MARKET INSIGHTS:

Demand & Supply of Cybersecurity Talent in UK

TALENTSPECTRA BY

AVANCE CONSULTING

Table of Contents

Summary - Key Highlights

TECHNOLOGY LANDSCAPE	TALENT DEMAND & SUPPLY	NEW HIRING PRACTICES
£64.8bn (U$83.5bn) Global demand-side Cybersecurity spend in 2017[1]	**Information Security, Firewell, Network Security and PCI DSS** Top 4 skills in demand in the UK in 2016-17[3]	**Lateral movement from other areas within IT:** Experience in applications/testing, IT support, operations etc.
Total Software & Services spend at £51.8bn **(US$66.8bn)** in 2017	Demand for **Cybercrime, Big Data and Infomation Governance** fastest growing[3]	**Diversity hiring:** Targeted hiring to increase the percentage of women in the Cybersecurity workforce; stands at just 11% today globally.
£93.2bn (US$120bn) expected global spend in 2021[1]	**VMware, Juniper, Palo Alto, Checkpoint** top tools/ technologies used, Phenomenal growth in demand for **Hadoop, QRadar, Metaspoilt** skills[3]	**Relaxing certification requirements:** Candidates with a blend of technical and soft skills; this include team management & problem solving skills
£3.78bn[2] Total UK Cybersecurity Market in 2017, 20% of the entire EU market.	**~74,000**[4] Cyberseurity Professinals in the UK (2017) **350K** and **100K** Cybersecurity jobs expected to go unfilled in **Europe** & **the UK** by 2022[5]	**More candidates in entry-level roles:** Candidates with experience in system admin, Networking without CSE/IT Degree
Digital-enabled industries, BFSI, Public Sector, Defence & Security driving demand	**£1.9bn** allocated under **National Cybersecurity Policy** **1 out of 3** Cybersecurity professional makes between **£47,000** and **£87,000**; **39%** make more than **£87,000**	**Developing & Hiring from local talent pool:** Talent being trained & developed by PGI Cyber Academy, CompTIA, YouthFed, UK Cybersecurity Forum and other organizations

GLOBAL OPPORTUNITY SIZE		
	£11.8bn[1] Managed Security Services market (bulk of the services delivered through security Operations Centres)	**£9.7bn[1] opportunity for Professional Services** (Consulting & Systems Integration)

Source: [1]IDC - Worldwide Semiannual Security Spending Guide, Oct, 2017, [2] www.export.gov, [3] The Tech Partnership, [4] Avance Consulting Analysis, (ISC)[2], An uniform exchange rate of US$1 = £0.7767 has been used (average exchange rate for 2017)

Foreword

Dear Reader,

Welcome to TALENTSPECTRA BY AVANCE CONSULTING.

Presenting our paper **'Market Insights - Demand & Supply of Cybersecurity Talent in UK', this is the first edition of our Talent Series.**

The paper aims to provide a holistic yet concise view of the Cybersecurity talent space in the UK, to equip the hiring teams, project teams, resource management groups and business decision makers with a ready reckoner, covering the overall Cybersecurity talent market, technology trends, challenges, and evolving best practices.

While many organizations and industry bodies have published extensive survey-based reports on technology talent, they are focused on analyzing salary trends, spending patterns, and skill demand projections. There are very few concise reports which look at talent from both the demand and supply perspectives.

With an average global unemployment in Cybersecurity hovering around zero, the question that bothers decision-makers is where to look for additional talent. What are the alternative sources beyond job boards and referral hires?

We have looked at not only the current demand for Cybersecurity talent, but also at the potential supply streams within the UK. We have also included a detailed analysis of some of the hiring strategies and practices now being followed by the global System Integration companies to beat the talent crunch.

Today, the nature of Cybersecurity jobs - the roles, key skills, responsibility areas and compensation are being increasingly driven by the nature of evolving threats. In this report, we look at some of the most comprehensive, yet evolving categories of Cybersecurity roles and responsibility areas.

While we prepare the ground for yet another edition of the series, we hope that you find this paper informative and useful.

London

September, 2018

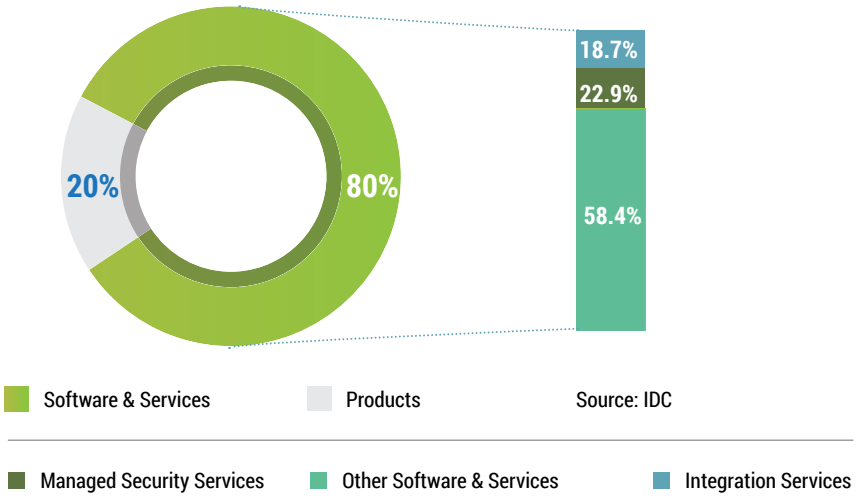
Global Cybersecurity Market

By almost all analyst estimates the global Cybersecurity spending between 2016 and 2021 is expected to grow at a CAGR of ~10%. IDC estimates that by **2021**, global Cybersecurity spending will touch **£93.2bn** (US$120bn), up from **£64.8bn** (US$83.5b) in 2017.

Organizations are acutely aware of the looming threats that affect their businesses and customers' data. Regulatory pressures, higher threat perception and the move toward Digital, is driving much of the spending.

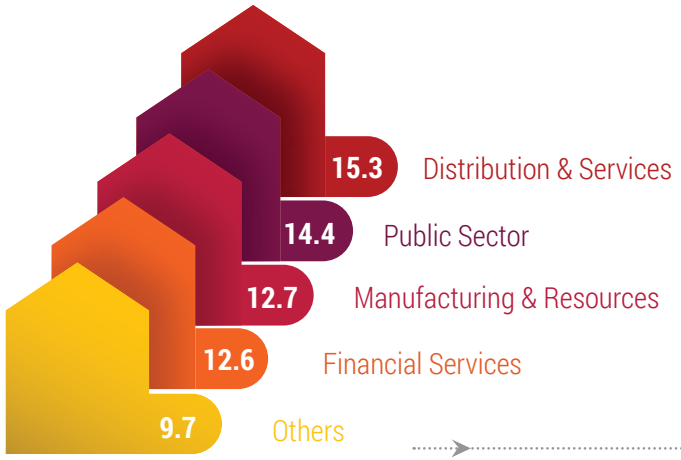
Software & Services stands out as the largest spend category; **£51.8bn** (US$66.8bn).

Global Cybersecurity Spending - 2017 (%)



£51.8bn - Global Spend on Cybersecurity Services & Software (2017)

Spending by Sectors (£bn)



Spending by Service Lines (£bn)

Cybersecurity Software spending will be led by End-point Security Systems, Identity & Access Management (IDAM), and Vulnerability Management.

Managed Security Services & Integration Services are the top picks on the services side.

