CYBERSECURITY
BUILDING BUSINESS RESILIENCE

A Robert Walters Group Company

VACANCYSOFT
Data Publishers for the Recruitment Industry

ROBERT WALTERS

INTRODUCTION

While a challenging economic climate has compelled firms to rationalise areas of their business, the data-centricity of operations has cemented the importance of an infallible cybersecurity strategy in a new era of work.

Against the backdrop of remote working and the rise of Covid-19 related IT security attacks, those investing in their cybersecurity function are proving to be the organisations that can ensure business continuity and take a proactive stance against emerging threats.

As cybersecurity takes centre stage in technology recruitment, Robert Walters and VacancySoft have partnered together to analyse the UK cybersecurity hiring market, exploring the key trends that have maintained job growth throughout 2020, and the key skills areas where we'll see demand thrive as the decade progresses.

CONTENTS

KEY STATISTICS

COST TO BUSINESS

£2.48m
average cost per instance to UK companies for data breaches

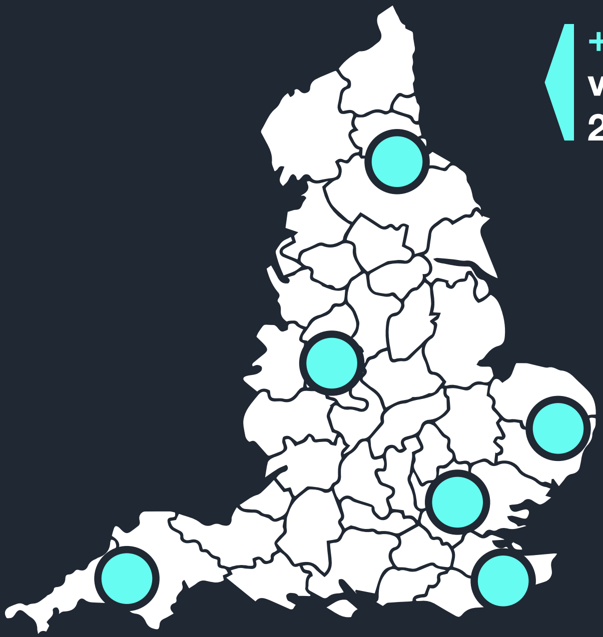
65,000
attempted cyber-attacks on UK SME's every day

48%
UK companies who do not have adequate cyber security for staff remote working

44%
would stop using a company online if they are breached during a cyber attack

£68bn
spent on cyber security in UK, representing 5.6% of overall IT budgets

CYBER SECURITY VACANCIES BY REGION



+5.5% – cybersecurity vacancy growth in H1 2020

London	**40.8%**
Yorkshire & North East	**18%**
South East	**16%**
South West	**8.3%**
North West	**4.6%**
East of England	**3.8%**

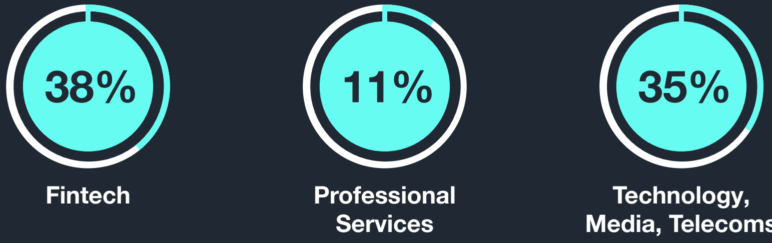
Fastest Growing Regions:

Yorkshire & North East	**+138%**
South West	**+85.7%**

TOP INDUSTRIES HIRING CYBERSECURITY PROFESSIONALS

1. Technology
2. Financial Services
3. Consumer Goods & Services

CYBERSECURITY HIRING: THREE YEAR GROWTH



KEY DRIVERS OF CYBERSECURITY IN 2020

1 Ransomware

2 Phishing

3 Artificial Intelligence (AI)

TALENT SHORTAGE

140,000
Talent shortage of cybersecurity professionals across Europe

70%
of companies in Europe do not have a sufficient cyber security team

1,000
firms in the UK providing cybersecurity services

10
average headcount of a UK-based cybersecurity firm

1/3
Employers state that cybersecurity professionals will be in demand post-Covid

940%
YOY increase in investment into UK cyber start-ups

OVERVIEW: CYBER AT A GLANCE

The business case for cybersecurity investment

Data breaches cost UK businesses an average of £2.48 million per instance, where increasingly businesses of all sizes are being targeted. Further research has found that there are 65,000 daily attempts to hack small-to medium-sized businesses in the UK - of which around 4,500 attempts are successful.

The reputational risk of being subjected to a cyber hack has been quantified, where in the UK 44% of people would stop using a company online if they were found to be breached during a cyber-attack.

With that in mind, combined with the regulatory burden caused by GDPR, and the pressures of Covid-19, one trend we expect to manifest more regularly is Cyber Audits being provided by specialist external providers, as a way of helping companies test their resilience and restore public confidence.

Demand for talent and skills shortages

According to the Robert Walters, cybersecurity was highlighted as one of the key growth areas for 2020. In fact, a third of employers stated that cybersecurity professionals will be in demand in their organisation in a post-Covid world, while 25% of businesses also highlighted the need for Cloud Computing skills to further develop their information security architecture.

However, while nearly half (48%) of businesses reveal that they need to improve their cybersecurity model, a recent study by ISC revealed that only 28% of companies have sufficient cybersecurity staffing and across Europe, this is exasperated further by the acute talent shortage of around 140,000.

Similarly, Robert Walters skills shortage research identified that cybersecurity was the most sought after skill (58%) for technology hiring managers, however only 10% of the technology candidate pool possessed the right level of cybersecurity skills and know-how.

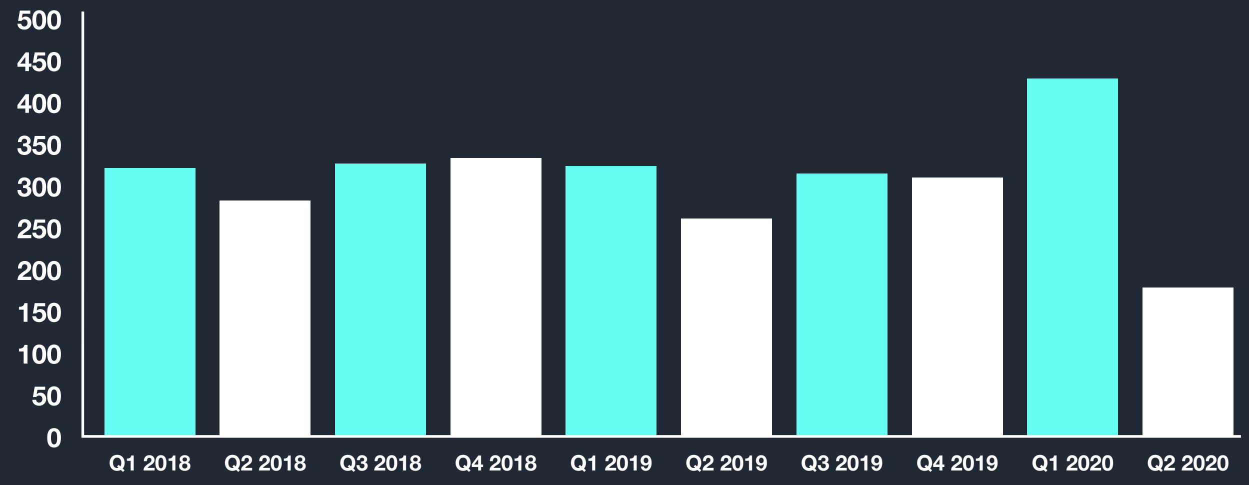
Impact on vacancies

Vacancies for Cyber Security professionals in 2020 are holding steady, despite the Covid-19 crisis which has impacted hiring across the board. Despite vacancies for IT professionals being down by -40% so far this year, cybersecurity volumes have increased by +5.5% in H1 2020 in comparison to the same period last year.

