THE SALARY SURVEY
2018-2019

Written by Ryan Farmer and Martha Tonks
on behalf of Acumin Consulting

ACUMIN

www.acumin.co.uk
info@acumin.co.uk
020 3119 3333

CONTENTS

INTRODUCTION

Acumin Consulting's Salary Survey is an original salary reference resource within the cyber security industry, and is now more significant than ever as we celebrate our 20th year as a recruitment consultancy.

With our tenure comes a significant amount of experience managing career paths from infancy to executive leadership. Our annual report brings together analysis on salary bandings and packages compiled from the largest cyber specific candidate database in the UK, and our recruitment teams' knowledge and activity from the past 12 months.

Acumin have moulded our position within this industry from a commitment to providing a recruitment service on two values, speed and accuracy. It is our intention that this resource can be used for both professionals and hiring managers to a take a fair representation on the average salary per skillset unique to this industry for the UK.

We have taken a view of job titles applicable in End User, SI and Consultancies, Public Sector and Vendor organisations, showing career paths where applicable with representations of junior and senior roles.

As a marker of our anniversary within the industry, we have included a record amount of market analysis, taking apart our predictions from previous editions of salary surveys and providing insight to current market risks and developments.

From taking a view of the expected impact of Brexit on hiring, reviewing the effect of GDPR and attitudes towards breach disclosure our Salary Survey compiles insider knowledge from within our maturing, and much beloved industry.

LOOKING BACK - PREDICTIONS 2017-2018 >

This year as an industry, we have made significant inroads in gaining the attentions of boardrooms and the greater public. The news of cyber security breaches and the looming threat of GDPR, filled headlines across media outlets, catching the mealtime attention of the nation and bewitching half-dazed commuters. For years, those of us in the industry have implored friends, family, and colleagues to take warnings seriously, to not re-use passwords, and not to click every link that shows up in their inbox. It would seem that many have started to listen.

This is all indicative of one thing; the cyber security industry is maturing. Some 53% of companies consider a cyber attack as the biggest threat to their business[1] and similarly 58% of organisations increased their security budgets from the previous year[2]. No longer are CISOs the pauper feeding from the cast-offs of the IT table; their position in some instances now affords a seat on the board, or at least a seat in the room, and security is becoming embedded across the business.

C-suite buy-in is improving, government is investing, and the population understand the need (if not necessarily the how) to protect themselves online. We might not be anywhere near achieving cyber security utopia, but the silhouette on the horizon is starting to get closer.

It was against the ever-brightening backdrop that last year we continued the practice of making predictions in this report about what we expected to see in our industry over the following twelve months.

In hindsight some of these may now seem altogether too safe as forecasts, however that is the luxury that growing market maturity affords, it is less volatile and more easily read; patterns are more often a continuation than new, and technology becomes progressive rather than disruptive.

Conversely, some of our other predictions were perhaps a little pre-emptive in their timing, and again this can be attributed to growing market maturity with the pace of change settling to incremental rather than exponential.

CERTIFICATIONS >

"...the range and number of security-related certifications increase[d] exponentially in recent years, and though this is a sign of market maturity, as the industry continues to develop we might expect the need for these to diminish."

If anyone followed the debacle of courses and certifications made available in the build-up to the 25th May deadline for GDPR, they will know all too well the pitfalls involved with immature education offerings. We have progressed beyond this in security, but the sheer variety and quantity of courses and providers that remain is staggering, and it can be difficult for quality to stand out against the noise.

We have not seen the truncation in the market that we might have predicted just yet, and if anything have seen more general IT training providers enter the arena with their own security courses or reselling those from others. The compression is likely to eventually follow the high growth, but it seems that in terms of market maturity we are still a little way off.

Those courses and providers offering validation of skills and knowledge still have a role to provide in the market, not just in upskilling professionals but also in offering reassurance to those hiring them. That isn't to say we question the purpose of certifications such as CISSP, but merely challenge their presence as a requirement for entry level positions, and so their use as a crutch for organisations seeking security professionals.

The allure of education to potential employers focuses on both sides of the fence, and we have seen those who deliver such training to be in high-demand when available on the market; not for deployment in direct training roles but rather because of their ability to present clearly and succinctly to a range of expertise, and the recognition of knowledge that such a position suggests.