An uniform exchange rate of US$1 = £0.7767 has been used (average exchange rate for 2017)

CYBERSECURITY ROLES CLASSIFICATION

Cybersecurity Skills Overview

While Cybersecurity is a defined area from a skills perspective, there are many developing factors which are continually changing the dynamics. Introduction of new technologies - **Artificial Intelligence, Machine Learning** and the increasing adoption of **Automation** tools are impacting the nature of Cybersecurity skills, their demand and supply.

Technology Skills

All Cybersecurity skill sets do not have the same intensity of demand nor do they have similar compensation benchmark. **Skills like Intrusion Detection, Penetration Testing, Application Security, Attack Mitigation** are becoming increasingly hard to find. As per the 2017 Cybersecurity Trends Report, **Incident Response** skill has been named as the most important security skill (59% of the respondents) followed by **Detection of Abnormal Systems** behavior (56% of the respondents) and **Knowledge of Critical Business Processes** (55%). The other desired skills include Malware Analysis, familiarity with commercial tools and feeds, and the ability to write correlation rules to link security events.

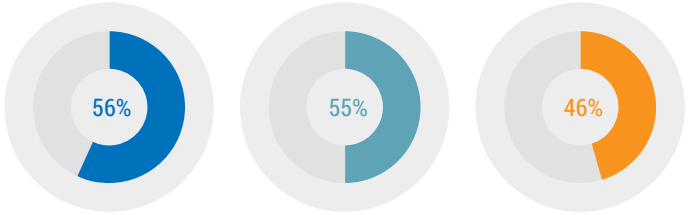
Business Skills

Today's Cybersecurity roles require more than just technology skills. At the 2016 ISACA/RSA Conference, it came out that one of the top skills that the companies value is the 'ability of the candidates to understand the business'. An overwhelming 75% of the participants said that this is one of the key skills. Interestingly, technical skills was the top pick for just 61% of the respondents.

"In the Cybersecurity domain those who can talk the business lingo and translate security in to real benefit for the business can see their career and their compensation progress fast and high"

59%
Incident Response Skills

Knowledge of critical business processes



Detection of abnormal systems behavior

Intelligence Analysis Skills

Entry-level Cybersecurity Role - The Security Analyst

Currently, the global entry-level job in Cybersecurity is that of a Security Analyst. The number of jobs is expected to see an increase of **18%** per year through 2024, 7% more than the average rate of growth across all job categories, according to a prediction done by **ISACA.** The following are the typical responsibility areas:

Primary Responsibilities

- Maintaining the security of information - planning & implementing security measures to protect systems, networks and data
- Implementing and maintaining an Information Security Risk Management Program
- Assisting in responding to incidents and investigations

Additional Responsibilities

- Also expected to carry out security research and keep up-to date with the latest security trends, vulnerabilities and attacks
- Carrying out, analyzing and reporting on vulnerability assessments

Education: A typical security analyst job requires a Bachelor's Degree in Computer Science, programming, engineering/ security or specialized degrees in security

Experience: Previous experience in IT - System/Database Administrators, Network Engineers, System Support

Classification of Cybersecurity Roles

The US **National Institute of Standards & Technology** (a non-regulatory agency of the U.S. Department of Commerce) has published the NICE Framework (National Initiative for Cybersecurity Education). It provides a ready and comprehensive reference point and lexicon to employers, Cybersecurity workers, training & certification providers, education providers. It categorizes and describes Cybersecurity work across 7 Categories, 33 Speciality Areas, and 52 Work Roles

NIST Catregories	Speciality Areas		Roles
01 Securely Provision	Risk Management Software Development Test and Evaluation	System Architecture Technology R&D System Requirment Plans	■ Authorising Official, Security Control Assessor, Software Developer, Secure Software Assessor Enterprise/Security Architect, Systems Developer
02 Operate & Maintain	Data administration Knowledge Management Customer Services	Network Services Network Administration System Analysis	■ Database Administrator,Data Analyst, Knowledge Manager Technical Support Specialist, System Admin. Network Operations Specialist, System Security
03 Oversee & Govern	Legal, Advise & Advocacy Training And Education Program / Project Mgt	Cybersecurity Management Strategic Planning And Policy Executive Cyber Leadership	■ Cyber Legal Advisor,Privacy Officer/Compliance Manager Instructional Designer,Cyber Instructor,Cyber Policy, & Strategy Planner,It Program Auditor

NIST Catregories	Speciality Areas	Roles
04 Protect & Defend	Cyber Defence Analysis Cyber Defence Infrastructure Incident Response Vulnerability Assessment & Management	■ Cyber Defence Analyst, Infrastructure Support Specialist, Cyber Defence Incident Responder. Assessment Analyst
05 Analyse	Threat Analysis Exploitation Analyst All - Source Analysis Targets Language Analysis	■ Threat/Warning Analyst, Exploitation Analys, All Source Analyst, Mission Assessment Specialist, Target Developer/ Network Analyst, Multi Language Analyst
06 Collect & Operate	Collection Operations Cyber Operational Planning Cyber Operational Planning Cyber Operations	■ All - Source Collection Manager, All - Source Collection Requirement Manager, Cyber Intelligence Planner,Cyber Ops Planner, Cyber Operator
07 Investigate	Cyber Investigation Digital Forensics	■ Cyber Crime Investigator,Law Enforcement/Counter Inteligience Forensics Analyst, Cyber Defence Forensics Analyst

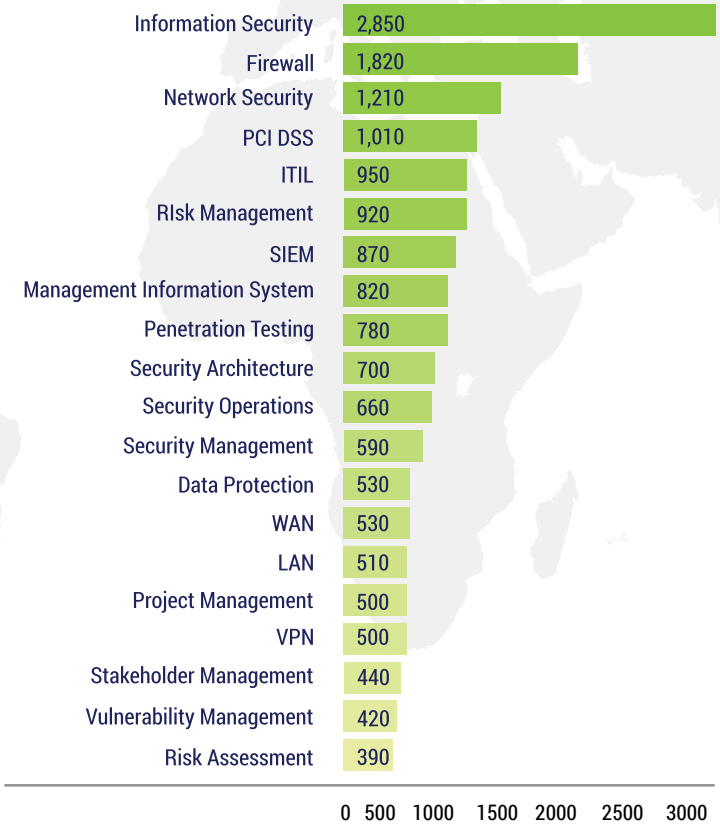
DEMAND SIDE ANALYSIS

Key Cybersecurity Roles - Skills View

In the UK, for both permanent and temporary positions, the process/methodological skills often mentioned in Cybersecurity job advertisements are - Information Security, Firewalls and Network Security. According to an study conducted by The Tech Partnership, 9 out of the top 10 skills requested on job advertisements have remained the same during 2016-2017 period. Additionally, most of the skill areas have registered higher rate of growth compared to Cybersecurity positions as a whole.