January 2020 in particular witnessed a surge in recruitment of cybersecurity professionals, where the total number of vacancies was over double the 2019 monthly average, at +38%.

Cybersecurity is becoming an ever greater part of the technology function as a result. Whereas in 2018 it accounted for 3.5% of technology vacancies, so far this year it is above 5%, where this growth is forecast to continue.

NUMBER OF UK CYBERSECURITY VACANCIES



Growth outlook

The outlook for cybersecurity professionals will stay positive. In the UK, organisations are collectively spending £68bn on cybersecurity, accounting for just 5.6% of an organisation's total IT budget.

This spend is far outweighed by the cost of data breaches, cementing the business case for increasing investment in the function.

IMPACT OF COVID-19 ON CYBERSECURITY

Remote working

The Covid-19 crisis has caused another layer of challenges for business. To start with, within the UK specifically, a recent survey of medium to large businesses found that 48% did not have adequate cybersecurity provision for home working.

With businesses having to test the waters with widespread remote working for the first time, security vulnerabilities have been exposed as employees move from a secure office Cloud environment to public Clouds - with threat actors using the opportunity for phishing and ransomware attacks.

Employers that have not already invested in remote working technology leave their data further under threat as employees continue to work on personal devices that do not comply with organisational IT security standards.

48%

of business decision makers have admitted that their existing cyber security policies are currently not suitable for maintaining a 100% remote working model.

Covid-19 related attacks

As the daily reality of the Covid-19 crisis has taken precedence, employees have become susceptible to cybersecurity threats in the form of fake Covid-19 related news such as track and trace technology, hand sanitiser, and fake crowd-funding pages, to name a few examples.

At a time when phishing attacks are at an all time high; financial services institutions, technology companies, and online payment platforms are having to adapt to compensate as they seek to protect both their reputation, as well as their data.

While Artificial Intelligence (AI) has a key part to play in shielding businesses from certain threats, it is not a panacea. Investment in people is becoming central to implement and sustain a proactive cybersecurity strategy.

How are organisations responding?

The vulnerabilities exposed by Covid-19, combined with the regulatory burden caused by GDPR have led to increasing numbers of cybersecurity consulting firms emerging. For context, in the UK it is estimated there are now over 1,000 consulting firms providing cybersecurity services, where over 90% have under 10 employees.

With this, a trend we expect to manifest is an increase in ‘Cyber Audits’ performed by specialist external providers, as a way of helping companies test their resilience and identify vulnerabilities.

“Businesses have been forced to make major changes to their cybersecurity programs and protocols in order to manage the transition to remote working, leading to a spike in recruitment activity in the InfoSec space. This trend shows no signs of slowing down as organisations respond to cybersecurity threats post-pandemic.”

Darius Goodarzi, Principal - Information Security and IT Risk, Robert Walters

SKILLS HOTSPOTS AND SALARY TRENDS

Roles in demand

Security Operations Centre (SOC) – As businesses take more steps to strengthen their cybersecurity strategies, a SOC takes both a preventative as well as reactive approach, detecting potential threats, and implementing measures to prevent them from happening. London salaries have spiked by up to 10.5% in large enterprises (with a headcount exceeding 250).

Security Engineer – The government has invested £10m in cybersecurity solutions over the past year, with a pressing need for security engineers to implement new security products and install updates that enhance security around current IT platforms.

Security Awareness Manager – with businesses becoming more data driven and staff gaining increasing exposure to commercially sensitive information, security awareness training is required to educate employees and provide data protection guidance to ensure compliance.

CISO - There's more technology in the workplace than there has ever been before, growing an organisation's attackable surface. With this comes a realisation the executive level that security is a key component in business continuity and operational performance - requiring an advocate to work alongside the C-suite to ensure compliance with security procedures.

Cybersecurity salaries in UK tech hubs

London

	Permanent Salary Per Annum GBP (£)						Contract Rate Per Day (PAYE) GBP (£)		
	Medium Enterprise (HC 50 - 250)			Large Enterprise (HC 250+)					
Role	Range	Average	YOY Change	Range	Average	YOY Change	Range	Average	YOY Change
Information Security Manager	72 – 110k	102,350	4.71%	73 – 124k	115,958	0.83%	690 - 935	687	2.93%
Information Security Analyst	42 – 75k	65,057	2.86%	54 – 91k	80,860	0.45%	425 – 740	652	1.25%
Security Operations Consultant (SOC)	51 – 71k	59,417	3.88%	60 - 100k	85,429	0.39%	545 - 680	598	4.00%
CISO	115 - 142k	125,733	4.13%	131 - 200k	177,161	0.25%	1,060 - 1,725	1,208	5.00%
Security Engineer	50 - 75k	59,715	3.85%	74 - 100k	86,524	0.32%	545 - 805	660	0.70%

Manchester

	Permanent Salary Per Annum GBP (£)						Contract Rate Per Day (PAYE) GBP (£)		
	Medium Enterprise (HC 50 - 250)			Large Enterprise (HC 250+)					
Role	Range	Average	YOY Change	Range	Average	YOY Change	Range	Average	YOY Change
Information Security Manager	50 - 80k	53,322	2.10%	60 - 85k	64,550	7.58%	450 - 600	533	0.00%
Information Security Analyst	38 - 60k	45,848	5.41%	38 - 65k	45,125	2.27%	375 - 475	445	0.00%
Security Operations Consultant (SOC)	45 - 85k	61,300	6.61%	45 - 95k	83,500	7.74%	500 - 700	615	4.29%
CISO	80 - 115k	103,827	5.40%	85 - 150k	132,500	8.33%	600 - 750	688	2.94%
Security Engineer	55 - 85k	60,400	3.53%	55 - 95k	65,214	10.40%	375 - 500	465	2.00%

Birmingham

	Permanent Salary Per Annum GBP (£)						Contract Rate Per Day (PAYE) GBP (£)		
	Medium Enterprise (HC 50 - 250)			Large Enterprise (HC 250+)					
Role	Range	Average	YOY Change	Range	Average	YOY Change	Range	Average	YOY Change
Information Security Manager	45 - 64k	54,428	4.18%	55 - 72k	64,557	0.94%	500 - 750	625	0.00%
Information Security Analyst	35 - 50k	42,392	4.86%	43 - 56k	49,923	5.34%	358 - 550	480	1.05%
Security Operations Consultant (SOC)	42 - 53k	46,400	7.05%	45 - 75k	56,100	3.08%	450 - 600	525	0.00%
CISO	90 - 120k	105,448	5.00%	100k+	-	0.00%	750 - 1,000	875	0.00%
Security Engineer	33 - 47.5k	40,375	5.38%	48 - 60k	54,167	8.33%	338 - 550	444	0.91%

Before the UK was battling with an epidemic, recruitment for cybersecurity professionals hit an all-time high in January 2020 - with vacancy levels +112% higher than the previous year.

