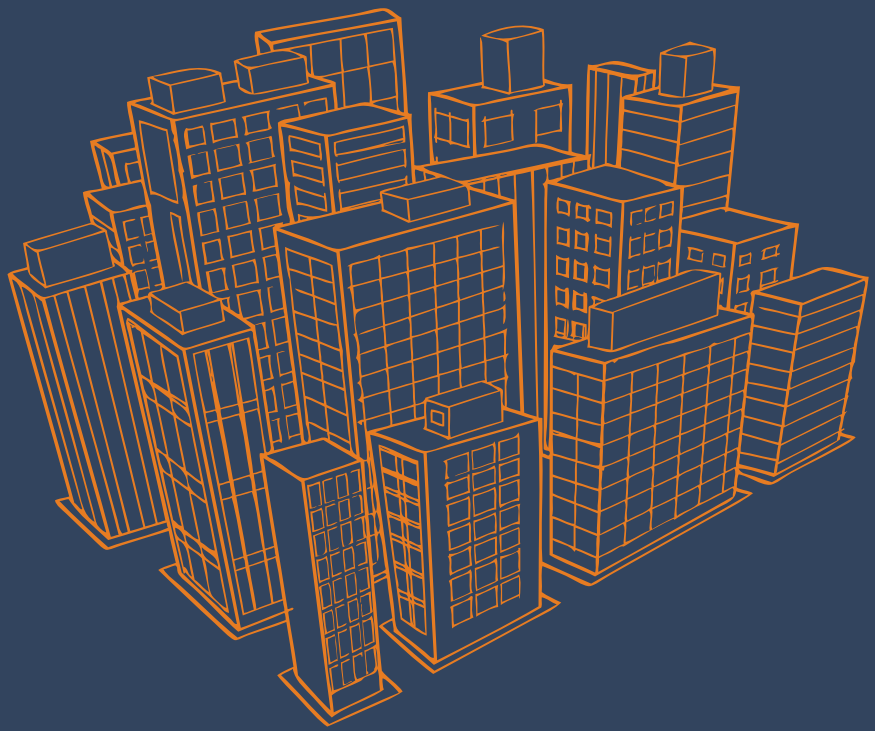
Experis™
ManpowerGroup

Tech Cities Job Watch

Q4 2016



IT Security

About Experis and **Tech Cities Job Watch**

As technology continues to significantly impact all aspects of business, companies in cities across the UK vie for top tech talent, so they can build their ability to innovate and cater to demand.

Yet, as the technology sector has evolved, so have the skills, expectations, and demands of the talent that powers it. As a result, employers are finding it increasingly challenging to find and secure the skilled individuals their business needs.

By combining the latest market intelligence with Experis insights and expertise, the Tech Cities Job Watch report provides employers with a barometer of the changing workforce dynamics within the technology sector. Five key disciplines are focused on in particular: Big Data, Cloud, IT Security, Mobile and Web Development.

It also puts a spotlight on the emerging opportunities and challenges businesses face in 10 UK cities that are rapidly developing reputations as technology cluster hubs - London, Birmingham, Brighton, Bristol, Cambridge, Edinburgh, Glasgow, Leeds, Manchester and Newcastle upon Tyne.

Experis is the largest IT recruitment specialist in Europe. We have been at the forefront of the search for the best in IT talent for over 25 years, placing tens of thousands of candidates.

Experis has the deep industry knowledge to understand the challenges organisations face and the access to highly skilled professionals to help companies seize opportunities.

Contents

Follow us on social:

Visit us at:
www.experis.co.uk

Call us on:
020 3122 0200

Foreword

Recent years have seen an explosion in the Internet of Things. It's created endless opportunities for businesses to deliver new innovations, create enhanced user experiences, and streamline their internal processes.

Yet, as organisations strive to deliver more value from their digital assets, they're faced with an ever-intensifying threat from cybercriminals. After all, as technology platforms become more closely connected, the potential for more complex and severe security issues increases. With numerous security breaches making the headlines recently and the EU General Data Protection Regulation (GDPR) reform due next year, the importance of fail-proof IT Security cannot be understated.