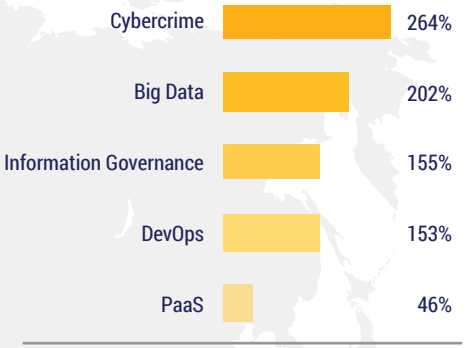
However, there are some other roles which have been growing at a much faster rate, though from a much smaller base.

No. of Jobs/adverts by 'Core' Skills/Roles



Tech Partnership's analysis of bespoke data from IT Jobs Watch, UK

Other Skills - Growth Rates (%)



Source: The Tech Partnership

Cybercrime:

Both the UK Public (Constabulary, Met Police, National Crime Agency) as well as Private sectors are recruiting for Cybercrime positions. Typical roles are - Cyber Threat Intelligence Analyst, Staff Cyber Investigator, Cyber Researcher etc. Most of the jobs need the candidate to have a Graduate degree along with a Security Clearance with experience in IT Risk & Compliance, Cybersecurity, and/or IT Intelligence exposure.

Big Data Analytics:

The International Institute of Analytics predicts that Big Data Analytics for Security will be the first line of defence when it comes to threat detection, deterrence and prevention.

DevOps:

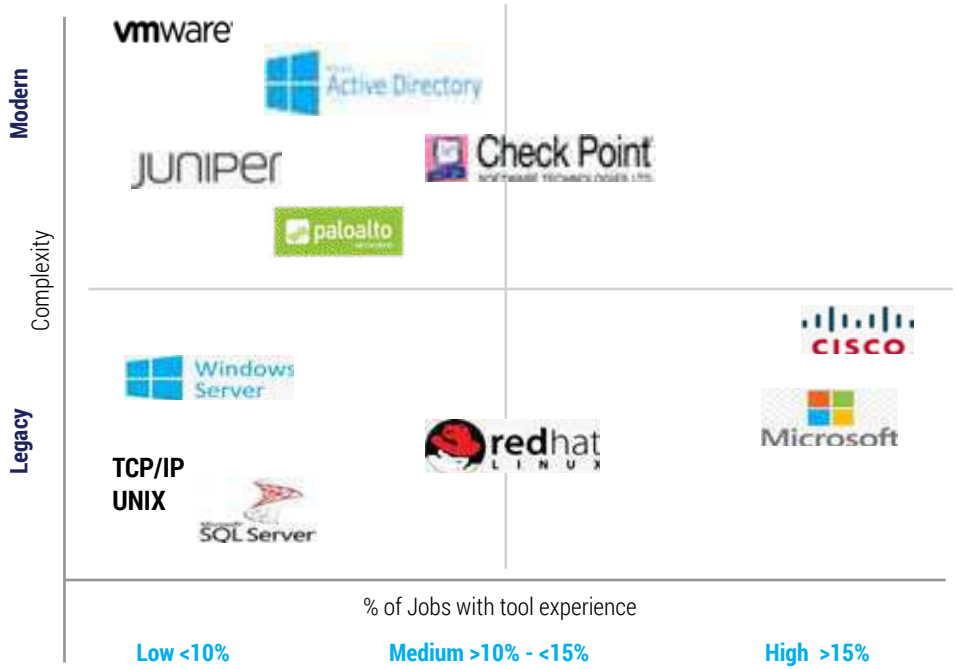
DevOps is the new keyword for Cybersecurity roles across the UK. Hiring Managers are looking for people with experience in either Linux or Windows, along with experience in public clouds - Azure or AWS. A number of DevOps tools have come into prominence and organizations are looking for experience in tools like Docker/ Kubernetes/Jenkins and infrastructure as code environment - Ansible, Puppet, Salt & Chef.

Key Cybersecurity Roles - Vendor Technology/Tools View

In 2016-2017, the most referenced tools/platforms for Cybersecurity job advertisements were: Cisco, Windows, Linux, and Checkpoint. C, Palo Alto, Java and Linux have registered stronger growth as compared to Cybersecurity skills as a whole.

The skills which make up the bulk of hiring requirements are still within the scope of **Legacy technologies.** Though the requirement for newer technology skills like **Vmware, Checkpoint** and **Palo Alto** is still small (with a small user-base) as compared to the Legacy technologies, their growth has been phenomenal in the past 2-3 years.

For e.g. the biggest increase for any specific tool/vendor in the UK has been recorded for **Hadoop, QRadar, Metaspoilt, C++ and Microsoft Azure.**



Technologies/Tools gaining traction - Typical Roles in the UK

Hadoop/Big Data	DevOps Engineer - Cybersecurity with Hadoop/Big Data, Big Data Cybersecurity consultant, Data Platform Engineer (Hadoop & Spark)
IBM QRadar (SIEM)	Information Security Analyst,SOC Analyst, Technical Consultant, Security Specialist, Senior Security Architects, Cyber Engineer, IT Ops Specialist, IT Security Engineer, Security Operations Manager
Metaspoilt	Penetration Testers, Engineer - Vulnerability Management, Assurance & Testing Analyst, Application Security Engineer, Cybersecurity Auditor, Application Security Manager, VAPT Analyst
C++	Software Developer, Software Engineer, C++ Developer
Microsoft Azure	IT Cybersecurity Engineer, Cloud Security Architect, Threat Intelligence Analyst, Cyber Response Analyst, Azure DevOps Engineer

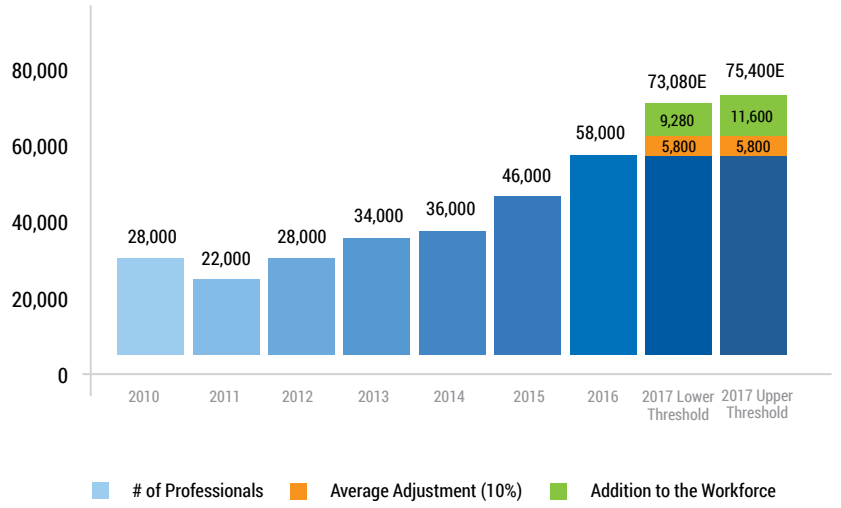
Source: The Tech Partnership

Cybersecurity Workforce estimates in the UK

For every **£1mn** increase in the overall Cybersecurity market, an estimated **19-20** Cybersecurity jobs were created in the UK in **2017**

The UK Cybersecurity market has been valued at **£3.78bn** (~US$5bn) in 2017 and by far is the largest in Europe. Despite flatter IT budgets, spending on Cybersecurity-related services is on the rise. Between 2010 and 2017, the UK Cybersecurity market has grown at an annual average of 5.44%. During the **current year (2018)**, our estimates show that the total Cybersecurity market in the UK is poised to reach **£3.98bn.**

Cybersecurity Professionals in the UK



Resultantly, expanded budgets will lead to increased hiring in key sectors.