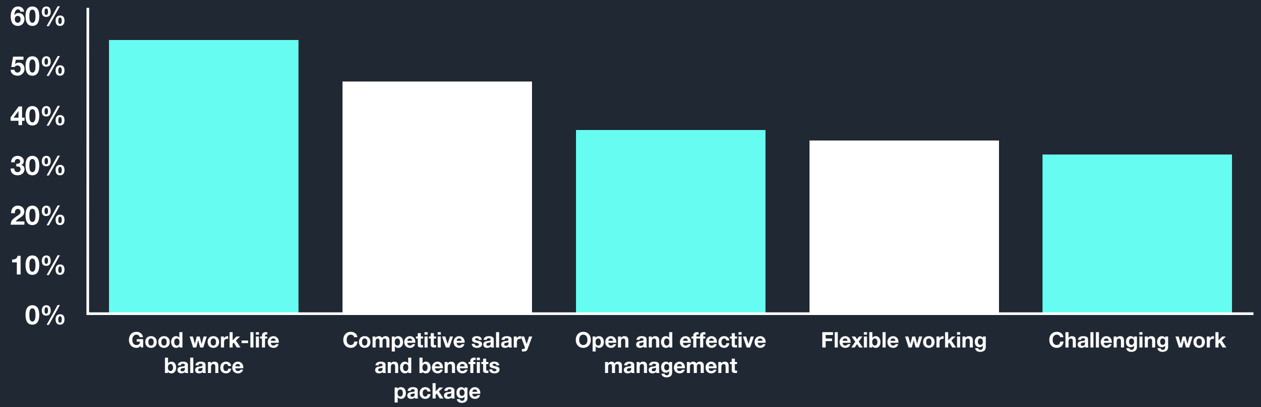
New data protection rules and the rising threat of cybercrime heightened the demand for cybersecurity professionals, as an alarming increase in costly data breaches resulted in heavy fines imposed by regulators.

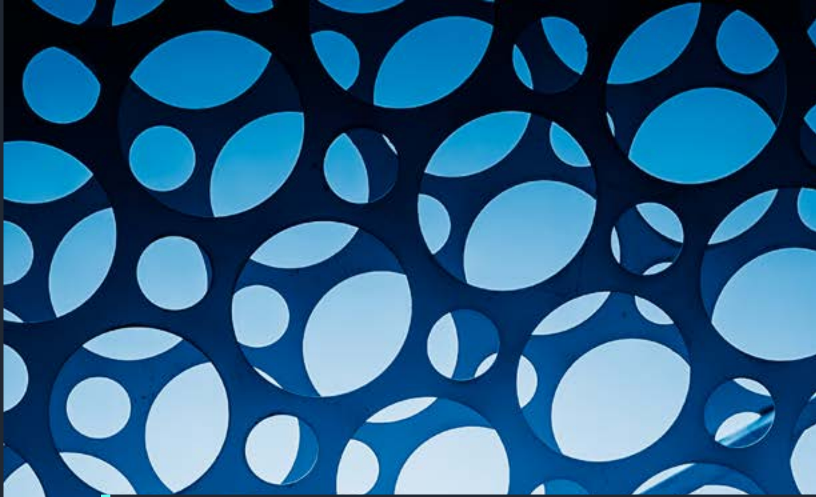
A global pandemic has only served to bring about new challenges for cybersecurity departments – so whilst technology recruitment has understandably dropped due to hiring freezes, cybersecurity recruitment has held firm - with salaries expected to remain stable over the next 12 months, putting further strain on the skills shortage.

Year-on-year growth is expected to plateau after salary hikes of up 10% seen in both the capital and the regions since 2019.

More than half (55%) of cybersecurity professionals value job offers that provide a healthy work life balance, compared to 48% that place importance on competitive compensation and benefits package. Over a third (35%) of the talent pool see flexible working options as part of a competitive offer. One thing is for certain, firms who want to make a top hire need to find the balance between competitive compensation and soft benefits.

TOP 5 EXPECTATIONS FROM CYBERSECURITY PROFESSIONALS





> "While diminishing hiring budgets will restrict salary growth across the next 12 months, businesses will need to topple the employment offer of competitors through other means. Flexible working arrangements are becoming more important to cybersecurity professionals to improve work-life balance."
>
> **Tom Chambers - Senior Manager Technology, Robert Walters**

Cybersecurity skills hotspots

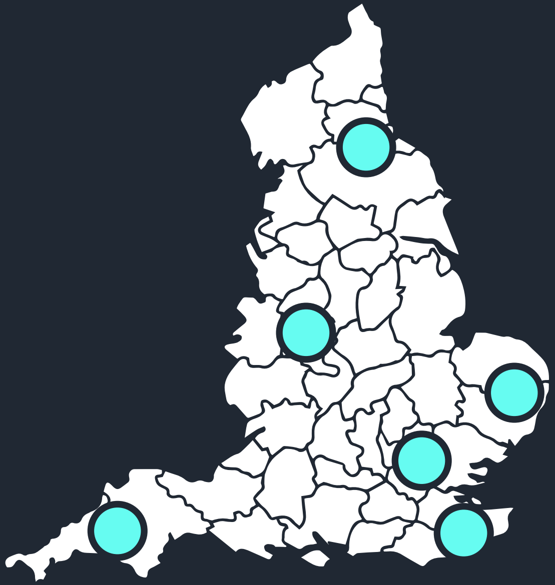
Cybersecurity hotspot	Average YOY growth	% of technology talent pool
AWS	62%	3%
Cloud Computing	11%	8%
Ethical Hacking	30%	>1%
Security Information and Event Management (SIEM)	50%	>1%

When focusing on the key skills in demand from the cybersecurity workforce, it is clear that there are evident gaps in the technology talent pool.

- Demand for AWS skills has skyrocketed by +62%, yet makes up for just 3% of the technology talent pool
- While SIEM (50%) and ethical hacking (30%) are emerging skills required to implement a robust cybersecurity strategy, less than 1% of UK technology professionals possess these skills

> “As businesses continue to invest in cybersecurity software and adopt new platforms, there will be a heavy emphasis on Cloud skills, security engineering and site reliability engineering. Professionals involved in security orchestration with strong SIEM skills such as Splunk will be highly valuable, as well as AWS container security and micro service security architecture. Businesses will have to make heady attempts to secure cybersecurity specialists, where possible tapping into passive candidate markets to secure the best talent.”
>
> **Ajay Hayre - Senior Consultant Technology, Robert Walters**

VACANCY GROWTH BY REGION



As the need for cybersecurity professionals is becoming more prevalent, roles are emerging more evenly across the country. While traditionally London had been the centre for hiring, the regions are catching up with the capital. We can see this in the shift from 2018 to the current market where we're seeing the following trends:

London

In 2018, 50.6% of all Cyber Security vacancies were in London, where in contrast so far this year, this has dropped to 40.8%.

Yorkshire & North East

The rising prominence of tech hubs outside of London – in particular in the northern regions – has had a significant impact on hiring patterns, with Yorkshire and the North East becoming the second largest region for cybersecurity talent. In fact, year-on-year volumes for cyber security vacancies has increased by an explosive +138%. The region now makes up 18% of overall cyber security hires.

North West

The North West – a prominent tech hub – has had a mild contraction in cybersecurity hires, though not as significant as other regions – down 6.4% year-on-year. Where the North West continues to play to its strengths on creative and start-up culture - focusing tech hires on UI & UX Design, Product Owners, Software Engineers, and Machine Learning experts – its neighbouring cousin Yorkshire & North East are focusing on providing the other end of the complete tech offering.

South East

The next most prominent region is the South East, representing 16% of cybersecurity hires in the UK. However, much like London activity has been down year-on-year by 12.4% as businesses adopt nearshoring tactics and hire in northern regions. Where 19% of cybersecurity hires was in the South East in 2019, this has dropped to 16% this year already. This has meant that the share of cybersecurity vacancies has dropped from 5.1 to 4.6%.