With this in mind, it comes as little surprise that IT Security has steadily risen up the boardroom agenda. Business leaders recognise that they can drive more value and better results out of their digital presence; but, at the same time, they realise they must also invest in their defence against potential security threats. Consequently, employer demand for IT Security skills has continued to rise, unabated by Brexit.

However, as our latest Tech Cities Job Watch report showcases, a shift in how organisations integrate these skills into their workforce has emerged. Businesses are no longer focusing solely on short-term fixes to plug the gaps. There's still a time and a place for this, but they're now also recognising that they need to develop their long-term defence against hackers.

As a result, organisations are increasing their investment in their permanent workforce, to ensure IT Security skills are embedded into their organisation for the foreseeable future. And, with expertise in this area in short supply, contractors are being used as a means to upskill existing employees.

IT Security has been one of the most critical and serious issues faced by businesses over the past few years. And, as the threats continue to intensify, it shows little sign of easing anytime soon. I hope you find this report a useful tool, as we all look to protect our organisations against potential security issues. As always, I would really value your feedback on our insights. Please feel free to reach out to either myself or one of our team if you'd like to discuss your own experiences in sourcing IT talent across the UK's Tech Cities.

Best wishes,

Geoff Smith
Managing Director, Experis Europe

Executive **Summary**

In Q4 2016, the demand for IT Security skills continued to surge to 46%. There were a total of 4,442 permanent IT Security roles advertised, with an increased quarterly and annual demand of 17.42% and 52.91%, respectively.

In comparison, demand for contractors rose by 15.28% year-over-year, with 762 IT Security roles advertised in Q4 2016. The top cities that demanded both temporary and permanent security experts were London, Leeds and Birmingham.

In terms of job roles, Security Engineers, Security Consultants, Penetration Testers, Security Analysts and Security Architects were the most sought after.

Key **Takeaways**

continued **surge in demand** for IT Security skills

Cybercrime **moves to the top** of the C-Suite agenda

The growth in the permanent over contractor market was reflected in pay too. Annual IT Security permanent salaries climbed across ten cities by 4.99% compared to 0.62% for contractor day rates.

However, the situation is reversed when all ten cities and five technology disciplines are observed. Advertised contract roles grew by 18.25% from Q4 2015 (with a total of 5,450 roles in Q4 2016).

In contrast, the number of permanent roles advertised this quarter grew by 6.38% (a total of 27,226 roles) from Q4 2015.

With regards to salary the split was more balanced. Across the ten tech cities and five disciplines, average permanent salaries grew by 6.83% since Q4 2015.

This quarter, the average day rate of £450 increased by 6.38% compared to the same period of 2015. All disciplines saw an annual growth, apart from Web Development, which dropped by 0.88%.

Salary Watch

Permanent salaries

Across the ten Tech Cities, average permanent salaries grew by 6.83% compared to Q4 2015, with all disciplines experiencing year-on-year growth.

Average permanent salaries for the key five disciplines across the ten tech cities

City	Big Data	Cloud	IT Security	Mobile	Web Dev	City Average
Birmingham	*£65,727*	*£52,185*	*£47,544*	*£39,589*	*£40,768*	*£43,949*
Brighton	^	*£43,777*	*£50,702*	*£46,625*	*£32,634*	*£41,821*
Bristol	*£55,109*	*£52,738*	*£48,106*	*£37,600*	*£33,304*	*£40,227*
Cambridge	*£47,277*	*£41,265*	*£50,643*	*£42,163*	*£33,706*	*£40,228*
Edinburgh	*£74,795*	*£47,273*	*£48,108*	*£45,671*	*£37,478*	*£44,864*
Glasgow	*£46,188*	*£44,212*	*£45,113*	*£41,123*	*£37,077*	*£40,835*
Leeds	*£52,304*	*£44,938*	*£41,749*	*£38,906*	*£38,739*	*£40,337*
London	*£71,521*	*£62,702*	*£62,596*	*£57,002*	*£46,763*	*£58,063*
Manchester	*£49,004*	*£46,310*	*£44,831*	*£41,423*	*£36,375*	*£40,548*
Newcastle upon Tyne	*£65,917*	*£47,441*	*£41,392*	*£33,106*	*£30,750*	*£35,867*
Average	*£68,799*	*£58,036*	*£57,706*	*£52,053*	*£41,990*	*£52,337*

