](#) – an educational platform aimed at helping interested tech candidates break into cyber security
- OWASP member
- On the Board of Buddies for The InfoSec Hoppers – supporting woman and other underrepresented groups attend conferences, get training and make businesses more inclusive
- CERIS Approved

Liam Fahey Network & Cloud Security

- 12 months experience
- Focussed on Cloud & Network Security
- Active within the Cyber Community – Bsides, Manchester Grey Hats, M1Con

Siobhan Gallacher Hardware, ICS & OT Security

- 12 months experience
- Focussed on Hardware Security, ICS and Operational security



In 2018, the consultancies were still hiring in force and this year we have seen over **60%** of our roles from Consultancies – Further analysis shows **40%** from Boutique consultancies, and **30%** from Big4 (with Defence consultancies, MSS and Product Vendors making up the other 30%) However, this has posed us with 2 challenges - In the senior management space we see that the consultancies all want the same thing – commercial experience of consulting with a wide range of clients – which means we move the top tier of talent around. The candidates we are dealing with also what challenging and interesting work – which means the clients need to be offering something different if they're going to pique the interest of gainfully employed candidates. We are seeing a good % of Management candidates that no longer want to work in consultancy, and want to move into the end user space where they can have real ownership for change and strategy.

Cyber Risk & Assurance roles have been the most in demand roles for this year making up **15%** of all vacancies in our Cyber team. This has been a mix of Consultancies, looking to build on new regulatory changes around NIST, FCA and of course GDPR. This has been one of the **biggest contract recruitment** areas, with the banks and retail industries all wanting the best talent, which has meant that contract rates have gone up.

In the **end-user** space, the salaries are varied, dependent on the sector and location of the role. A good FS **CISO** for example, could command a salary of anywhere from £150k - £300k with Defence more moderate around £120-£150k. A CISO job description can be very varied, but they all encompass the need to be able to translate business risk to the tech teams and vice versa, understand the changing legislation in the sector, be able to set and influence strategy and develop the security team to work in hand with the business.

We are getting more requests for **diverse shortlists** from our clients, and the **gender pay gap** has meant that our clients are asking us how to address this balance – whether their challenge is not having any females / BAME in senior management roles, or advice on how to address this balance and create a more inclusive culture. We do have a D&I Programme Lead who can help with this challenge, and due to the events that we do, and networks we are part of, we are confident we have one of the most diverse networks of candidates in the UK.

We do always get asked about the **Cyber Skills shortage** and this always causes debate. There is no shortage of talented individuals that want an opportunity to prove themselves, and get the foot in the door. There are also different profiles, for example; career changers, returning parents and carers, military veterans, neuro diverse people and candidates with different backgrounds that can challenge the status quo and help your organisation to think differently and creatively. The organisations that fill their requirements quickly, and grow rapidly, are the ones that tackle their skills shortage differently, with a blended recruitment model looking for different talent profiles, and ensuring a great inclusive culture, leadership development and mentoring programmes internally. If you need some ideas for different recruitment models, or how to solve your hiring headaches, do reach out to us to see if we can help – We have helped clients with Tech meetups as a passive attraction campaign, military hiring with training blended in via our Bench Resource model, and talent pooling.

In 2019, we are already seeing more requirements for end users with some interesting roles for Defence, Financial Services and Start Ups. I hope this continues, although I know the consultancies we are working with all have aggressive growth targets, as Security as a Service is predicted to make up 50% of the market by 2020. With Brexit still in limbo, and uncertainty over how / when / if we are crashing out of the Euro, this has had an effect on contract demand, but I am confident this will pick up again once there's more stability.