According to an estimate by The Tech Partnership, there were approximately **58,000 Cybersecurity professionals in the UK in 2016**, up from **28,000** in 2010. Between 2010 and 2016, the number of people in the profession grew at a ***CAGR of 12.9%.*** This reflects an analysis of bespoke data from **IT Jobs** Watch and the **ONS Labour Force** survey undertaken by **The Tech Partnership.**

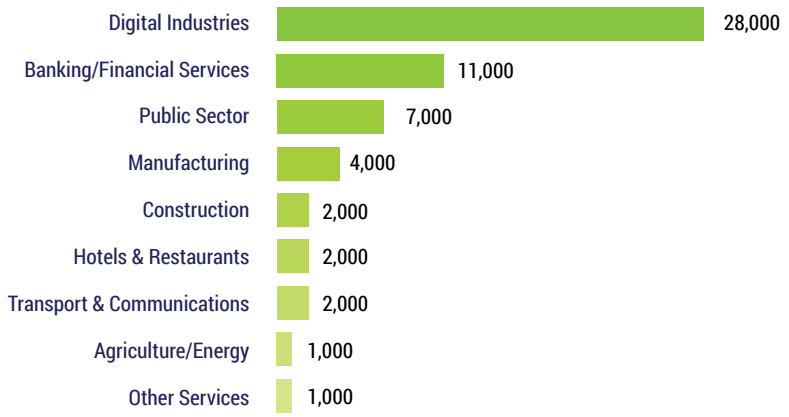
Estimates for 2017

We estimate that the number of Cybersecurity professionals working in the UK to be between **73,080** and **75,400**, in 2017; the former being the lower and the latter being the higher estimate for the year. This also includes a 10% average annual adjustment to account for new joiners in to the workforce, net immigration and re-employment of the previously unemployed.

Cybersecurity Professionals by Industry Type

- **Digital Industries** employ the biggest chunk of Cyber Professionals in the UK. This is followed by Banking & Finance. Due to increased Government spending on Cybersecurity, the **Public Sector** has moved to the forefront in terms of employing Cybersecurity professionals
- Manufacturing, Construction, Hospitality & Transport & Communications are the other important industry segments employing Cyber & Information Security professionals in large numbers

Cybercurity Professionals by Industry Type (UK) 2016



Source: The Tech Partnership, Statista, Avance Consulting Internal Analysis

Sectors driving Cybersecurity Talent Demand in the UK

1. Large Enterprises:

The bulk of the UK Cybersecurity market is oriented around large commercial enterprises. Financial Services, Utilities, Transportation companies are large spenders

2. Public Sector:

Central & Local governments are investing heavily in securing health and education data, as well as new services that are being placed online (e.g. universal credit)

3. Defense & Security:

The Defense & Security market is relatively niche and is focused on securing the country; involves the security & intelligence services as well as the UK Ministry of Defense (MoD)

4. Small & Medium Business:

Many small businesses are unprotected and are seen as easy targets. The Government is encouraging SMEs to adopt minimum Cyber requirements

Source: The Tech Partnership

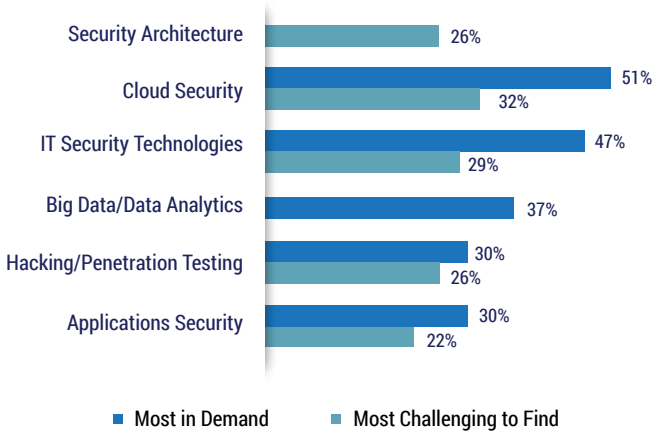
Cybersecurity Skill Gap - What it means for the UK?

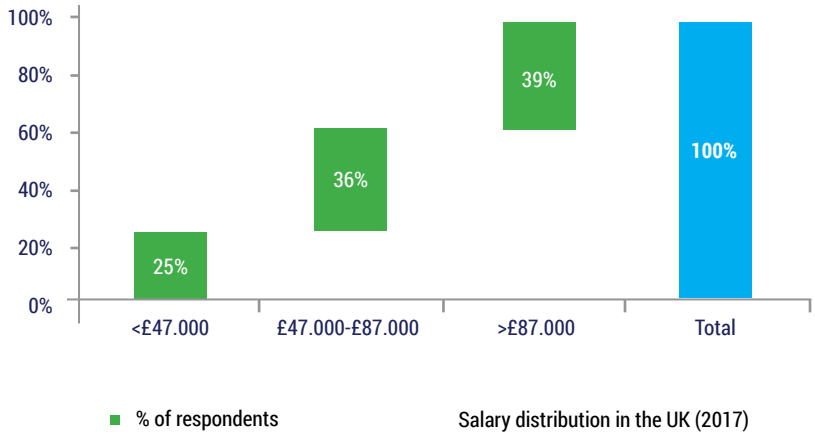
Since the Government's current National Cybersecurity Policy was unveiled in 2016, describing Britain's Cybersecurity skill gap as 'a national vulnerability that must be resolved', it is found that 66% of UK companies do not have enough information security personnel to meet their current needs, impacting economic security. Converted to numbers, by 2022 UK alone will have 100,000 Cybersecurity jobs unfilled, as against 350,000 for entire Europe and 1.8mn unfilled positions globally.

- The skills shortage also means that many UK businesses are less-than prepared for the EU GDPR, which will impose a mandatory 48-hour window for disclosing data breaches
- Close to a quarter of the respondents (22%) surveyed by ISC^2 say that it would take more than 8 days to repair the damage if their systems or data were compromised, far more than the legally required window

- In the previous National Cybersecurity Program (2011-2016), the HM Government had allocated **£860mn**; however during the current plan (2016-2021) in the face of higher threats, the budget has been increased to **£1.9bn** to tackle the evolving threats and formulate a robust national policy
- According to Cybersecurity Ventures, cybercrime will cost the world **US$6tn** annually by 2021, up from US$3tn in 2015. UK is not immune to this threat

Most sought after & most challenging to find roles* - UK





Salary distribution in the UK (2017)

Challenges in Hiring

Cybersecurity has emerged as one of the key spending areas both for the UK corporate sector as well as the Government. While entities are allocating larger funds to address security and intrusion-related threats, which has a direct positive impact on the number of roles/positions on offer, the challenge faced by talent /HR/project teams is the shortage of Cybersecurity professionals. There aren't enough people on the market with the requisite skills or capabilities who can be hired to fill the positions.