** Shading to indicate the top three cities, salary-wise for each discipline*

IT Security

Across the ten cities, average permanent salaries for the IT Security discipline in particular grew by 0.46% compared to the previous quarter, and by 4.99% year-on-year.

Unsurprisingly, London offered the highest average salary of £62,596. This was almost a fifth (19%) higher than any other region. Permanent salaries for IT Security roles in the Capital have climbed annually by 6.92%, with pay rates increasing every quarter since Q4 2015. Outside the Capital, Brighton and Cambridge offered the highest average salaries, at £50,702 and £50,643, respectively. This is in spite of Cambridge's average salary decreasing by 14% compared to the previous quarter, representing the biggest drop across all cities.

Comparing salaries from Q4 2016 to the previous quarter and prior year, Bristol saw the largest annual increase in permanent salaries at 9.34%, whilst Newcastle saw the biggest drop at 21.55%, losing its position as the third highest paying region. In contrast, Edinburgh reported the biggest quarterly increase of 7.01%, whilst Cambridge saw the biggest drop of 14%.

Contract rates

This quarter, the average day rate of £450 was 6.38% higher than the same period of 2015. All five technology disciplines saw an annual growth - apart from Web Development, which dropped by 0.88%.

Average contractor day rates

City	Big Data	Cloud	IT Security	Mobile	Web Dev	City Average
Birmingham	£425	£392	£422	£284	£272	£341
Brighton	^	^	^	^	£360	£267
Bristol	£593	£447	£326	£468	£228	£394
Cambridge	£482	£353	^	£325	£321	£348
Edinburgh	^	£476	£586	£378	£316	£426
Glasgow	£303	£348	£322	£344	£364	£338
Leeds	£421	£425	£454	£389	£318	£368
London	£555	£502	£501	£421	£354	£471
Manchester	£530	£437	£442	£348	£307	£390
Newcastle upon Tyne	^	£330	^	£387	^	£341
Average	£548	£482	£484	£409	£338	£450