In the **AppSec** space contractors are still commanding £700-750 per day in the UK while salary expectations for permanent staff have gone up to compete with this. Due to a growing workload many businesses have started to look out to wider Europe where salaries are slightly lower – but who knows how this will be effected by the ‘B’ word as lots of banks start to move their operations out of the UK in preparation. Unfortunately we are still expecting AppSec professionals to wear many hats and wondering why we can’t hire someone who wants to be overworked on a budget. There’s still a shortage and huge need for AppSec professionals that can code, design, manage, lead, train and communicate with every other part of the business. All the while there also seems to be a shortage of C-Suite who give them enough buy-in to make the changes they need too. For the most part I still believe that they are some of the most passionate people in Cyber Security because they have the hardest job which is hands on but relies on their influencing powers to try and slow down production to increase security posture. Often a thankless task- no board wants to hear that. Which leads me to **PenTest**...because we know that in the absence of real DevSecOps and the rush to get products to market and save a few pennies in the short term businesses will often outsource this periodically or at a later stage in the product lifecycle.

In the **PenTest** space, businesses are becoming more demanding, talent shortage has driven salaries up and whilst that’s old news, businesses are now becoming particularly fastidious about their hires because they want more bang for buck. PenTest contract rates are very broad from £350-£800 per day depending largely on clearance levels and CHECK status with DV cleared CHECK Team Leaders in London commanding the most. Salaries appear to have peaked last year as I haven’t seen a huge increase, but of course there’s still the occasional diva. I’ve seen an influx of Ethical Hacking **Graduates** this year, but please, if you’re working with students in any capacity, tell them it’s not all about the money! Those that are finding jobs quickest are the ones who are getting out to meetups and OWASP as well as studying in their own time and dabbling with home labs and secure environments to practice their skills. **OSCP** is still the most in demand certification across all levels of seniority – if you’re a student who wants to get into PenTest it’s the best investment in your career you can make.

I’ve also seen a rise in a number of hugely talented Penetration Testers leave consultancy to set up on their own – great growth and success for Digital Interruption for example (a business built by two very talented ex-permie consultants who care about ‘good infosec’). They have recently made a great new hire *and* moved into a new office in Manchester Technology Centre. It looks as though some changes at NCC are slowly starting to have a positive impact on the industry, I’m hearing more good things about work life balance there. As well as this, in my experience, they were the most accommodating consultancy for people with disabilities in 2018 during interview process. I think the impact of people moving into contract and own business is showing and Professionals Services companies are starting to offer better packages in terms of wellness and utilisation whilst more and more internal roles are difficult to fill and forcing businesses to outsource. I think behind this is the increased demand from strong PenTest talent to work on more interesting projects and experience varied environments as a way of keeping their skills current and the job interesting.

For **2019** the Mystic Meg in me thinks that **AppSec salaries in Europe will increase** as demand there does, and we’ll start to see an **increase of women in Senior AppSec roles** globally as they push through the ranks from Development. For PenTest I think we’ll see even **more companies outsource** or a big **increase in contract work** for the businesses who can’t necessarily offer the most exciting work but are still putting security at the top of their agenda this year. I think **Social Engineering skills will be more in demand** as criminals turn to this as a much easier way to extract valuable data from our businesses, so get your security awareness programs in motion if you haven’t already, we’re not just talking about “don’t plug that USB in” anymore, we need to be thinking about phishing campaigns, physical access, analogue data and social media platforms too. I’m still in the clutches of a very busy Q3 and expect that to continue well into Q4, so for the sake of *my own* work life balance, let’s all stop leaving security to the last minute in 2019!



Cloud Security Analysis – Liam Fahey

The trend I'm seeing is that first and second-generation security devices (firewalls essentially) aren't enough to protect against increasingly sophisticated attack methods. They also don't reflect the needs of organizations in the cloud as more and more companies switch from legacy to Cloud platforms. As a result, it seems client organizations large and small are adopting more advanced next-generation firewalls. There seems to be an increase in a need for people with a wider experience of configuration and implementation of different firewalls vendors, particularly next gen firewalls which incorporate IDS/IPS (intrusion detection/ intrusion prevention systems) such as Palo Alto, Forcepoint etc..

With Cloud Security Architects/Professionals, it seems that when managers are looking to hire, they are particularly interested in seeing people who have completed industry specific qualifications such as CCSK, AWS/Azure Certified Architects . Within the consultancy space, candidates who are vendor agnostic and have a broad range of skills within cloud, rather than vendor specific are also very much in demand.