There is also a cyclical aspect to this talent shortfall that is affecting the business.

Escalating compensation benchmark:

With an existing demand-supply mismatch (where the former far outweighs the latter), the cost of hiring people is going up. The market has become very competitive which has, in turn, led to escalating salary costs. This has a negative effect on project bottom-line. 75% of UK Cybersecurity professionals earn over £47,000 annually and 39% (of the total) have salaries over £87,000, thus confirming the inflationary trend

Retention is becoming more expensive:

Typically, in a demand-supply mismatch scenario, as in the case with Cybersecurity, retaining talent becomes a challenge. Companies are forced to restructure/redesign their retention policies to make it work. This has its own financial implications

Job seekers' market:

It is estimated that unemployment levels for Cybersecurity talent in Europe is just 1%. While getting the right person for a role is challenging enough, any person with a specific skill has multiple job offers in hand. Today, the Cybersecurity job market today is being driven by the job seeker

Experienced hires Vs. training on the job?

Sample this:

- 71% of the respondents say that the biggest demand is for non-managerial staff, indicating that the bulk of hiring traffic is in the 2-4 year experience band
- Only 6% of the UK respondents stated that they will hire university graduates, while 93% emphasize the need for experience hires, thus narrowing the pool of potential candidates
- Just 12% of the current Cybersecurity workforce is below 35 years of age, an overwhelming 53% are above 45 years of age, indicating a top-heavy workforce structure which is fast approaching productivity plateau

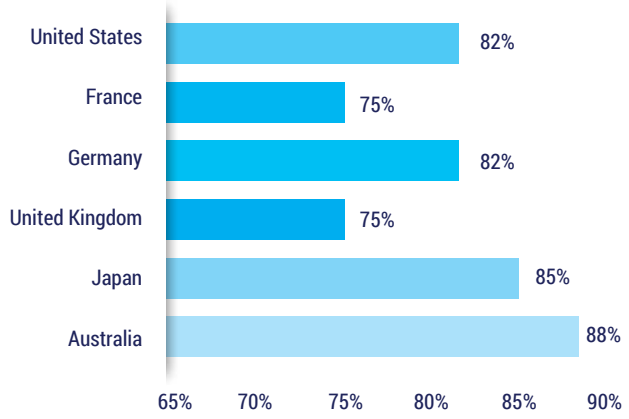
According to the ISC² Global Information Security Workforce Study (2017) British companies suddenly find themselves approaching a 'Retirement Cliff Edge'. Continuing refusal on the part of the industry to hire freshmen coupled with failure to hire university graduates has resulted in an ageing Cybersecurity workforce which will be going in to retirement soon.

Source: Global Information Workforce Study. 2017 (ISC ²)

Skill Gap Dynamics in the UK (comparison with other economies)

A survey-based study conducted by McAfee across the major geographies in Europe as well as in the Americas, found that countries likes UK, France, & Germany are relatively better placed in terms of Cybersecurity resource availability. While this is a relative comparison metric, another important metric is the **expected number of unfilled** jobs. According to the survey, by 2020, 13% to 15% of the UK Cybersecurity jobs will remain unfilled. This is much better than the overall projection of unfilled jobs globally. In France, 15% of the Cybersecurity jobs will remain unfilled.

% of respondents saying there is a shortage of Cybersecurity professionals in their country

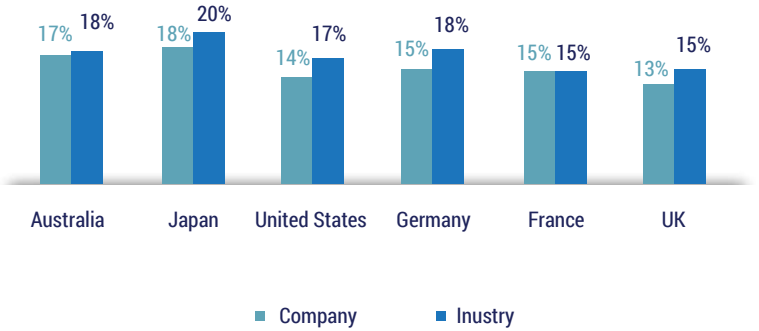


Rising importance of the CISO

As Cybersecurity becomes a matter of concern at the Board level, the role of the CISO is also undergoing rapid changes. While 97% of the respondents feel that Cybersecurity is considered to be one of the Top 10 business risks today, it did not feature in the list of the Top - 10 Board-level concerns according to Lloyd's Risk Index, 2011. CISOs in many organizations are already reporting to the Board, rather than the Chief Information Officer (CIO).

As per an estimate by IDC, 75% of CISOs and Chief Security Officers (CSOs) will report directly to the CEO or the Board of Directors by 2018.

By 2020, what % of Cybersecurity jobs in your company/Industry will go unfilled



Source: McAfee Report - Hacking the Skills Shortage, July 2016 and IDC

SUPPLY SIDE ANALYSIS

Government-led Initiatives for incubating Cybersecurity Talent

The Government has already invested **£860mn** between 2011 & 2016 in its countrywide Cybersecurity program, since the **National Security Strategy** identified Cyber as one of the top threats to the UK in 2010. It has earmarked **£1.9bn** for the current 5-year plan (2016-2021).

One of the core objectives enshrined in the UK Cybersecurity Strategy 2011-2016, has been, among other things, to make the UK a hub for Cybersecurity **knowledge, skills,** and **capabilities.** There are **8 strands** to this approach which aims to address the critical capability gaps in the industry, government as well as in the academia. They are:

Potential Talent Pool	Short-term (<1 year)	Medium-term (between 1 & 2 years)	Long-term (2 or more years)
Schools	Introduced Cybersecurity in Computer Science GCSE Cybersecurity teaching & learning materials for Key Stages 3-5	Cybersecurity Challenge Schools Program - 800 schools have participated and 23,000 students have access the complementary learning materials since 2012.	Resources for Teacher Professional Development in Cybersecurity
Higher Education	Has been included in all CSE degrees accredited by the British Computer Society and the Institute of Engineering & Technology	**Cyber First Program:** Supporting exceptional undergrads in Cybersecurity careers 12 British Universities awarded grants from the Higher Education Academy	12 Masters Degree in Cybersecurity certified by GCHQ
Further Education & Research	Has been made an integral part of computing & Digital educational qualifications at Levels 3&4 (September, 2016 onwards)	2 Centres providing Doctoral training in Cybersecurity; first batch of 100 PhDs in the subject by 2019	13 Academic Centers of Excellence in Cybersecurity Research being established 3 Research Institutes

Source: Internal Research, UK Cybersecurity Strategy Annual Report - 2011-2016

Potential Talent Pool	Short-term (<1 year)	Medium-term (between 1 & 2 years)	Long-term (2 or more years)
Apprenticeships	300 Level 4 Cybersecurity Apprenticeships; including 50 within the Government 170 apprentices have either joined or graduated since 2012 for GCHQ	—	—
Careers & Professional Initiatives	**Cybersecurity Challenge & Cyber Growth Partnership:** Mentoring & Cyber development camps for Computer Science students/graduates	**Inspired Careers:** Online hub for those joining this field Cyber security eLearning for the HR, Accounting, Legal & Procurement functions	**Cybersecurity Challenge** immersive gaming platform is a new approach to attract fresh young talent in to the profession
Educational Support & General Awareness creation	**80,000** sign-ups for Open University's Massive Open Online Course **'Introduction to Cybersecurity'** Over 2mn adults use safer online behaviors since 2014	—	—