** Shading to indicate the top three cities, salary-wise for each discipline*

IT Security

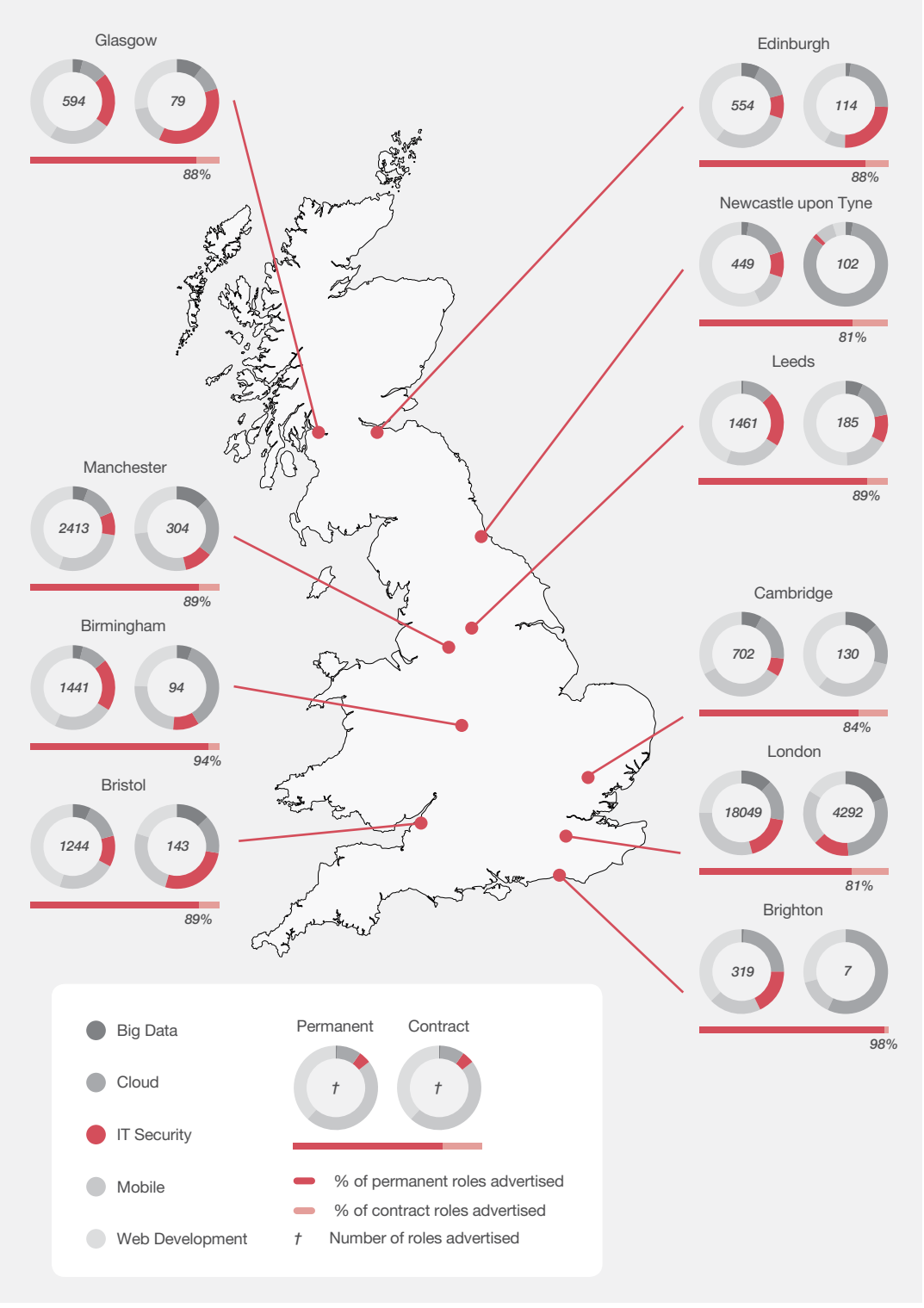
Within the IT Security discipline, average day rates across the ten cities rose by 4.54% compared to the previous quarter, and by 0.62% compared to prior year.

Edinburgh not only offered the highest average day rate of £586, but also saw a quarterly and annual growth of 25.49% and 43.98%. Following Edinburgh, the top paying cities were London (£501) and Leeds (£454).

Comparing day rates to Q3 2016 and Q4 2015, the Capital saw an increase of 7.28% and 0.2%, respectively. This meant London regained its status as the second highest paying city for IT Security. Leeds, however, saw the biggest annual decrease, at 7.91%. Nonetheless, it kept its position as the third highest paying city out of the 10.

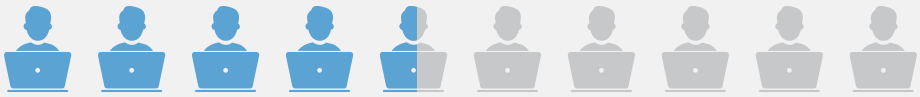
Employer Demand

A national comparison of permanent versus contract roles for employer demand (for the five key technology disciplines, across the UK's 10 tech city hubs).



Permanent

The number of permanent roles advertised across all ten cities and five disciplines in this quarter, grew by 6.38% compared to the same period of 2015 - a total of 27,226 roles.



Annual demand for permanent and contractor IT Security professionals combined has **increased by 46%**.