+5.5% – cyber security vacancy growth in H1 2020

"The north has been rising for some years now in regards to tech hubs – from a year-on-year increase in VC funding, less barriers to entry for start-ups, relocation of headquarters, and some of the best tech courses in the UK. It is quite clear to see that Yorkshire and the North East is making quite an aggressive play to dominate the cybersecurity field, and increasingly we are seeing more consultancy firms base themselves in the region as a result of low cost base and quality talent pool"

James Perry, Associate Director of Technology at Robert Walters

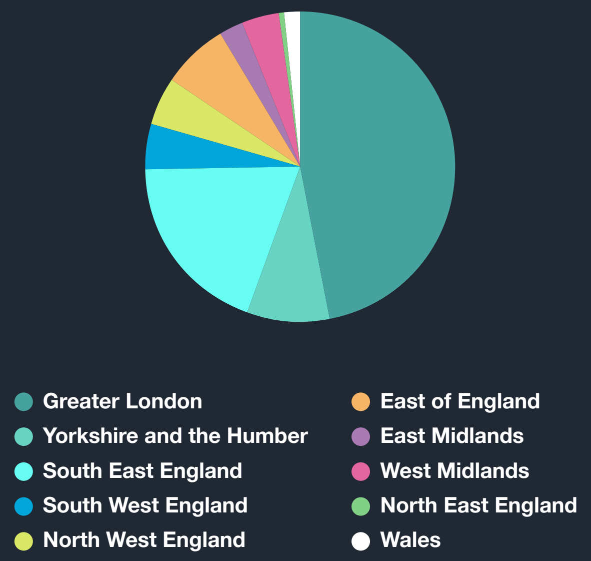
South West

Another notable region worth mentioning is the South West, where job vacancies in cybersecurity have increased by 85,6% - not least because of its active retail and e-commerce industry. This has meant that the share of vacancies has increased from 4.6% to 8.3%.

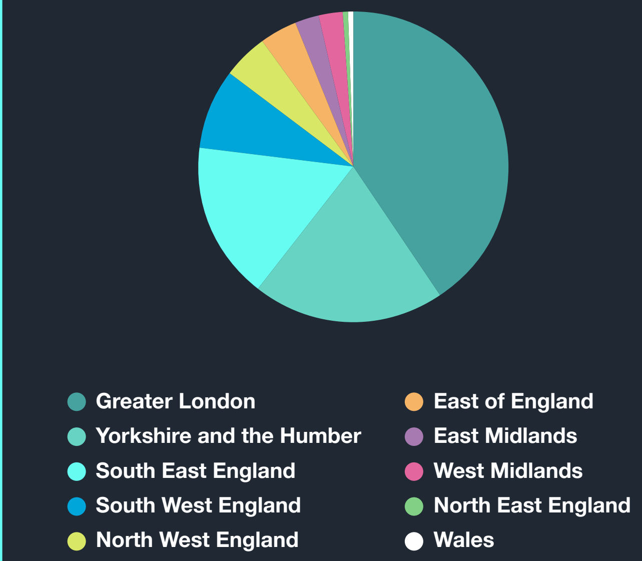
East Of England

The biggest decline in vacancies within the country was in the East of England, with a collapse of 41.1% This has meant the share of cyber vacancies in the region has dropped from 6.7% to 3.8%. With a dominant manufacturing industry, companies in the region expanded hires and investment in critical areas around logistics, supply chain and health & safety in light of Covid. As new infrastructure and channels continue to be built within manufacturing, investment will also need to go into cyber security which we will likely see come to fruition at the latter end of 2020.

CYBERSECURITY VACANCIES BY REGION 2019

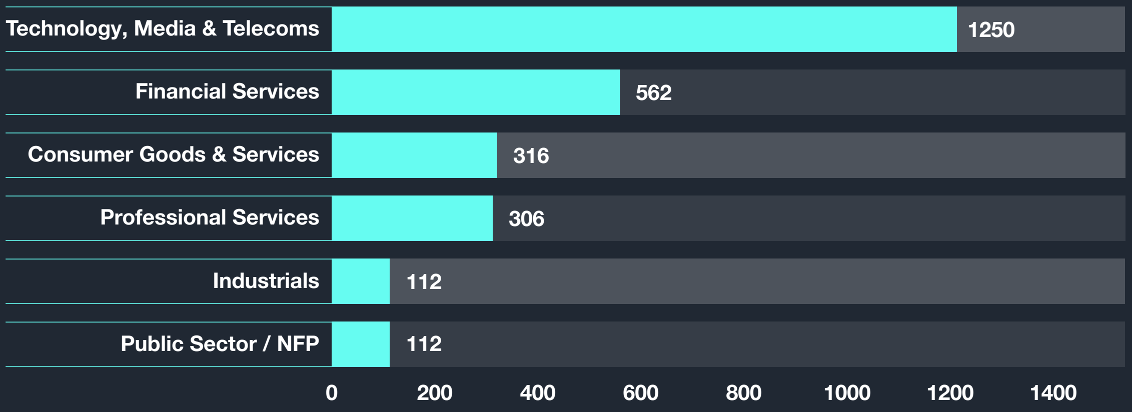


CYBERSECURITY VACANCIES BY REGION 2020*



INDUSTRY BREAKDOWN

CYBER SECURITY VACANCIES BY INDUSTRY 2020*



Technology, Media & Telecoms

Analysing activity by industry, Technology, Media & Telecoms (TMT) dominates, where overall they now account for 44% of all recruitment in cybersecurity, up from 35% in 2018.

However this growth has mainly been within Technology companies specifically. Within Telecoms we see that there has been a drop in activity of over 55% since 2018, while within Media volumes are down 40%.

In contrast, there has been a surge in recruitment in Technology, with cyber security vacancies up by 33%,

Fintech, Banking and Financial Services

Fintech has been the star area within the technology space, with vacancies up by 37% since 2018. Interestingly, as activity has picked up within Fintech, it has dropped within Financial Services, where since 2018, volumes are down by 23.5% for cybersecurity professionals.

The increase of cybersecurity hires within fintechs has been driven by fast growing & scaling fintechs who have acquired banking licenses and therefore have an urgent need to protect data in transit or in the cloud. Cyber security hires are also being driven by the demand for 'open banking' which involves data being shared between different institutions, coupled with an increase indemand for online payment platforms due to Covid-19.

While facilitating secure open banking and automated fraud and threat detection remains a priority for traditional banking and financial services organisations, it's quite possible that more mature financial institutions had sufficient talent onboard to stay resilient against Covid-19 related cyber threats, warranting a freeze in hiring.

Consumer Goods and Services

Recruitment within Consumer Goods & Services is also continuing on an upward trend, where in 2020 so far vacancies are up 17% compared to last year. As businesses in the sector shift towards developing secure e-commerce platforms and card-less transactions, accelerated by Covid-19, it's predicted that this could see a record recruitment year for cybersecurity professionals across Retail & E-Commerce.

The rise of the Cyber start-up

Given cyber roles are concentrating within Technology, investment activity in the cybersecurity space suggests expertise will increasingly become concentrated within the specialist cybersecurity sub-sector.

Since the start of lockdown investment into cyber start-ups in the UK has increased by a staggering 940% compared to the same quarter in 2019. The total investment secured by the UK's top 10 cyber start-ups equates to almost £1.2bn – suggesting specialist cybersecurity offerings will be sourced en masse as technology teams seek to address underlying cybersecurity concerns and implement cyber products as the UK phases out of the Covid-19 pandemic.