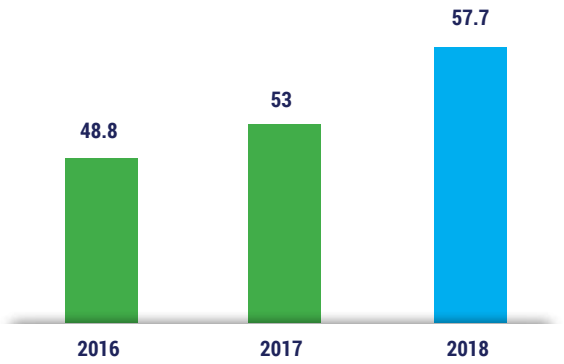
Source: Internal Research, UK Cybersecurity Strategy Annual Report - 2011-2016

Outsourcing - A Potential Source of Cybersecurity Talent

Globally in 2018, enterprises are expected to spend £71.72bn (~US$96.3bn) on Cybersecurity, an 8% increase over 2017, according to **Gartner.** By 2020 more than 60% of the organizations will have invested in multiple data security tools - data loss prevention, encryption and data-centric audit & protection being the most important ones.

While Cybersecurity spending is increasing, companies are already facing skill shortage. Since supply is limited, many companies are beginning to discover the benefits of ***Security Services Outsourcing.***

Global Cybersecurity Services Spending US$bn, 2018



Managed Security Services (MSS)/Security Services Outsourcing:

- In 2018, the global **Outsourced Security Services** market is expected to touch ~£14bn (US$18.1bn), an 11% increase compared to 2017
- The IT Outsourcing segment is the second largest security spending segment after Consulting globally

Security Outsourcing Services in the UK:

While UK is conservative in terms of its general intent to outsource Security-related services, there are some areas which organizations are looking to outsource to bring in cost synergies and efficiencies: Risk Assessment & Mitigation, Network Monitoring & Access Management, and repair of compromised systems. Some of these processes are also moving towards automation to facilitate a faster response

Which function does your organization outsource?

Functions	France	Germany	UK	US
Risk Assessment & Mitigation	49%	65%	52%	59%
Network Management & Access Monitoring	60%	68%	71%	67%
Repair of Compromised Systems	39%	45%	23%	40%

Source: Gartner, McAfee Report - Hacking the Skills Shortage

New Talent Streams - 4 Ways of Bypassing Traditional Recruitment Bottlenecks

While the shortage of Cybersecurity talent is being widely recognized as a critical issue facing companies and government, few are willing to challenge the traditional recruitment themes that are in vogue. However, the contours of alternate hiring practices are already emerging. We take a look at a few of them:

01

Beyond headhunters & job boards

The global IT talent pool is very large and related technology professions can be a source of long-term Cybersecurity talent. Companies must be willing to look for people who have strong experience in other areas of IT, and not necessarily in Cybersecurity. As more and more Cybersecurity roles become software and automation-led, people from application development and operations will increasingly find their way in to the Cybersecurity talent pool

02

Diversity Hiring

Global Cybersecurity and IT Security Professional Organization - ISC^2 estimates that just 11% of the global Cybersecurity workforce comprises of women. Affirmative action leading to proportional representation of women in the Cybersecurity workforce will open the gates to permanent talent pool

03

Redefining skill-sets

Organizations put a lot of emphasis in a candidate's technical skills as well as specific certifications. While it is very important to look for people with the right skill sets and/or certifications, making it a hiring policy automatically leaves out a lot of candidates who have the potential but are not considered due to the cut-offs. Companies need to adapt to the changing dynamics of the talent market and also look for people who have the right combination of technical skills and soft skills. Skills like team management, analytical and problem-solving skills are slowly becoming important

04

Hiring entry-level candidates

Freshers with less than 2 years of experience can be considered for junior roles. Companies should have a robust talent development/training plan which can kick in post on-boarding of new hires. Candidates without formal CSE/IT degrees can be considered for these roles, who have experience in IT, Networking or System Administration. The training plans can help fill knowledge gaps

Building a Local Cybersecurity Talent Pool

The National Cyber Security Programme is funding a pilot named Cyber Skills Immediate Impact Fund (CSIIF), which consists of **7 initiatives.** The CSIIF aims to quickly increase the diversity and numbers of people working in the UK's Cybersecurity sector. This is one of a range of initiatives designed to develop a sustainable supply of home-grown Cybersecurity talent in the UK. The pilot was launched in **February, 2018.**

Immersive Labs - The Neurodivergent Digital Cyber Academy

Helps neurodiverse candidates to develop their Cybersecurity skills.**Immersive Labs** have developed a browser-based, practical learning environment. Based on their skills the candidates will be able to apply to jobs with participating companies.

PGI - Cyber Academy

Designed for **women candidates** to get into both technical & non-technical **entry-level** Cybersecurity jobs, with paid employment opportunities. This is being implemented by **PGI-certified Cyber Academy** and recruitment specialists **Hawker Chase**

CompTIA - Cyber Ready

A **6-month** programme for candidates from a diverse range of backgrounds to up-skill around existing work, to get ready for a Cybersecurity career. Potential certifications - **CompTIA Security+** and **Cybersecurity Analyst** (CySA+)

The Integrate Agency CIC- Cybersafe Lambeth

Brixton-based programme provides practical Cybersecurity training to lone parents in Lambeth with the aim to create a community with expertise. This is in partnership with **Battersea Power Station Foundation**

YouthFed - Cyber Threat Hub Academy

Running a pilot programme to set-up a **Security Operations Centre (SOC)** in **Salford** to provide real-life work experience to young-adults interested in a career in Cybersecurity. YouthFed is partnering with **Raytheon UK** and number of other organizations to run this initiative

National Autistic Society - NAS Enterprise Cybersecurity Programme

This initiative will help develop an autism-specific apprentice scheme, through both Cybersecurity training and preparation for employment. The NAS - an UK-based charity, will conduct this training at the **Anderson School** and **Enterprise Campus** in Sussex

UK Cybersecurity Forum CIC - Community Cyber Security Centre

This is a social enterprise, representing sole traders and small and medium companies actively working in Cybersecurity. Under this programme a **Community Cybersecurity Centre** has been set up in Worcester, to train neurodiverse individuals in Cybersecurity

Source: www.gov.uk - Cybersecurity Skills Immediate Impact Fund

EVOLVING BEST PRACTICES AND NEW RECRUITMENT STRATEGIES

Evolving Best Practices in Augmenting Cybersecurity Capabilities

In this section we try to look at the various practices being adopted by organizations in the UK/Globally to deal with Cybersecurity talent crunch.

Budgets to support additional hiring

Major breaches in the past 2 years have prompted organizations in the UK & globally to increase their Cybersecurity budgets.for bolstering their defences, boosting their Cybersecurity offerings (for consulting firms) and hiring additional people

Most of the positions being filled are in the areas of Advanced Threat Monitoring and technologies to improve data protection

Deloitte is set to invest £430mn to help restore client confidence, enhance its Cybersecurity service capabilities and hire 500 additional people by the end of 2018

NHS (UK) is spending £150mn to avoid future breaches; since it was knocked by WannaCry

Investing to build technology talent pool

Some organizations have started sponsoring Graduate programs to bridge the Cybersecurity skill gap

This starts with creating a pool of candidates who can be taken in as apprentices and can be imparted on-the-job training. Some candidates will achieve foundation and full degrees while others will receive fully funded qualifications

British Telecom (BT), through its **Work Ready Program** (launched in 2014) is looking to attract talent in diverse areas related to Telecom, including Cybersecurity

To date more than **3,500** people from the UK have participated in this and almost 50% have joined gainful employment

Automation & Gamification are the new tools

Automation, is catching up with fast Cybersecurity best practices. Automation clubbed with human intelligence puts human-machine learning in to practice.