BREXIT >

"Key areas for cyber security that we might expect to see affected include the hiring of EU nationals and the attractiveness of the UK for companies as a base location".

The act of leaving the EU is unquestionably going to have an impact on the UK's economy and the composition of its workforce. Whilst work continues on determining what a post-Brexit agreement might contain, the uncertainty has seen the draw of the UK lose some of its lustre to European migrants.

Putting aside any mention of skills shortages in cyber security, the fact remains that EU nationals are on-the-whole better educated than those in the UK, "about 44% have some form of higher education compared with only 23% of the UK-born[3]". Regardless of your political views, it is difficult to argue that that isn't a substantial proportion of skilled and educated workers, which will still have some presence in the workforce but whose representation will be substantially diminished.

Far fewer migrants are arriving at UK terminals with the intention of living and working here. For the first time net immigration from Europe has fallen and that drop has been substantial with a decrease of around a third in the first year since the results of the referendum were announced[4]. Extrapolate that scenario further and in summer 2018 we find that number only continuing to fall, with an annual drop of 43%[5] in net migration from the EU; all this before any agreements have been reached around freedom of movement.

The UK currently represents the largest employer of cyber security personnel in the EU with 13% of the total workforce[6], so there is no doubt that it is an attractive place to focus your security capabilities, but this also highlights the inevitable dependence on European workers.

It may be that lack of certainty that is driving organisations and individuals to take action sooner instead of later, opting for proactivity rather than waiting for Theresa May's negotiations to bring clarity later in 2018 and the potential 'cliff edge' moment.

The financial services industry has been among the hardest hit by the fallout of Brexit already, with several organisation notably relocating out of the UK or at least downsizing their capacity here. This isn't purely to do with workforce availability but also the lack of clarity around post-Brexit arrangements and whether UK-based financial houses will still be able to provide their services freely within the EEA. Whilst Goldman Sachs have put their entire UK workforce on notice, HSBC have already committed to moving seven of their UK offices to France as well as switching these functions from their UK to their French entity.

The effects of Brexit are not unique to cyber security or indeed financial services, but they are a considerable factor that will only serve to fuel skills shortages further. As leaving the EU is a broader societal issue, so too is the general shortage of individuals undertaking STEM subjects in tertiary education. STEM businesses across the UK are impacted with as much as 89%[7] said to be experiencing skills shortages, cyber security is not atypical but rather symptomatic of a broader failure to attract a new generation in to the technical workforce. This compounds not only the number of professionals in security but also its ageing population, industry body (isc)[2] found that "only 12% of the cyber security workforce is under age 35... 53% of the workforce are over age 45"[8].

Inevitably the impact of Brexit will stretch far beyond a decreased working population and driving organisations to base themselves elsewhere. It has the potential to put businesses at risk as threat intelligence exchange and Europol collaboration may not be possible if agreements cannot be reached. Although in such an instance the UK will lose the benefit of shared European intelligence, the argument can be made that the loss of the Five Eyes signals intelligence link that the UK brings means the EU will feel the brunt of such collaborative agreements ending[9].

Another potential impact of Brexit could come around whether the EU grants the UK an adequacy decision for data protection and therefore allows it to process the personal data of EU citizens.

Whilst the DPA 2018 effectively mirrors GDPR in to law, there is concern that this might be used as a diplomatic bargaining tool or that the recent damning verdict of the UK government's mass surveillance programme by the European Court of Human Rights will prevent the adequacy being granted. The consequences of such a rejection would wreak havoc across British businesses, particularly those with a multinational presence, and the flux of data processing agreements would rival the May 2018 build-up to GDPR.

STANDARDS >

"Standards such as Sarbanes-Oxley and PCI-DSS have driven security adoption over the years, and the latest standard that will motivate best practice is of course GDPR".

Never have so many marketing databases simultaneously self-destructed. As the deadline for GDPR enforcement approached, a combination of panic, bad advice, and poor historical data capture practices sent organisations across the globe scrambling to re-opt prospects in to receiving their communications. Data protection became not only mainstream news but the subject of numerous memes across social media platforms as various corporations performed the email equivalent of courtship rituals to try and re-entice people back to their dwindling target lists.