The top 10 funded cybersecurity startups in the UK (Beauhurst)

		Total funding to date (£)
1	OneTrust	322m
2	Snyk	200m
3	Darktrace	173m
4	Privitar	120m
5	Onecom Group	100m
6	Featurespace	85.3m
7	Digital Shadows	53m
8	Tessian	44.4m
9	Garrison Technology	39.2m
10	Glasswall Solutions	38.8m

I3SECURE LIMITED: INDUSTRY INSIGHT

i3Secure is a UK-based cybersecurity and data protection consultancy, focused on providing services and solutions to enable their client's strategies. They have deep industry expertise and extensive experience, from supporting start-ups, to leading global enterprise security programmes, helping businesses make intelligent investments in security to unlock opportunities. i3Secure knows that security, data protection and compliance challenges are different for every organisation in every industry. Utilising a proven and pragmatic approach, they help embed tailored solutions which provide assurance for businesses.

Nathan Tittensor, Director, and Adam Casey, Managing Director at i3Secure Ltd, spoke to Robert Walters around the drivers for growth in the cybersecurity sector.

> "As a result, one of the main drives for cyber security over the next 12 months will be to amend and create sustainable and secure systems."

1. What has been the key drivers for the security market in the last 2-3 years?

More people have been aware of privacy and security than they ever have been, and for the last few years GDPR has been a big driver in that.

GDPR law requires personal data to be processed securely using appropriate technical and organisational measures. Up until this point, the base line for personal data processing was relatively fluid.

With the regulation not mandating a specific set of cyber security measures, the biggest task here has been 'how is it going to look and be enforced.' The message here was for firms to take 'appropriate' action, but with the rise of cybercrime, phishing, and ransomware, businesses were being called out for the lack of protection of customers data. In some large cases of security failure such as Easy Jet, brand damage was caused.

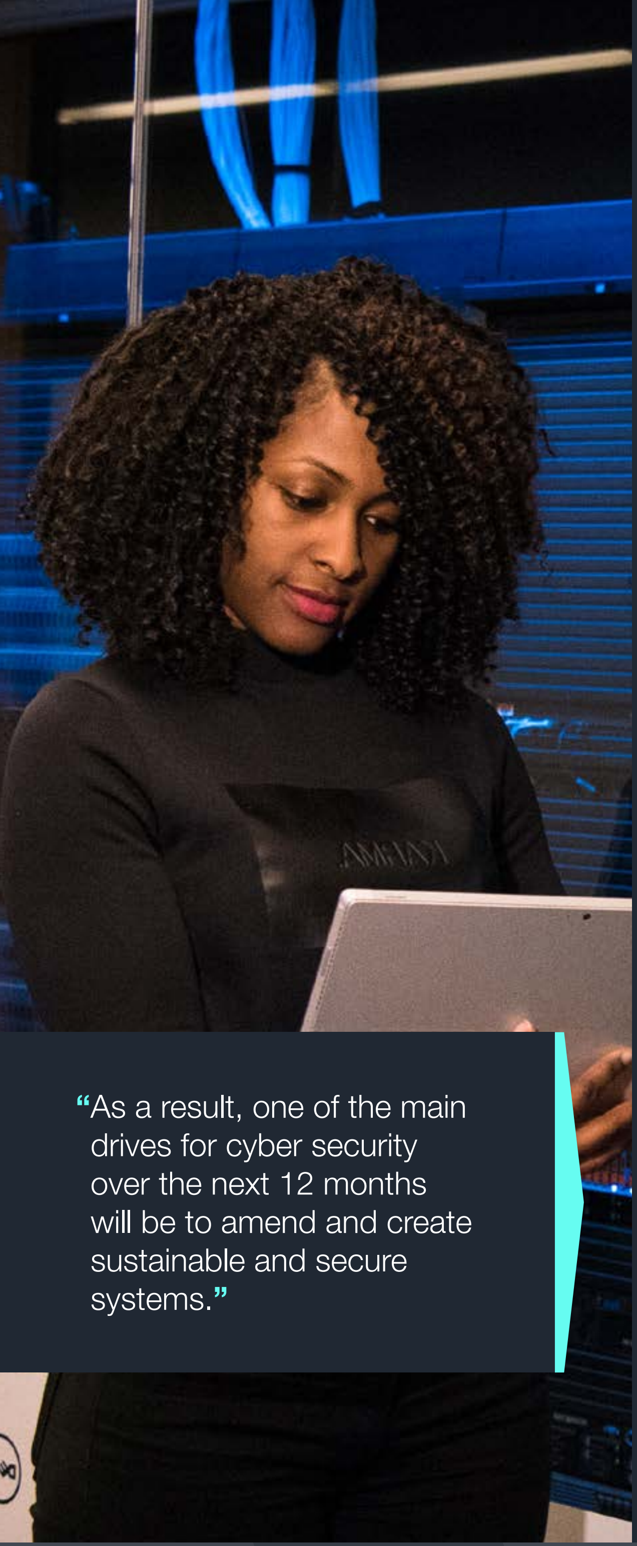
This, along with the GDPR has been a real catalyst for cyber security in the past few years. Increasingly, customers expect to see a level of transparency about how their data is being used and protected.

2. What will be the key drivers in the next 12 months?

Security is increasingly been seen as a 'differentiator' for companies and brands, and almost acts as a marketing tactic to build brand trust. For example, Apple has recently built a name for itself not because of its operating system – where arguably Anroid are stronger – but because of the strength in its security. Apple are known worldwide for their stellar end-to-end encrypted software and products and have not been shy to show their commitment to security even when under the media or political landscape.

Just like the trend for businesses to focus on ethical practices and CSR as a USP and brand culture, so will the commitment a company has to cybersecurity.

The pandemic forced companies to undertake a digital transformation overnight, and not surprisingly COVID-19 will remain the dominate issue for all businesses for the next 12 months (at least). What we will likely see at the back end of this year is a period of 'rationalisation' – where firms will need to check whether what they fitted 'overnight' is totally secure and fit-for-purpose. As a result, one of the main drives for cyber security over the next 12 months will be to amend and create sustainable and secure systems.



“As a result, one of the main drives for cyber security over the next 12 months will be to amend and create sustainable and secure systems.”

3. Which industries are a model of best practice for security?

The gold standard for cyber security practices will certainly have to be the financial services sector as a whole, who are encouraged to give due focus to cyber security practices as a result of and large by the level of regulation laid on in the sector.

The tech boom within the sector has also led to the industry setting the gold standard for the adoption of security techniques, such as encryption. As competition grows on the tech side of things, banks and fintech’s will continue to ramp up their security practices in order to attract and retain customers.

4. Which industries have a lot of work to do, and it what areas?

The e-commerce industry are relatively new to the cyber security space, and as a result there is a lot of work that still needs to be done in this area. The pace at which e-commerce grew during COVID-19 in particular raises questions as to whether their cyber security has been up to par with the sharp increase in traffic to online sites. Given that the move to e-commerce looks to be a long-term change, businesses must really consider a holistic approach to cyber security rather than a short-term fix.

The next industry which we suspect will be looking at their security posture is the legal sector – in particular law firms. Whilst the legal sector deals with high volumes of confidential information, they have never been mandated to have certifications around security. Although, we are starting to see firms achieve certifications such as ISO 27001 to demonstrate they have robust practices and enhance customer trust.

It is remote working that has really shone a spotlight on this, and the sector should act fast before it is faced with the consequences of personal information being mishandled when not on-site in offices.

Interestingly, we’d also highlight software companies in this ilk. Gone are the days where you develop a software product and sell it. Now software products are expected to be flexible and meet individual requirements, all whilst meeting the criteria of things such as the GDPR. For businesses that do this well, it can become a competitive advantage.