Gamification is also growing in importance as a tool to drive efficiencies in Cybersecurity hiring programs

Automated programs helps to free up resources to be proactive in threat hunting. **TCS**' AI-driven automation system **ignio** to preempt threats.

Cybersecurity Challenge UK conducts yearly competitions to recruit talent. **Marriot International** has deployed a recruiting game targeted at MIllenials. While **L'Oreal** uses **Brandstorm** to attract undergraduates, **Unilever** has added game-based assessments to its hiring process

Job Aggregator, Career Apps & Platforms

Job Aggregators and Online Digital Platforms are the newest tools to hire critical talent. Employers are hosting competitions on these platforms to zero-in on the right talent.

For hiring external talent, hosting Hackathons is also proving to be a useful resource

Kaggle and **TopCoder** platforms have got the attention of the recruiters in recent times.

Google has recently launched a local version of its job hunting tool in the UK having secured some of the largest job sites as its partners, e.g. Reed, Haymarket, and Guardian Jobs

New Recruitment Strategies - India-headquartered Service Providers

To cope up with talent-related challenges, top IT service providers are adopting alternate hiring strategies. In this section we take a look at the various initiatives undertaken by Professional as well as Business Consulting Services providers in the UK, since 2015.

Infosys

Working with Global Institutions & the academia to standardize the Cybersecurity landscape, with common language, standards & best practices:

- Working with institutions such as Global EPIC and the US-based NIST to facilitate knowledge sharing and co-creation of Cybersecurity solutions
- Has partnered with **Queen's University, Belfast** (GCHQ accredited) for a potential candidate pool of 250 students who are currently pursuing Master's & PhD programs

Augmenting capacities through investments:

- Investing in technology innovations incubated in the **Infosys Security R&D Labs**
- Create a Cybersecurity talent pool from career gamers and ethical hackers, along with an adequate knowledge and talent base for the future
- Had earlier invested US$4mn in CloudEndure (cloud-based disaster recovery solutions); additional investment was made in April, 2016

Internal Imperatives - Training & Knowledge Sharing:

- Imparting Cybersecurity knowledge to internal employees, in accordance to their roles in the organization; focusing on proactive security practices rather than reactive; and preventative than curative

TCS

Sponsoring Graduate Programs:

- Since, 2016-2017, TCS has been co-sponsoring the **Chevening TCS Cybersecurity Fellowship**, in association with the **Foreign & Commonwealth Office (FCO).** This is a 12-week fully-funded residential programme delivered at the **Cranfield University,** Shrivenham for mid-career Cyber professionals
- Also offers a year-round Graduate program positions for recent graduates and post-graduates with a minimum 2:1 degree in IT and Computer Science

Developing home-grown Cybersecurity talent:

- Has formulated a programme outlining how the government and businesses can work together to address STEM skill shortage. The Program is based on 3 pillars: Raising the profile of STEM, supporting school curricula with appropriate private sector engagement and encouraging employers to create opportunities
- Has reached over 10,000 people across UK & Ireland providing them with IT challenges - coding & application design
- Set to provide **12-month Internship** opportunities to **1,000** (between 2016 & 2020) UK STEM graduates in association with **The British Council** across TCS' facilities in India (Innovation Labs and Software Development Centres)

Leveraging its Global Alliances to create CoEs:

- As a leading provider of SOC services (Security Operations Centre), TCS has developed a **Centre of Excellence** (CoE) in India, in association with Palo Alto networks that helps its client base with Cybersecurity solutions, expertise and tools

Source: Company websites, annual report, press releases

Wipro

Sponsoring STEM Internships:

- Since 2014, Wipro has been running the **India Gateway** programme, jointly funded by the **UK-India Education & Research Initiative**. The programme - a 3-month technology induction course, followed by 6 months on-the-job training, is open to Engineering graduates from the UK

Adding to its Global chain of 'Digital Pods':

- Wipro has added **Edinburgh** on its **'Digital Transformation'** map with the opening of a **Digital Pod,** to facilitate a collaborative and adaptive workspace, enable its digital strategy, and its design and engineering teams to quicken time-to-market

Investing in Training & Certifications:

- Has a strong Cybersecurity talent pool; its global engagements are being supported by more than 7,500 Cybersecurity professionals. Out of this ~5,500+ are certified Security professionals (CISSP, CISA/CISM, CheckPoint, IBM Qradar, Arcsight etc.)
- Logs in 130,000+ annual hours of Cybersecurity training
- Language competency in 110 languages with 45+ Security Skill Experience Centre and 1,200 use cases
- More than 2,800 people trained quarterly

HCL

Plans to double its investments and headcount in the Cybersecurity practice:

- HCL is upgrading its Security Operations Centres (SOCs) in India located in Noida, Chennai & Bengaluru, which are now being called **Cybersecurity Fusion Centres**
- It is consolidating its existing centre in Cary, North Carolina and is shifting to a bigger centre in Dallas, Texas. A new centre is also coming up in Melbourne, Australia. The company already has a centre in Gothenberg, Sweden that came as a part of its recent Volvo acquisition
- Through its Cybersecurity Fusion Centres across 3 major continents, HCL is in a position to provide 24X7X365 Threat Hunting and Network Security related services to its global customers. It also has dedicated emergency response teams

Cybersecurity Centre of Excellence:

- Has established a Centre of Excellence for Cybersecurity in The Hague, Netherlands and plans to set up an Innovation Centre of Excellence in the future

Upgrading Products and Platforms

- New enhancements include advanced analytics, machine learning, artificial intelligence

Cognizant

Digital Collaboration Lab:

- Has opened a **Collaboration Lab** in Paddington, London, its second in Europe after Amsterdam (July, 2017)
- This brings together multi-disciplinary talent consisting of social scientists, design thinkers, creative technologists, to help its customers in their quest for digital transformation
- This will showcase new technologies such as IoT and Industry 4.0 in action, space for prototyping, collaboration tools and configurable workspaces.

Source: Company websites, annual report, press releases. There is not enough free-source information on HCL's alternate recruitment strategy for Cybersecurity

New Recruitment Strategies - Global Systems Integrators

Capgemini

Cybersecurity Higher Apprenticeship and Technology Degree Apprentice Program:

- Since 2011, Capgemini has already inducted 500+ apprentices, drawn from 13 country-wide locations, in to full-time roles across its offices in the UK. The program started with recruiting 44 apprentices in 2012 which was increased to 100 IT apprentices who were hired from the Birmingham region, as a part of its commitment to a Government-backed project
- This involves 9-week residential training at the **Capgemini National Training Centre,** Telford, followed by on-the-job training
- The 18-month level-4 Cybersecurity Apprenticeship program is open to candidates with A-level or equivalent. The roles offered after the completion of the program are **Cybersecurity Specialist** and **Cybersecurity Analyst.**
- The 4 1/2-year Technology Degree Apprenticeship is another source of talent for Capgemini. It provides a BSc. (Honors) in Digital & Technology Solutions for eventual roles in Insights & Data, Cybersecurity, or Software Development
- The candidates receive a salary of £10,000 annually which is raised to £16,000 at the end of 10 weeks