Misconceptions abound and the sensationalism attached to "€20m fines" sent some organisations to take extreme measures; JD Wetherspoon deleted their entire email marketing database [10], and some media outlets have taken the approach of blocking EU citizens from accessing their websites altogether[11]. It would seem for many, that two years simply wasn't sufficient preparation time, despite the fact that those following the guidance of the Data Protection Act 1998 should have seen little in the way of change.

Although much of the furore has now settled, it is fair to expect some of the issues around data protection rights to resurface in the not-so-distant future as updated legislation comes in to replace the current version of Privacy and Electronic Communications Regulations (PECR), which conflict with some of the guidance and requirements of the GDPR.

There was certainly an increased number of data protection roles on the market, and many of the positions available in security requested an understanding of the new legislation, in reality the impact was less than many had thought. Responsible organisations with data protection maturity had embarked on their GDPR programmes in the years leading up to the deadline, so found themselves refining rather than defining as the 25th May deadline approached. Many of those seeking to paper over the cracks at the last moment chose not to hire and build functions but to engage charlatans and peddlers of snake oil; indeed some contractors in the space refused to engage new clients in the 6 month period leading to the enforcement deadline, as they knew that initiatives would be treated as a minimal tick box exercise as opposed to real meaningful improvement.

Whilst Europe (and some of the USA) were busying themselves with GDPR-readiness (and to a lesser extent the EU Network and Information Systems Directive, or NIS), across the Atlantic, the Americans were dealing with meeting the updated requirements of the NIST Cybersecurity Framework. Although unrecognised outside of its country of origin, NIST became a consideration for many organisations with an international presence and remit, even appearing as a requirement on the job specifications for a smattering of UK-based positions.

CYBER CRIME >

"...security teams and law enforcement struggle to keep up with the pace of change around emerging threats and vulnerabilities."

Whilst acting as Home Secretary in 2010, Theresa May proudly announced decreased crime rates as a back drop to cutting police budgets by 19% and as a consequence front line officers by more than 20,000[12]. Fast-forward 5 years to 2015 and we found cybercrime was finally being included in crime rate figures for the first time.

What we saw was cybercrime and digital fraud bucking the trend of what otherwise would have been a further 8% fall in overall rates had the combined 7.6m digital incidents not been included; with them factored in though we saw an effective doubling over 12 months[13]. Crime is not in demise, rather it has transitioned to become digital and like any growth industry with ever-improving technology, it is becoming cheaper and easier to practice.

This revelation about the volume of crime online came three years ago, yet we seem to be making no serious inroads in to tackling the issue. Indeed prosecutions have fallen year-on-year and in 2017 cybercrime convictions fell to 47 for the entire 12 months[14], representing a relative drop in the ocean. This decrease could be attributed to the classification of crimes (cyber-enabled vs cyber-dependent; digital fraud vs traditional fraud), to the increased scale and complexity of cyber attacks, ineffective and outdated legislation to prosecute against, or to the international cross-border nature of most attacks. Yet there is a general consensus that the UK Police Force is simply not ready and not being supported appropriately to pursue further prosecutions; the remedial measure of pressing already over-stressed and over-worked security professionals to volunteer as Special Constables, seems short-sighted and wholly insufficient. As of 2017, there were a reported 40 volunteers specialising in cyber security, by comparison there are around the same number of[15] police forces in the UK. Given the increasingly digital nature of the UK economy and the country's growing dependency on online services and ecommerce, essentially expecting the public to solve the problem is never going to produce any kind of sustainable strategy; it represents a major risk to UK industry and should be a primary focus of law enforcement.

MERGERS & ACQUISITIONS >

"...the contraction of the number of vendors operating in any such space is inevitable, and will be brought about by fire sale acquisitions, restructuring, and consolidation."

Venture capital funding and investment rounds featured heavily across the industry over the course of the previous year, and were accompanied by little in the way of IPO activity. This year effectively saw that position switched on its head. Decreased funding in to what had been new solution areas, came about as the market started to grow over-saturated with companies offering products in areas such as threat intelligence and next-gen anti-virus. The volume of these alongside the lofty expectations of investors created an environment of heightened commercial pressures. Inevitably organisations started to focus on maximising profits on current revenues, and the CEOs of smaller firms set about working toward exit strategies.