5. Which industries do you anticipate to be hiring rapidly in this area?

The public sector will be one of the biggest recruiters for cyber security professionals in the next 12 months. Already we can see from the Cyber Security Sectoral Analysis 2020 report published by the Dept for Digital, Culture, Media & Sport, the acknowledgement from government that this is an area that should be worked on.

Security Consultancies will also be hiring at pace, for the large part due to the scale at which organisations will be outsourcing projects. With 80% of organisations having gone through or still undertaking a digital transformation programme, cyber security projects around resilience and Cloud security will be prevalent.

6. Has Covid-19 been an opportunity to change security thinking?

COVID-19 has 100% changed security thinking, partly because the ‘hand was forced’ and remote working highlighted to many businesses how vulnerable or susceptible they actually are. Businesses soon learnt that had they thought about this previously, they wouldn’t need to go through a clunky retrofit process now.

Previously in-house IT was seen as the ‘Department of No’ where challenges around timescale and budget would often be the biggest barriers. Fast-forward to COVID-19 and all of these barriers were eradicated and IT is now viewed as the department that can enable business objectives.

Whilst business continuity and resilience is not technically a security problem it has typically fallen into the remit nonetheless, which meant that during COVID-19 IT & security were back at the heart of things. Where previously it was an ongoing case of rationalising spend on security – making up just 10% of the total IT budget – it is now being considered as a crucial part of the business plan.

> “Where previously it was a case of rationalising spend on security, it is now being considered as a crucial part of the business plan.”

7. What specialisms or skillsets within IT security will be in particular demand?

It will all boil down into two main skillsets – technical skills, and communication skills.

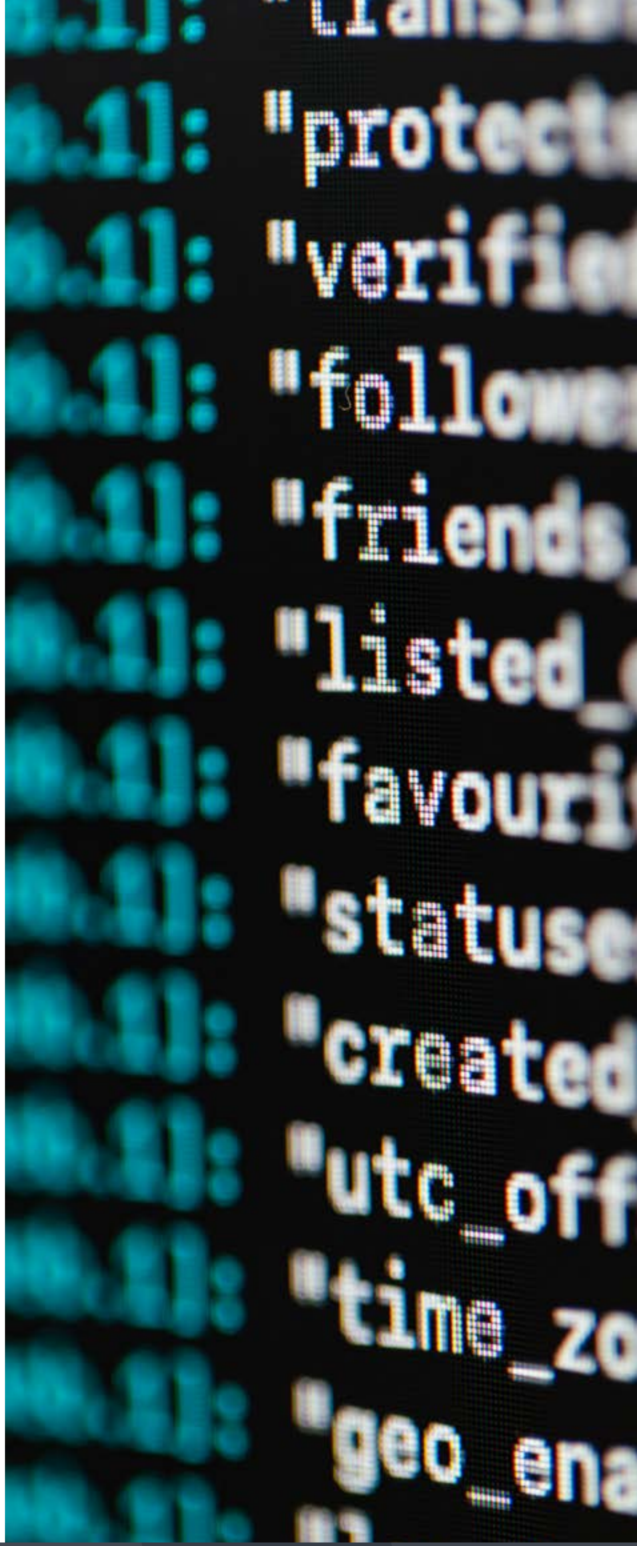
On the technical side of cyber security the industry was experiencing a huge gap pre-COVID, and this issue will be even more exasperated in specialisms such as security architecture, security testing and network security. The softer skills that will be in demand are all centred around communication and the ability to translate cyber security into non-technical speak. Increasingly the cyber security team are having to work more closely with a company’s governance team or board, and so the ability to relay technical risks to the board is crucial and there will me many who don’t yet have this experience.

8. What type of candidates will be in demand?

The sweet spot for hires is someone with around 3-5 years of experience – they are not going to be as costly as a CISO, but they are what we call the ‘work horses,’ the boots on the ground that will deliver the strategy or project.

Even at the junior-mid experience level soft skills are important, at every level your ability to ‘sell the story’ to be able to get budget to allow security to improve year-on-year.

Given the constant pace of change in technology, training is a given in this industry and will constantly be provided, however those with a software background or industry experience will always be more desirable.



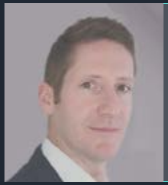
9. What type of requirements will security professionals have of their employers?

The tech industry as a whole is no stranger to a more flexible approach to working – and given the commonality of working with tech teams from other countries they have been used to remote working technologies for some time now.