IT Security

Within the IT Security discipline, there were a total of 4,442 permanent roles advertised in Q4 2016. This represents a quarter-on-quarter rise in employer demand of 17.42%, and a rise of 52.91% compared to the same period of 2015. As a result, the permanent market considerably outperformed the contract market, which only saw an annual increase in employer demand of 15.3%.

There were almost three times as many permanent IT Security roles advertised in London (3,164) in Q4 2016 than in every other region in the country combined (1,278). The city also saw a quarterly growth in demand of 25.66%.

Outside the Capital, Leeds (303), Birmingham (281) and Manchester (222) experienced the highest demand for IT Security professionals this quarter.

IT Security skills in demand for this quarter are **CISSP** [Certified Information Systems Security Professional], **SIEM** [Security Information and Event Management] **SOC Analysts and Engineers and Security Architects**, as well as **biometrics** and **penetration testers**.

Contract

Contract roles across all ten cities and five disciplines grew by 18.25% compared to Q4 2015 (with 5,450 roles advertised).

Employer demand for IT Security contractors only saw an **annual increase of 15.3%**

IT Security

Employer demand for IT Security contractors only saw an annual increase of 15.3%, compared to a 52.91% growth in permanent roles. With just 762 IT Security roles advertised in Q4 2016, there was also a quarterly advertising decline of 17.89%.

The Capital remained the city with the highest employer demand for contractors and this outstripped permanent demand in the same area. Almost 80% (604) of contract IT Security roles that were advertised were based in London.

From a regional perspective, Bristol, Manchester and Glasgow saw the highest number of contract roles advertised for IT Security professionals.

Insights

A talent-driven security strategy

Current **state**

There was a time when corporate security was a perimeter issue. One that could be addressed by walls, locks and a few beefy-looking personnel. Today, every person, and every smart device is - inadvertently or otherwise - a potential security threat.

The associated drivers are not always economic in nature. The spectrum encompasses mischief-making through to ideological motivation.

Here are some recent examples of high profile breaches:

- Clinton presidential campaign – **thousands of party emails released onto WikiLeaks**
- Anthem health insurer – **records of 80 million customers exposed**
- Dailymotion video sharing service – **over 82 million emails extracted**

Consumers need to feel confident that their privacy is respected. Such compromises resonate at the highest levels of the organisation concerned. Thus today, IT Security is a leadership issue. And, as we will see, IT Security talent lies at the heart of the solution.

An organised **foe**

At one end of the spectrum, hacking is a sport conducted between teenage gangs, where the victims are simply numbers on a scoreboard. At the other end, the attacks are carefully crafted. The perpetrator sees the workforce as a soft entry point into the target organisation.

The growth of the **Internet of Things (IoT) will provide perpetrators with millions of new entry points**. Robots and algorithms will add to the assurance headache.

In many respects, the hacking ecosystem is much better organised than that of the victims.

For example: a wallet is stolen, the thief pockets the cash and then puts the cards on the black market for sale. That card could be cloned and reused for a short period. Or it could be bought by an organisation who, having established the owner and where they work, can use it to target the workplace.

This can either be opportunistic, or it might be that the card buyer has been waiting patiently for a card associated with a strategically important organisation.

The growth of the Internet of Things (IoT) will provide perpetrators with millions of new entry points. Robots and algorithms will add to the assurance headache.

Workforce **culture**

Security breaches can have a negative impact on culture. Workers wonder who they can trust. Perhaps the breach came about through a thoughtless click on a link in what looked like a plausible email from a credit card company. Or perhaps an individual working at the organisation is responsible, knowing that their family is at risk if they do not comply with the perpetrator's instructions.

Often, the workforce is inadvertently a security risk through:

- **Basic human error** in respect of data management, including misplaced USB sticks, inadequately secured devices, and sending data to others without checking their security status
- **Lack of awareness** in respect of why passwords are not to be shared and the need to treat email web links with great caution

Such issues can be resolved by the creation of appropriate information security policies, coupled with management action to weave them into the culture so that they are followed. Education is an important element of this cultural transformation.