Hardware Security Analysis – Siobhan Gallagher

Within the OT (Operational Technology) Market, I've seen an increased demand for ICS (Industrial Control Systems) candidates with an engineering background due to their broad understanding of ICS from both an engineering and cyber security perspective. Candidates with this varied skillset are beneficial as they can understand the workings of PLCs and SCADA ie. how to upgrade and modify control systems, as well as how to secure these systems, which proves valuable with the need to secure vulnerable legacy PLCs. GICSP and GIAC qualifications are also becoming more popular.

Within the hardware sector, candidates with a combined experience in reverse engineering and manual testing have proven to be in demand. These skills, alongside C & C++ , have proven valuable within hardware vulnerability testing.

SOC & IR Analysis – Rebecca Jane

Christmas 2018 was really busy for me and that seems to be continuing into 2019. 90% of the IR & SOC roles I have worked in the last 2-3 months have been permanent and I have had a number of Incident Response roles which have been to head up or grow a new Incident Response function, meaning instead of learning the hard way it seems more and more organisations want to be in the best possible position to mitigate a risk should one occur.

Over the past couple of months, I have also seen an increase in clients being more flexible towards candidates that are looking to get into Cyber Security, mainly with the SOC opportunities I get, this is a real positive and means as an industry we are recognising that to close the skills gap we need to develop the talent within. A SOC can have a high turnover, this tends to be because the role requires candidates to work 24/7 shift patterns which for some people is only feasible for 12 months or so, clients are becoming more aware of this so are offering opportunities to candidates who have a genuine interest in getting their foot in the door in terms of cyber security. If you have a relevant degree, attend events, listen to podcasts, have your own home network and are working towards/have a relevant certification such as CompTIA Security + it will really set you apart from the competition and shows prospective employers that you are actively immersing yourself in the industry to achieve your career goals.

So what happened within the Cyber hiring community?

Data taken from no. roles logged with Outsourc Jan – Dec 2018

Most sought after roles

In 2018 we received 4 new roles every week, and this analysis is taken from these statistics.

Cyber Management (17%) once again made up the most indemand roles for 2018, however we broke this down into for **Cyber Managers (9%)** and **Head of Cyber** up to **CISO** function (**5%**) and **Cyber Project Management (3%)** This is separate to **Cyber Risk and Assurance** roles, which accounted for **15%** of the roles received. Organisations are looking at their security posture, and seem to be taking cyber seriously, which is no doubt linked to the increased pressure for the board with potential GDPR fines of 4% of turnover.

Pen Test roles still make up almost **12%** of our roles, with **AppSec/DevSecOps** not far behind at 10%

The roles were **28% contract**, with **72% permanent**, but this is likely due to the make up of **60% consultancy** clients we work with, which is why we are focussing on more end user clients.

Consultancy	60%
Financial Services	14%
MOD / Public Sector	8%
Telecoms	7%
Engineering / Automotive	5%

Most in demand roles

Cyber Management	
* Further breakdown below	17%
Cyber Risk & Assurance	15%
Pen Test	12%
AppSec / DevSecOps	10%
SIEM & SOC	9%
Security Manager – Function	9%
Security Architecture	7%
Hardware / ICS	5%
CISO / Head of / Director	5%
Incident Response	5%
Network Security / Cloud Security	4%
IDAM	4%
Pre-Sales	4%
Endpoint / DLP	3%
Cyber Project Management	3%
Threat Intel	3%
Audit / PCI / ISO	2%