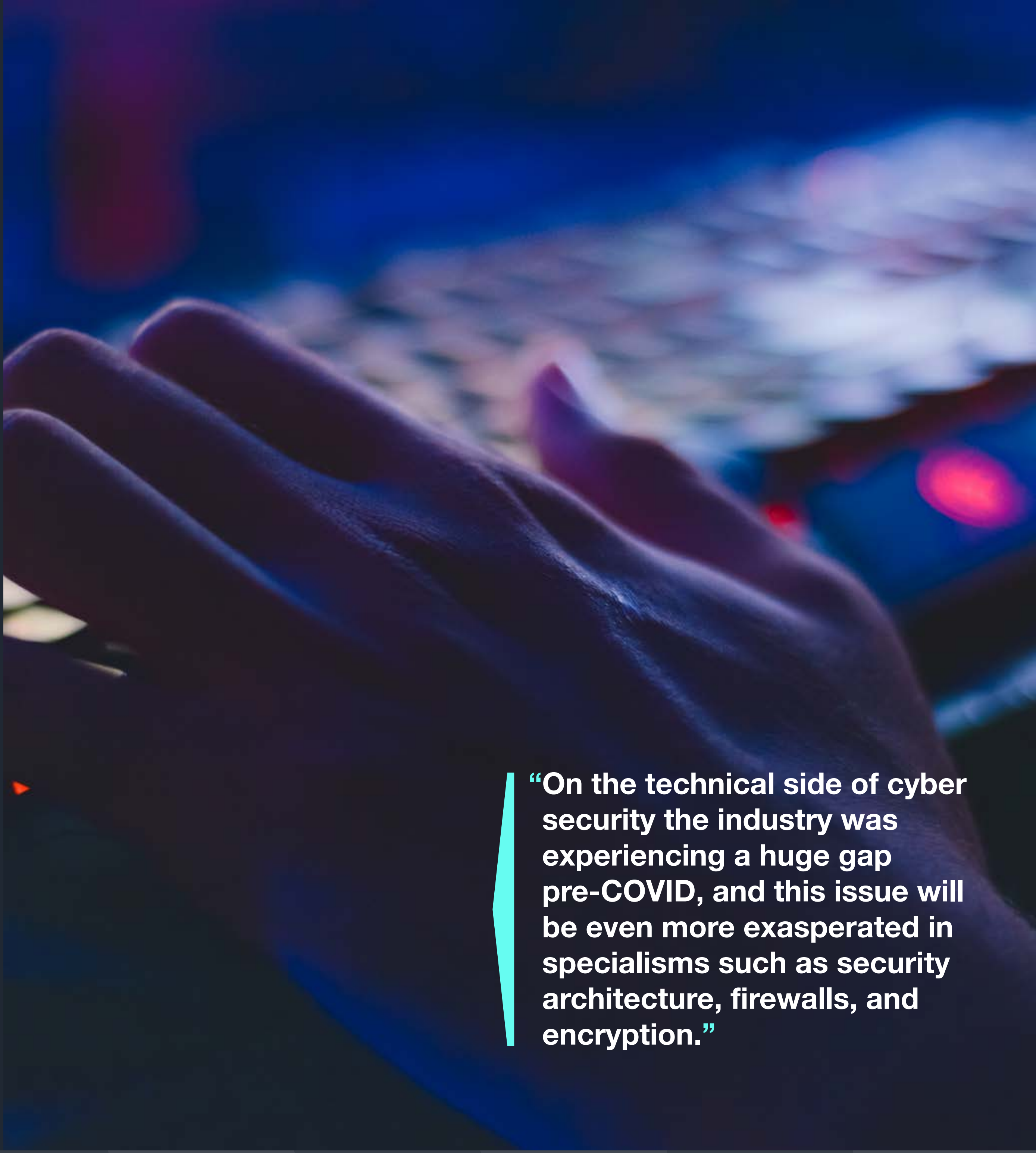
Whilst there is no denying that COVID-19 will bring about the biggest changes in employee expectations, we imagine for the cyber security world professionals are keen to work with organisations who are bought into the importance of security and who are able to make decisions relatively fast.

One thing that has always been a key driver for cyber security professionals is the variety and excitement of projects that they get to work on and this will continue to be a key trend.

Nathan Tittensor,
Director, i3Secure



Adam Casey,
Managing Director,
i3Secure Limited



> **"On the technical side of cyber security the industry was experiencing a huge gap pre-COVID, and this issue will be even more exasperated in specialisms such as security architecture, firewalls, and encryption."**

KEY FINDINGS

1 BUILDING TRUST

As cyber-attacks rose to an all-time high and GDPR took prominence in the last few years, cyber security has increasingly become a 'differentiator' for brands to be able to win new and maintain existing customers.

With the likes of Apple, Whatsapp, and fintech's all putting security at the centre of their marketing messaging, the tide has turned on how brands are able to build trust and showcase transparency to their customers. With 44% of customers stating that a cyber attack would deter them from using a website or business again, cyber security sits at the core of the solution.

2 ACCUTE TALENT SHORTAGE

With 80% of organisations undergoing some form of digital transformation during Covid-19, the IT sector has never been under more pressure. Couple that with short-term cyber security solutions that were put together almost overnight which will all need to go through a process of rationalisation, retro-fit and re-fit in order to be fit for purpose in a new world.

Currently, just a quarter of firms have sufficient cyber security staff in the UK and across Europe the sector is facing a talent shortage of 140,000 professionals this year.

3 BUDGETS INCREASING

Historically representing only 5% of a company's IT budget, cyber security has been thrust to the centre of business continuity plans – having proved its worth in enabling business objectives during lockdown.

Budgets are expected to double at the least, putting UK spending this year on cyber security to £136bn. Part of this will be the war for talent where competitive offers will be made, and the cost of consultancies fees going up as demand rises.

4 REMOTE WORKING

The immediate change to remote working highlighted to businesses the scale of their vulnerability. Industries such as law, HR, and finance will soon have much to answer for in regards to their processes of handling important and personal information at home.

Whilst remote working has been mandatory, businesses have been able to get away with weak security measures, however if they are to listen to the needs of their employees who want to continue with greater flexibility then investment needs to be put in to avoid any PR disasters.

5

RISE OF THE NORTH

Whilst London still dominates when it comes to overall cyber security employment – representing 41% of total jobs in the UK, the budding tech scene in the North is beginning to pay its dues.

In fact, cyber security job roles increased by a staggering +138% in Yorkshire and the North Eat in the past year – compared to London where job roles have stalled. Yorkshire and the North East is now the second biggest recruiter for cybersec talent, after London.

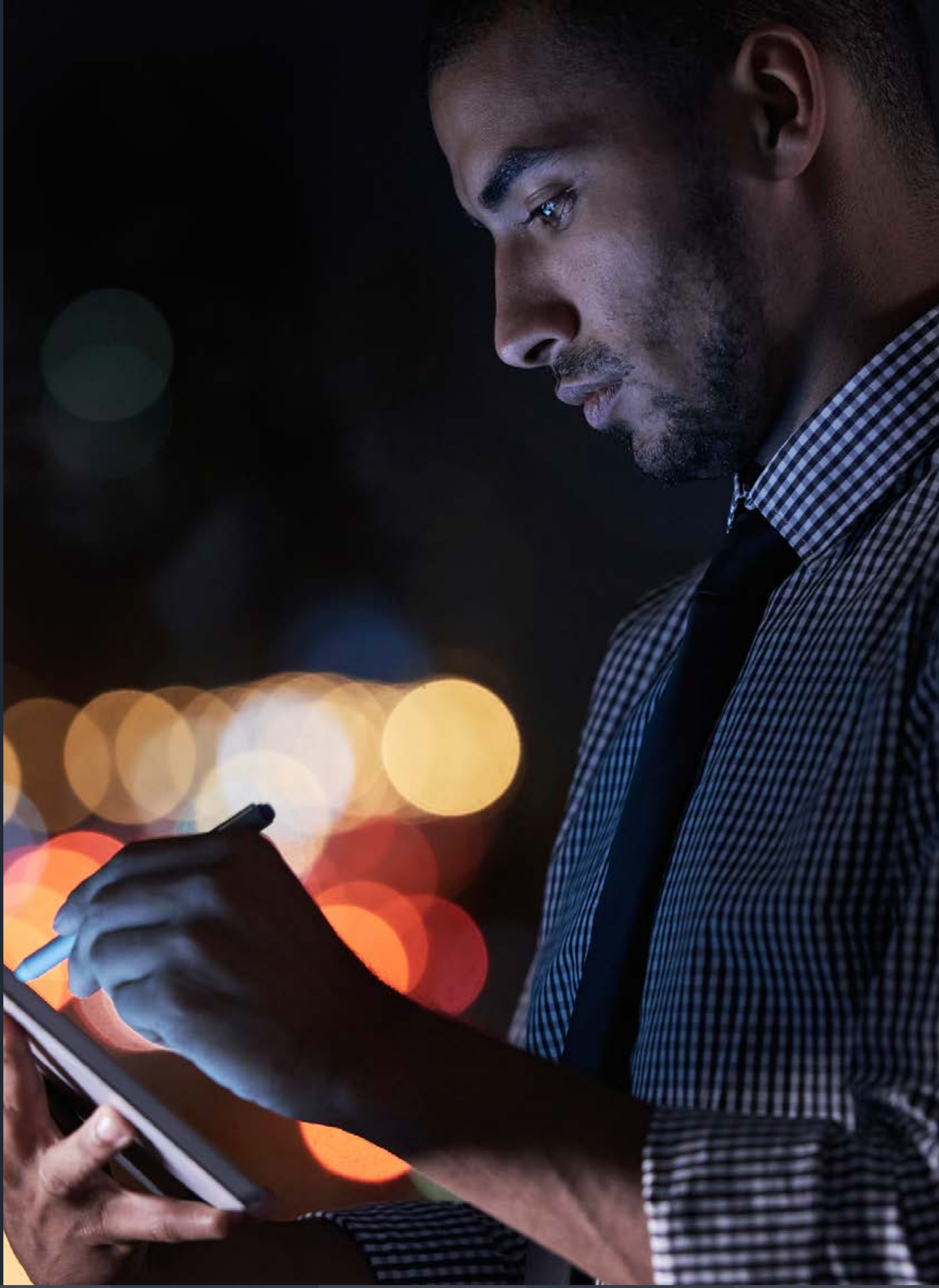
Low barriers to entry for cyber security start-ups, a thriving tech scene in neighbouring Manchester (North West), and Northern universities producing some of the industries best talent, have been some of the key drivers in the pull away from the capital. With remote working here to stay, geographical barriers are being removed in their droves.