A number of IPOs across the year saw the likes of Zscaler, CarbonBlack, Okta, Tenable, and ForeScout all go public, reinforcing if there were any doubt that cyber security is big business. Those who floated were able to benefit from the buzz of and media spotlight afforded by such news, and provide early-stage staff considerable compensation as they were able to benefit from the various stock options and capital-based incentives taken up over the years. For employees in the vendor space, picking up additional benefits like this when working in a start-up represents a significant pull factor, it can be somewhat of a risk but could ultimately also prove to be lucrative. The real benefactors though of any flotation are majority shareholders and venture capitalist backers.

Perhaps not quite as eager to spend on their cyber portfolios, VCs were a little quieter than they have been in recent years, however this didn't prevent some considerable funding rounds for the likes of Cylance ($120m), Tanium

($175m and a further $200m), and CrowdStrike ($200m) in 2018. Meanwhile, private equity firm Thoma Bravo added LogRhythm and Centrify to its sizeable security investment portfolio which already included among it the likes of McAfee, Barracuda, and SailPoint.

This is perhaps indicative of a broader trend we saw in the vendor market, with organisations keen to be able to offer their customers a breadth of solutions. This meant companies attempted to develop new product solutions or acquire others in an effort to diversify their offerings. To that end we saw web app hosting power house Amazon Web Services (AWS) pick up security big data analytics tool Sqrrl[16] whose behavioural monitoring adds additional threat intelligence feeds to SIEM platforms; virtualisation specialists VMWare acquired public cloud security start-up CloudCorero[17] and in a move not dissimilar to AWS's, E8 Security who provide behavioural security analytics and intelligence[18]; and Oracle in an effort to improve its cloud and DNS capabilities picked up Zenedge, who specialise in bot and DDoS protection[19].

As the market has shifted and changed, many of the household names have been affected by disruptive solutions and rapidly growing start-ups. In some organisations that offer a broad suite of solutions we have seen attempts at streamlining propositions and business models. As such over the last year, two of the oldest and largest security vendors have gone through significant restructures with Symantec fresh off its sale of DigiCert looking to cut its workforce by 8%[20], and McAfee with its majority share recently acquired by venture capitalists making numerous layoffs across the business with unspecified numbers so far affected and no imminent end in sight. Other major players IBM and HP Enterprise (the hardware part, not DXC) have likewise made some redundancies across various parts of their businesses in an attempt to streamline operations, with the latter jettisoning 10% of its total workforce.

LOOKING BACK - WHAT HAPPENED 2017-2018 >

According to a recent industry report, 55% of large companies experienced a breach over the last year and of those, 30% dismissed an employee due to negligence associated with the incident[21]. With companies investing ever increasing amounts in to improving their security capabilities, we often find humans identified as the "weak link" in security. Although of course breaches do occur because of employee incompetence or malfeasance, to blame rather than train staff is unfair and reflective of a lazy approach to security awareness; it is indicative of the same blame-culture that often sees the finger pointed at the CISO in the wake of an incident, and a security model more akin to a house of cards than a fortress. Given the prevalence of technology in business, security teams must implement security and data loss controls that are more resilient and mitigate the vulnerabilities of human behaviour. As much as security awareness has matured across the populace, no longer can we operate in a way that allows millions of pounds of security investment to be circumnavigated by mistakes that are impossible to eliminate entirely. Breaches will happen, we know and accept this as an industry; it is about reducing the attack surface, segmenting systems to limit impact, and ensuring that even if data is lost it is appropriately protected (let's agree SHA-1 encryption doesn't count anymore) and data sets are sufficiently limited in scope. Not all incidents are avoidable, but with the average breach now estimated to cost a company £2.48m[22] , the need to ensure the lowest common denominator attacks don't get through should be the end-goal. As an industry we have a duty of care to the organisations that employ us but also to protect our colleagues who may eventually find themselves culpable for something well outside their own expertise. The human factor can never be totally mitigated as a risk but we must ensure that it is treated to the point that people are not losing their jobs through honest errors made in the performance of their daily tasks.