Capability enhancement through acquisitions:

- Capgemini, through its recent acquisition of Leidos Cyber, the commercial Cybersecurity division of Leidos has reinforced its global Cybersecurity capabilities. Apart from adding more than 500 highly-skilled professionals in Capgemini's portfolio, the acquisition also enhances the reach and breadth of its portfolio
- This acquisition is expected to equip Capgemini to meet the growing demand for Cybersecurity services

Source: Company websites, annual report, press releases

Accenture

Technology Apprenticeship Program:

- Accenture is training 40 apprentices in 2017-18 through Movement to Work; a part of Accenture's flagship Skills to Succeed program. Professionals with digital and technology skills have been a key target for the recruitment drive

New jobs created and filled with locally available talent

- It has hired 1,700 people in the UK in 2017, primarily in London and Newcastle locations. This includes 500 positions in new technology areas - **Robotics, Cyber Defence, Artificial Intelligence (AI), Data Science, DevOps and Virtual Reality (VR)**
- To expand its intake beyond University graduates, Accenture has taken in **600 entry-level** employees which include both graduates and school leavers

Launch of Accenture Digital Skills Program in the UK to address digital skills gap

- Offered through FutureLearn, a social learning platform, the courses are easily accessible and optimized for mobile to enable anytime, anywhere learning. The Digital Skills Program is designed for people returning to work after a long time, and for those looking to reskill with digital knowledge to survive in the digital economy
- There are 7 courses designed and developed by **digital experts** from Accenture - Grow your Career, Social Media, Web Analytics, Digital Marketing, User Experience, Retail and Mobile

Digital Studio incubators in London - Liquid Studios

- Working with similar incubators in the Silicon Valley, Paris and Milan, the London Liquid Studio is focused on Artificial Intelligence (AI), Blockchain, Cybersecurity, Internet of Things and cloud computing software
- Part of Accenture's Innovation Architecture, the Liquid Studios enable rapid application prototyping, and software development using Agile and DevOps principles

Source: Company websites, annual report, press releases

IBM

Partnership with the Academia:

- In 2016, the University of Warwick, in association with IBM had launched a Cyber Security Centre to design, develop and deliver a module aimed at developing technical and managerial skills in the Cybersecurity domain
- The Cyber Security Centre and IBM are also jointly developing **Master's level module** which will be a part of MSc. in Security and Management, aimed at people who are looking for technical or managerial role in the area of Cybersecurity. It is also open to people who are looking to augment their skills in this area

Cybersecurity Skills Initiative - an alternative education model (Global):

- IBM is sponsoring alternative education models such as Hacker High School and Pathways in Technology Early College High School (P-TECH) which IBM started in 2011. The idea is to define newer workforce strategies to create a broader pipeline of candidates based on skills, experience and aptitudes as opposed to traditional hiring models based on Degrees alone. These programs include skills-based education, training and recruitment - vocational training, coding camps, professional certification programs and innovative public/private education models

'New Collar' jobs:

- A new initiative by IBM and ISECOM, focuses on bringing Cybersecurity exposure and skills to students - as a part of this collaboration IBM provides sponsorship, expert guidance, and IBM Security Tools for a new Hacker High school lesson to build up skills needed for an entry-level SOC Analyst. Participants have unique access to market leading tools such as IBM QRadar and security analytics
- IBM has redefined the way of attracting and recruiting Cybersecurity talent - IBM calls them 'New Collar' employees, which prioritizes skills and capabilities over degrees - as opposed to 'Blue Collar' or 'White Collar'. Since 2015, nearly **1 out every 5 new hires in IBM's Cybersecurity business are 'New Collar' employees**

Bringing in AI to complement Cybersecurity - IBM Watson on BlueMix platform

- IBM has Partnered with 8 U.S. Universities (chosen on the basis of their strength in Cybersecurity program) in a year-long research project to provide IBM Watson (this leverages Machine Learning with Natural Language Processing) with the requisite data to expand its security protocol and to be eventually made a part of IBM's **Security portfolio for SOC** use - **Cognitive SOC**
- Students and faculty input security data while Watson learned the specifics on Cybersecurity. It has plans to build up to 15,000 documents per month, containing threat intelligence reports, cybercrime strategies and threat databases. 40 organizations globally have already become a part of IBM's Watson Cybersecurity beta program
- The project, powered by IBM BlueMix platform helps security analysts with advisory support to be able to respond to threats effectively across networks, endpoints, users and the cloud
- IBM is now looking to **commercialize its Watson for Cybersecurity** offering and expecting it to evolve in terms of functionalities, as more participants join in
- Has showcased the solution at **CYBERUK** in April, 2018

Source: Company websites, annual report, press releases

Conclusion

What is common among some of the world's largest and professionally managed companies -Yahoo Inc., Equifax, eBay, Target Stores, Uber, JP Morgan Chase, Sony PlayStation Network?

They all have been prime targets of **Cybercrime** - DDoS, Data Breaches, Identity theft, Malware, and phishing emails to just name a few. They have witnessed the worst cyber attacks in recent memory. Moreover, it is not just corporations - large or small, numerous Government agencies and departments have also become victims of organized cyber crime - particularly those which are sponsored by hostile state/non-state actors.

Gartner predicts that the global enterprise security spending is expected to top **US$96bn** in 2018, registering an y-o-y growth of 8% over 2017 (US$89.1bn). Organizations will spend more on security as a direct result of regulations (e.g. GDPR), shifting buyer mindset and an increasing awareness of emerging threats and evolution of the Digital technologies. Security software vendors, organizations and Governments are finding it increasingly difficult to cope up with the shortage of qualified people who can take up the ever-increasing Cybersecurity job roles.

By **2022,** it is estimated that **100,000** Cybersecurity jobs run the risk of going unfilled in the UK as against a global figure of **1.8mn.**

Alternative sources of talent (less than a 4-year University Degree in Computer Science) are being looked at; **apprenticeships, sponsored technical degrees/diplomas, diversity hiring, hackathons,** and **Bug Bounty** programs have caught the attention of recruiters globally.

The imbalance between demand and supply of Cybersecurity talent in the UK and elsewhere will continue unabated for at least the next 3-4 years before it stabilizes. Till then the challenge will be two-fold; to **attract** and **on-board** the right talent and to **retain** the talent to gain competitive advantage.

TALENTSPECTRA BY

AVANCE CONSULTING

TALENTSPECTRA is the advisory and insights team of **Avance Consulting**, a world-class provider of innovative talent acquisition solutions and Executive search services. With a global presence in the UK, US and India, it brings together a decade-long experience in recruitment best practices matched by a strong service delivery ethos.

Continuous evolution of Digital business models has disrupted the existing norms; new roles are being created while old ones are becoming redundant. Hiring methodologies are changing and re-skilling initiatives have taken the centre-stage. Automation, Cloud & Cybersecurity, IoT and Immersive Technologies are driving the next round of change. Businesses are becoming more customer-centric and decision-making being driven by Data.

We aim to partner with our customers and stakeholders in their recruiting journey by providing them with information & analyses pertaining to **talent acquisition**, combining the dimensions of Business, Technology and Skills.

Backed by a strong understanding of Digital Technologies and IT landscape, **TALENTSPECTRA** is the right partner to assist you in your day-to-day decision-making.

TALENTSPECTRA BY

AVANCE CONSULTING

Learn more about us at:

https://www.avanceservices.com/about-us

For enquiries, questions and feedback, connect with us at:

talentspectra@avanceservices.com