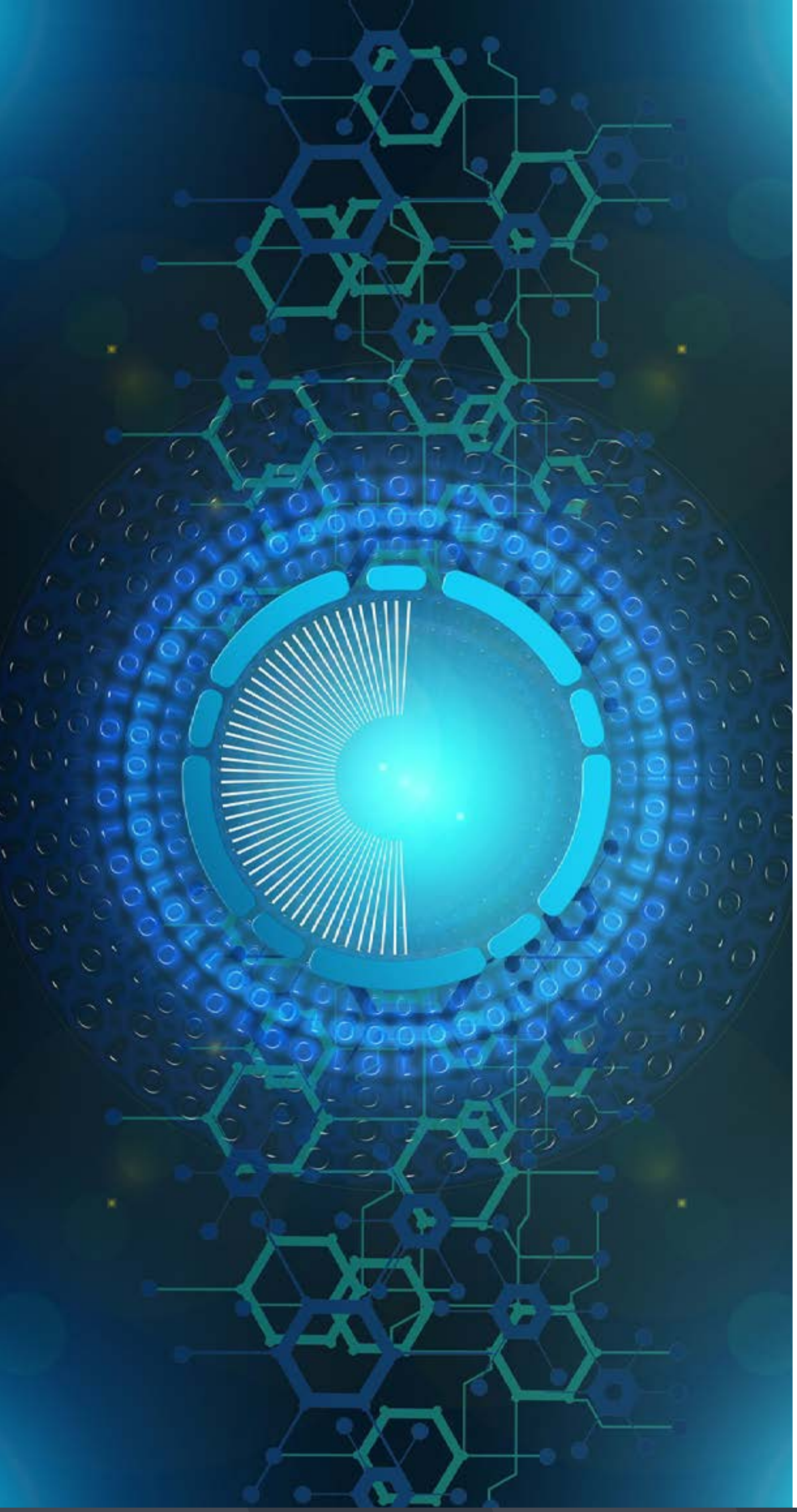
6

NEW KIDS ON THE BLOCK

Cybersecurity consultancies are one of the fastest growing start-ups in the UK, now at 1,000 companies. With the average consultancy only having 10 members of staff, firms are increasingly out-sourcing projects to these new & exciting firms promising efficient project delivery, in place of hiring a CISO and in-house team at a significant cost to the company.

The pace at which companies are having to undergo digital transformation means security projects will be continuing in volumes for some years.





ABOUT THE PARTNERS

Robert Walters

Robert Walters is a global, specialist professional recruitment consultancy. Operating across 31 countries, with offices in technology hubs in London, the North West, Midlands and South East. Organisations rely on us to find high quality professionals for a range of specialist roles. Leaders in technology recruitment, we place candidates on a permanent, contract and interim basis in organisations ranging from the largest corporates world-wide, through to SMEs and start-ups.

Darius Goodarzi, Principal - Information Security and IT Risk (London), Robert Walters
e: darius.goodarzi@robertwalters.com
t: +44 20 7509 8040

Ajay Hayre, Senior Consultant (Information Security - Midlands), Robert Walters
e: Ajay.Hayre@RobertWalters.com
t: +44 121 260 2524

@robertwalterspr
facebook.com/robertwaltersplc
robert-walters

www.robertwalters.co.uk

Vacancysoft

Vacancysoft is a subscription-based data publisher for the Recruitment Industry. Established in 2006, we now have thousands of subscribers worldwide, clients range from FTSE listed businesses to industry specialists, whereby we optimise new client generation, key account management and business strategy.

+44 20 7193 6850
www.vacancysoft.com

@vacancysoft
facebook.com/vacancysoft/
vacancysoft-llp

AUSTRALIA
BELGIUM
BRAZIL
CANADA
CHILE
CZECH REPUBLIC
FRANCE
GERMANY
HONG KONG
INDIA
INDONESIA
IRELAND
JAPAN
LUXEMBOURG
MAINLAND CHINA
MALAYSIA
MEXICO
NETHERLANDS
NEW ZEALAND
PHILIPPINES
PORTUGAL
SINGAPORE
SOUTH AFRICA
SOUTH KOREA
SPAIN
SWITZERLAND
TAIWAN
THAILAND
UAE
UK
USA
VIETNAM

www.robertwalters.co.uk