GOVERNMENT - STATE OF PLAY >

In 2018, something significant happened; offensive cyber units carried out attacks on behalf of the UK government. Spies being spies isn't exactly a new concept, but the move to undermine and neutralise Islamic State's digital recruitment and propaganda efforts was something of a watershed moment. In the US, CYBERCOM has been running such offensive cyber attacks for a couple of years now, but for GCHQ this was new ground, as Director, Jeremy Fleming revealed,

"This is the first time the UK has systematically and persistently degraded an adversary's online efforts as part of a wider military campaign."[23]

Buoyed by this success, GCHQ has recently announced the formation of a new cyber taskforce. This will see some 2,000 cyber roles created with the purpose of dealing with the digital threat of nation state actors. The wars of the future will be fought across holistic battlegrounds, with cyber an inevitable part of any conflicts. The ability to disrupt communications and critical national infrastructure in tandem with military efforts is obviously attractive as an effective method in enhancing the impact of physical strikes. The successful attacks on the Ukrainian power grid that preceded the annexing of Crimea in 2016 shows us first-hand how such methods can be combined to devastating effect.

Much of war has precedent, and international laws have been developed to prohibit some of the more horrendous tools used like cluster bombs and chemical weapons. That is not to say such things are not used, but that the global community has a line in the sand at which to take action; there are effectively an established and broadly understood set of protocols. Cyberwarfare is a relatively new construct and so such legislation does not exist. At what point is a cyber attack acceptable or not, when in attribution is retaliation acceptable, and how far is too far? Neutralising Iranian centrifuges used for the enrichment of uranium might draw universal applause (see Stuxnet), and no one is going to dispute the validity of undermining the digital presence of terrorist groups, but how do we define 'acceptable' in such instances?

Without clear and internationally agreed cyber rules of engagement we run the risk that atrocities could be carried out from behind a keyboard purely on the basis of subjective decision-making. Indeed this may not even be possible to define with so little known about the full extent of cyber arsenals and capabilities.

This summer, we saw a potential precursor to the future when Russian hackers gained remote control over a number of US power stations[24]. Nothing was damaged, no blackouts occurred, even though the access meant such attacks would have been possible. This was clearly an exercise in intelligence-gathering and in testing the attackers' ability to access air-gapped control systems that weren't connected to the internet; considering the perpetrators were operating undetected the consequences could have been very real. In a joint US-CERT alert statement, the FBI and DHS referred to the attacks as a "multi-stage intrusion campaign by Russian government cyber actors"[25].

The energy sector has not been the only area where efforts have been made by state actors to undermine western democracies, with the US elections having been tainted by tales of Russian interference. In 2016 there had been attacks on American political parties as well as state voter registration databases, the former of these incited by Donald Trump as he implored, "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing"[26]. It was later that day that the first attempt to access the emails of Hilary Clinton and the Democratic National Committee was made[27].

Whether attribution back to the Russian state is possible or not, that Russian-based actors were able to perform such attacks, coupled with the disparate and unpatched nature of electronic voting systems, a real risk of international interference in American elections is developing. It remains to be seen how such an attack might play out, whether it would involve registering votes for those who had not themselves voted, or if simply accessing such a machine would undermine and cause uncertainty in results. So weary are western governments of the potential impact of foreign state-backed cyber espionage that they have effectively embargoed

technology firms deemed to be too closely linked to their own regimes. Russian antimalware vendor Kaspersky found itself embroiled in arguments with both UK and US governments as the eponymous Eugene sought to distance himself from current links with the FSB, and his past at a KGB-feeder school and subsequent service in Russian military intelligence. Much of the suspicion and attention which befell Kaspersky came about as a NSA contractor inadvertently leaked sensitive hacking tools used by the agency from a home computer using the product, with the Department of Homeland Security recommending all government agencies avoid using the Russian vendor's technology on state-owned systems. Kaspersky Labs for their part dispute the version of events and there seems some uncertainty about what exactly happened, but there are two common themes, the NSA contractor did not follow suitable and secure processes, and the files were accessed by the Russian state from Kaspersky servers[28], either after a deliberate attempt or because the antivirus had detected a malicious zip file and uploaded it for closer inspection, depending on perspective. Off the back of all this, Kaspersky has made attempts to distant itself from the Russian regime, relocating much of its infrastructure to Switzerland and providing greater transparency about its operations.