outsource Salary & Rate Survey – UK Averages

Job Title	Median Perm Salary		Contract Day Rate (Excl. agency fees)	
Identity & Access Management Consultant	£62,500 per annum	↓	£563 per day	↑
Cyber Ark Consultant	£70,000 per annum	↓	£625 per day	↑
SOC Analyst	£45,000 per annum	↔	£425 per day	↓
SOC Manager	£70,000 per annum	↔	£550 per day	↓
Penetration Tester	£68,750 per annum	↑	£500 per day	↑
Check Team Leader	£73,750 per annum	↓	£500 per day	↓
Vulnerability Analysts	£65,000 per annum	↑	£419 per day	↓
Threat Hunter	£70,000 per annum	↔	£538 per day	↓
Incident Response Consultant	£60,000 per annum	↓	£500 per day	↓
Security Engineers	£55,000 per annum	↔	£475 per day	↔
Network Security Consultant	£66,000 per annum	↔	£500 per day	↔
Cyber Security Manager	£72,500 per annum	↔	£525 per day	↔
Cyber Security Risk Manager	£70,000 per annum	↔	£600 per day	↑
Cyber Security Director / CISO	£120,000 - £180,000 +	↑	£1000 per day +	↑
CCP Information Assurance Consultant	£65,000 per annum	↓	£525 per day	↓
Cyber Security Architect	£87,500 per annum	↑	£550 per day	↓
Splunk Consultant	£70,000 per annum	↓	£550 per day	↓
Security & Risk Analyst	£60,000 per annum	↑	£450 per day	↓
Compliance / Data Privacy Consultant	£62,138 per annum	↔	£448 per day	↓
ICS / SCADA Security	£80,000 per annum	↔	£700 per day	↓
Application Security *new data	£75,000 per annum		£550 per day	
Hardware Security *new data	£70,000 per annum		£400 per day	
Cyber PM *new data	£63,750 per annum		£525 per day	

2019
dates for
your diary



AFCEA London Meetings
1st Thursday of every month

BSides Leeds
25th January

**M1Con, Manchester
Recruitment Workshops**
7th March 2019

CyberUK, Glasgow
24-25th April 2019

**M1Con, Manchester
Incident Response Talks**
May 2019

Steelcon, Sheffield
12th July 2019

2018 Summary

Diversity



Diversity continues to be a key focus for our customers. In May we partnered with Nationwide Building Society, and in November [we partnered with NCSC](#) to discuss 'Inclusion in the Workplace' with senior leaders from all industries championing diverse topics.

GDPR



We rolled out our own internal GDPR compliance schedule well ahead of the May deadline. We now have a super cleansed database, and are confident this gives us the most up to date relevant network of cyber candidates.

M1CON



We hosted our first M1CON events in Manchester in March & June and September in Leamington Spa. With a CTF and talks on everything from Hardware Security to Android Hacking, each event had over 30 attendees which was great!

Military Hiring Campaign



We have had our first successful military hiring campaign, via our Outsource Bench Consultant model. The candidate gets a great opportunity, commercial experience, paid a fair salary and ongoing training and the client gets a skilled resource with bespoke training tailored to them, and a free hire after 12 months.

Placements



Over 50% of our placements have been female candidates or BAME candidates, with 14% being ex- military veterans

2019 – what's to come?

Diversity

We plan to host an M1Con event in March which looks at attracting different talent into Cyber, to promote diversity of thought. If Diversity is on your agenda, and you want help [attracting a more diverse workforce](#), ask to speak with our Diversity Manager

Audit offerings

Outsource love compliance! We now [offer IR35 audit services](#) as a standalone service, along with compliant onboarding processes. To find out more, ask to speak with our Compliance Team

M1CON

We are planning two events – one in March with more 121 workshops focussed around cv and interview techniques, with advice on diverse hiring practises, and one in May focussed around Incident Response. If you are interested in speaking, attending or co-hosting an event do get in touch.

Military Hiring Campaign

We want to continue to roll out our [bench resource](#) campaign across other customers – both for ex military hires, and for junior cyber (and non-cyber)staff with ongoing support and training via Outsource. To hear more, ask to speak to our Bench Resource team

Placements

We are working hard to promote cyber careers to diverse groups, and actively work to have the best network of diverse candidates, including females.



How can we help you achieve your goals?

Rosie Anderson
Cyber Manager

Outsource UK
RAnderson@outsource-uk.co.uk
07854 072480

outsource

Birmingham · London · Manchester · Stoke-on-Trent · Swindon