Many years ago, we lived in settlements. We were on the inside, and they were on the outside. The perimeter walls demarcated the boundary. Today with outsourcing, extranets, crowdsourcing and the gig economy, the boundary has become blurred. We are used to seeing strangers in our office; though, of course, it would be a mistake to assume that those we don't know are to be trusted less than those we believe we know. The accelerating clock speed coupled with market volatility means that the workforce will be increasingly transient, as talent management takes on a more tactical approach. Despite the difficulty of retaining the workforce, it is safe to say that IT Security specialists will be part of the talent landscape for the long-term.

Emerging **challenges**

The IoT has already been mentioned as a potential security vulnerability. The risks associated with wearable healthcare devices, including pacemakers, and driverless cars are significant. The possibility of terrorists commandeering delivery drones to launch a swarm attack on a commercial plane is a reality. Artificial intelligence (AI) has also become part of the hacker's armoury, and AI-driven business processes will be a new target for hackers.

The Digital Age means that we are living more of our lives online, which in turn means we are more exposed to security breaches. As the IoT migrates from machines to the everyday usage of people, this again increases the security risk from a workforce perspective.

Organisations are under constant pressure to accelerate their innovation cycles to get products and services to market faster. The notion of the minimum viable product, as a means to test whether the market likes the offering, exposes both the buyer and seller to security risk. In such circumstances, security assurance is often an afterthought, or something that will be addressed if the market bites.

> **"Increased connectivity in the IoT age is something else that keeps security professionals awake at night. We're all linking things like smart watches and bands, medical devices and our home appliances to the internet, leaving each one of us vulnerable to dangerous and widespread hack attacks. To mitigate against this ever-intensifying threat, it's important that organisations can get in place the security personnel they need to help them batten down the hatches."**
>
> ***Chris Hodson, Zscaler***

Talent matters

We could not have anticipated this exponential growth in new technology capability, and the extent to which it would permeate our lives. Unfortunately, this is reflected in the supply-demand imbalance of IT Security professionals, whom we need to ensure that our safety and privacy as consumers and citizens are preserved.

Even if there was a Government-backed initiative to build dedicated IT Security universities today, it would be another five or more years before the students were of sufficient industrial-strength to be effective cyber professionals. In any case, a syllabus developed today would by its very nature be addressing yesterday's security challenges. Keeping up with emerging and zero-day threats will be a challenge.

Recommendations

Take **action**

1. **Ensure your organisation treats information security as a leadership issue** – it needs to be owned by a CxO, rather than being an isolated team sitting in the far corner of the IT function

2. **Regard threats as inevitable** and operate as if you are already compromised

3. **Invest in the best IT Security talent**. Technology investment is not enough - someone has to choose, deploy and manage the tech. You also need policy specialists and ethical hackers, along with specialists who can weave policy into the processes and culture of the organisation

4. **If you already have great people, do all you can to keep them**. Explore what will motivate them to stay, and don't wait until the exit interview to find out. Money might work in the short-term, but offering ongoing opportunities to up-skill are likely to boost retention in the long-term. Such initiatives might include:
   - Hiring contractors with the aim of transferring their skills to your people
   - Encouraging your people to experiment with new technologies

> **"The tech industry is going through rapid expansion, and the breadth and depth of talent simply isn't there to meet the growing demand for skilled individuals who can propel organisations forward during this period of flux. To counter this, there must be an emphasis on nurturing existing employees. Don't focus on what they know, but whether they have the aptitude and mindset to learn new skills."**
>
> ***Mark Segelov, Information Security Director***

5. **Identify potential specialists who have worked at the periphery of security** - for example network administrators - who might appreciate the opportunity to embark on a career in IT Security

6. **Work closely with the talent supply chain**, such as universities and recruitment specialists. Don't wait to see what they have; engage in co-developing talent solutions in anticipation of what lies ahead

7. **Manage your staff mix with care**. Certain security requirements will be an intrinsic part of your business model, so it makes sense to opt for a permanent solution. At the same time, some requirements will be incident-based, so a temporary talent solution may also be necessary

Conclusion

The challenges associated with information security are growing, in line with the exponential evolution of technology and our increasing reliance on emerging technologies. Some challenges can be anticipated; but many cannot. We need the judgement and skill that only IT Security professionals can provide to navigate this hostile territory.