Russian firms were not the only ones to find themselves falling foul of such treatment, Chinese telecommunications giants ZTE and Huawei were also subject to their own sanctions by the US for their purported collusion with their government. In August of this year, the Trump administration having scaled back initial outright bans on both, added their names to the National Defense Authorization Act, effectively preventing any government department or employee from using their products[29]. Indeed other Five Eyes nations, Australia[30] and the UK [3132], introduced similar guidance and embargos, despite the firms' involvement in commercially valuable 5G spectrum work in both countries.
With the aforementioned creation of 2000 roles as part of a strategic capability development, GCHQ is blazing the way for other government departments to follow.

With a number of large multi-year digitisation and transformation programmes taking place across several major government departments, it would seem there are likely to be a number of new security opportunities being created, although inevitably many of these will be on a contract basis and perhaps subject to IR35 restrictions.

MAJOR BREACHES- KEEPING COUNT >

The last year has seen a number of significant breaches; significant in scale, cost, impact, and legacy. Yet for all of these recent incidents, an old favourite from the archives continues to occupy column inches as 2018 was the year that Yahoo (now trading as Altaba) finally faced up to US regulators for the 2013 and 2014 breaches, receiving a fine of $35m[33] from the Securities and Exchange Commission (SEC). This was of course additional financial impact on top of the acquisition price reduction of $350m negotiated by Verizon[34] as a consequence of the breach and Yahoo's failure to identify and report it, and other costs normally associated with an incident such as the $16m in legal costs[35].

Of course no industry commentary covering the last 12 months can be complete without an obligatory reference to cryptocurrency or blockchain. A number of exchanges, mining operations, and high value wallets have been targeted with numerous tales of seven- and eight-figure sums being spirited away. The anonymous nature of cryptocurrencies coupled with their obvious high value and a lack of regulation associated with such immature markets, makes them particularly attractive to cybercriminals and heavily-sanctioned cash-strapped nation states (read: North Korea).

In terms of sheer size of security breaches that have taken place since the last time we released a salary report, the 'honour' is tightly conflicted between Maersk for the extent of impact on business operations, and the Indian government for the volume of data lost.

Scandinavian shipping giant A.P. Møller-Maersk was one of the organisations that was caught up in the spate of ransomware attacks that followed the WannaCry outbreak. The point of entry was exceptionally small, third party accounting software from M.E.Doc, a firm based in Ukraine, added to one device in its Odessa office[36]. Once inside Maersk's infrastructure, NotPetya was able to replicate itself extensively across tens of thousands of end points, utilising the EternalBlue vulnerability that Microsoft had recently issued patches for. The fallout saw cargo containers and freight ships stuck in docks across the globe as one of the world's largest logistics networks ground to a standstill. The recovery was impressive, but was reliant on the company's IT staff going above and beyond the call of duty to rebuild in excess of 40,000 endpoints and 4,000 servers in 10 days, rather than through any sense of cohesive corporate planning. Indeed as they raced to produce back-ups, most from within the previous week, it quickly became apparent that none existed for critical domain controllers that underpinned Maersk's disparate architecture. These were eventually found on an offline computer in the company's Ghana office, the data had remained intact by chance and after a staff relay across the globe, order could fortuitously be restored. With a financial impact thought to be in the region of $300m[37], the attack highlighted failures in patch management, digital resilience, and disaster recovery; despite annual revenues of $35bn the firm was caught unprepared and unprotected.

In 2009, India took a step in to the brave new world of biometric citizen databases tying essential services to it and effectively mandating over 1 billion people to enrol as it released the largest scheme of its kind. A vulnerability in the systems used by a state-owned utility company left data exposed for all 1.1bn members of Aadhaar, which included names, registration numbers, services used, and some banking details[38]. Despite being informed of the issue, the government essentially over-looked it for more than a month, and only took the data offline once ZDnet had published an exposé article. This is not the first such an incident reported around Aadhaar's APIs and applications leaking elements of the database, and given the intrinsic nature of the scheme to India it is unlikely to be the last.

became so bad at one point that Google had indexed large portions of the database as a number of government-run websites spilt information[39]. Large-scale programmes with such rich and verified data will always represent an attractive target, and the issues experienced with Aadhaar serve as a stark reminder of the perils of large and full data sets.