IT Security talent management needs to be at the fore of your organisational strategy.

Expert Opinion

Chris Hodson, Senior Director of Information Security, Zscaler

The two key areas we're consistently talking to our customers about now are encryption and the uptake of cloud technologies. While the fact that web traffic is increasingly being encrypted is good news for consumers (as their data can't be snooped on by unwanted eyes), it prevents security professionals from being able to monitor it – and potentially harmful malware that may have infiltrated it – as it passes through their network. Looking at cloud uptake, organisations are leveraging the benefits of on-demand elastic computing that can be scaled up and down as needed.

Moving ever greater volumes of data to the cloud, however, requires more bandwidth. If this bandwidth isn't available, the user experience can be affected, leaving workers open to higher latency and network implications. Cloud-based collaboration platforms (e.g. Office 365, Google Apps) are a great example of this: the business benefits are well known but there are hidden costs in terms of significantly increased bandwidth, operations management and network configuration. At Zscaler, we are helping many of our customers on this journey.

Another area that organisations are growing concerned about are the increased data security regulations and legislation being put in place to protect critical assets and IP. One example of this is the General Data Protection Regulation (GDPR), which is set to come into force in the UK from May 2018. While the implications of GDPR have pushed cyber security up the boardroom agenda, there is uncertainty over some of the clauses within the legislation, leaving many organisations scrambling to ensure compliance.

Increased connectivity in the Internet of Things age is something else that keeps security professionals awake at night. We're all linking things like smart watches and bands, medical devices and our home appliances to the internet, leaving each one of us vulnerable to dangerous and widespread hack attacks. To mitigate against this ever-intensifying threat, it's more important than ever before that organisations can get in place the security personnel they need to help them batten down the hatches.

That said, it's very difficult to find the talent with the right expertise to meet these requirements. Looking to plug the gaps, employers must decide whether to upskill existing employees or invest in new recruits. In my own personal experience, I've often needed to fill positions short-term with contractors while searching for individuals with the right skills who can be employed on a more permanent basis.

There is a common perception that investing in security measures that prevent attacks is futile, fuelled by the knowledge that it's not a case of 'if' but 'when' hackers will strike. However, prevention must be the first step to protecting a business, if the organisation is to keep out as many unwanted threats as possible. Prevention in isolation is an insufficient defence against the contemporary threats that we see today. Organisations must maintain capabilities that prevent, detect and respond to cyber-attacks.

Mark Segelov, Information Security Director

One of the biggest security challenges facing businesses is ensuring that the security measures and processes employed balance the needs of the organisation with the requirement to protect sensitive information from continuously evolving threats. All too often security experts will be brought in who don't necessarily have the right skills and experience to understand the key business requirements, resulting in too much money being spent on a solution that is left underutilised and does not necessarily address the true risk.

A successful Chief Information Security Officer (CISO) isn't necessarily one with a big budget, but one that can show they are making a genuine difference in enabling the organisation to take advantage of the business opportunities available in the full knowledge of the risks being taken. Of course, people are in business to make money, and so any investments that are being made in security solutions must be seen to be securing genuine business benefit and not just improvement in the security measures employed. The board need to see demonstrable improvement for security functions to be given the continued support required to protect the organisation from any adverse security related event.

The tech industry is going through rapid expansion, and the breadth and depth of talent simply isn't there to meet the growing demand for skilled individuals who can propel organisations forward during this period of flux. To counter this, there must be an emphasis on nurturing existing employees. Don't focus on what they know, but whether they have the aptitude and mindset to learn new skills. Also, encourage junior members of staff to move around different departments so that they have exposure to new skillsets and experiences. Once they learn how to manage penetration testing for instance, they can get involved with incident management, stretching out to other lines of security including governance, policy and risk management, to broaden their knowledge base. Security professionals should also involve themselves in areas outside security to help learn one of the key attributes of empathy. The ability to understand the drivers of different individuals will enable a security professional to adapt their message to genuinely support others in achieving their objectives.

Security measures are often perceived as restricting the business from innovating and experimenting as it wants to. If you think about the brakes on a car, however, they're not there to slow the driver down but to enable them to move as quickly as they can in a safe way. Security measures should be viewed in the same way; as enabling the organisation to be as nimble and agile as possible, while ensuring critical assets, data and IP are appropriately protected.

Methodology

The statistics referenced in this report were obtained via an entity extractor provided by Innovantage, which scans and logs IT job postings across over 180 global job boards and in excess of half a million employer websites.

This information was then put through a normalisation process, where the data was matched to defined regions and types. Where roles were unsortable due to vague or foreign language job titles, they have been omitted.

This data was further sorted into disciplines, job types, sectors, and other categories to provide a detailed analysis of the current recruitment market. Instances where data was minimal or for regions where information was unavailable were not included.

Experis drew upon its years of IT talent industry experience to compile the detailed analysis of the recruitment market found in this report.

Special thanks to Ade McCormack, for his contribution to the 'Insights' section of this report.

Ade McCormack is a digital strategist and near futurist. He is a former technologist, FT opinion columnist, and CIO 100 judge, and has lectured at MIT Sloan on digital leadership. More of his strategic insights can be found via his blogs at www.ademccormack.com.

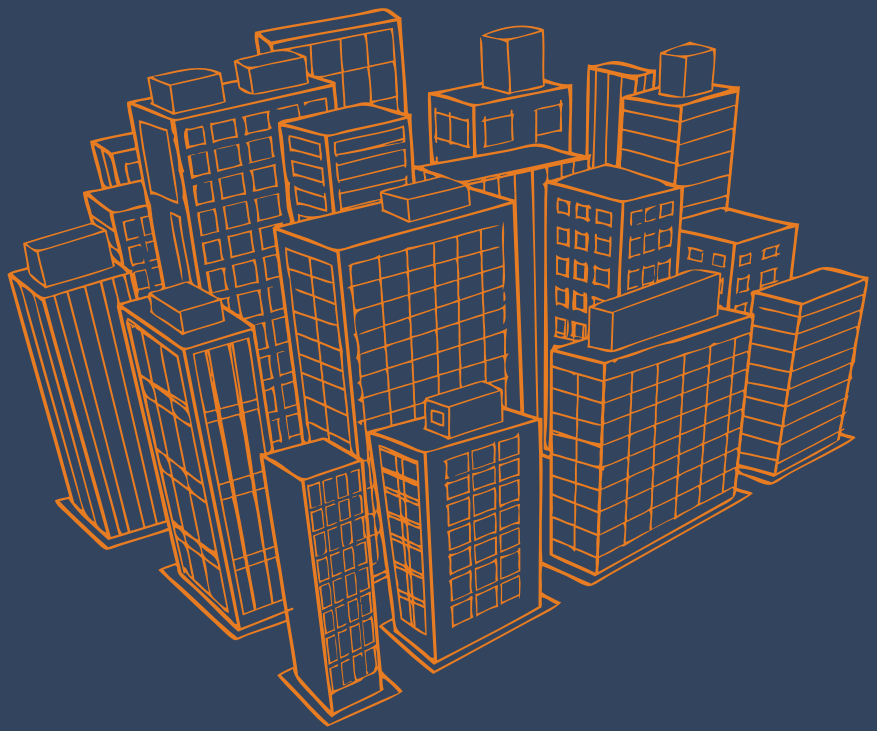
Get in touch

- Visit us at: **www.experis.co.uk**
- Email us at: **info@experis.co.uk**
- Call us on: **020 3122 0200**

twitter.com/ExperisUKIE

linkedin.com/company/experis-uk-&-ireland

facebook.com/ExperisUKIE



Experis™
ManpowerGroup