Although not on the same scale, a breach involving website MyHeritage emphasised the extent to which segregating data can protect it in the event of a breach. Despite the credentials of some 92m users being stolen, the data set contained only email addresses and hashed passwords, with payment card details and genealogy stored on separate servers and so remained un-accessed and uncompromised[40].

An organisation that wasn't so diligent about separating large data sets to their chagrin was credit-reference agency Equifax. Although this incident took place in time for the initial breach to appear in our report last year, much of the fallout has taken until now to play out. Boasting one of the largest private sector data sets ever to be lost, the company was forced to re-run the hackers' database queries to discover what they had lost[41]. It's no surprise then that Equifax's approach to security and disclosure has drawn scrutiny from regulators, consumers, and the press. Despite accusations of negligence, insider trading, and poor processes, the company was able to claim back $75m of the total (varying between $250-600m depending on your source) of breach-related damages from its insurers[42]. The incident also caught the attention of the ICO here in the UK as it transpired that a significant number of British nationals had been included in the breach. Despite the extent of personal data lost and the practices that pre- and proceeded the incident, the regulator was limited to pre-GDPR levels of fine and so hit the firm with the maximum £500,000 under past legislation[43]. With the combination of fines, small claims and class action, and reputational loss, some have argued that it could represent the costliest breach to hit the private sector[44]; disappointingly markets interest in Equifax seems unabated with the firm reporting record profits and share prices have effectively recovered[45].

Despite the claims around the financial impact to Equifax, and of course the personal data of the hundreds of millions of consumers that was lost, there has been a prolonged campaign of cyber attacks focused on universities, the scale of which arguably eclipses the hack experienced by the credit agency. A US investigation found that 320 universities, 144 of which were American-based, had been successfully targeted by Iranian hackers in attempts to steal academic research and intellectual property over a 5 year period[46]. Across the 31.5TB of data stolen was research and IP which has been given a total procurement value of $3.4bn. The nine individuals responsible have been broadly identified as belonging to an Iranian state-sponsored group with connections to the country's Islamic Revolutionary Guard Corps[47], despite the charges the collective seem to have continued their efforts in targeting educational institutions with a focus on attaining potentially valuable intellectual property. Many of the methods used in the sustained campaign focused on various forms of phishing to lead university employees to provide their login details via spoofed websites, and reinforces the moves that organisations have been making in recent years to improve user awareness and reduce insider threats.

There does seem to have been a lesson learned across industry from large-scale incidents such as these; we have seen increased demand from end user organisations with a global presence for those with skillsets in security hardening, cloud and endpoint/DLP security, and technical assurance to embed security throughout project lifecycles across the entirety of a business. Likewise we have seen an increased demand in those who are able to deliver user security education and awareness training to reduce the risk of people-based attack vectors such as phishing and social engineering; in the past such niche positions have been the reserve of enterprises but we are seeing increased demand for specialists in communicating security issues to non-technical audiences, as well as it becoming a more prominent aspect in information security management roles.

VULNERABILITY DISCLOSURE - PATCHY TUESDAY

A hobby for some, a stream of income for others (see: Anand Prakash); security research and bug bounty hunting can be profitable work, with some $23.5m paid out through HackerOne to December 2017 . Whilst many companies are grateful for responsible vulnerability reporting and disclosure, and offer rewards in return others refuse to provide such pay-outs. In 2017[48], Google paid out nearly $3m in bounty rewards[49], but they also operate their own security research group, Project Zero.

In a thinly-veiled PR move, Google having had its Play Store overlooked as a release platform by Epic Games, quickly set about providing its 'help' in detecting security issues with the Fortnite game on Android. With the game developer requesting 90 days before disclosure to allow users to update their Fortnite installer apk, Google followed its own process to the letter, waiting one week from the issuance of a fix before making what some may deem a somewhat gleeful public vulnerability disclosure [50]. Given that Epic required users to bypass standard Android security settings and activate the permission to install applications from unknown sources, there was always going to be a certain amount of scrutiny around the release. The practice has been criticised for the potential insecurity it could cause users, allowing malicious applications to be installed through the same permission, and leaving the device vulnerable to man-in-the-middle attacks.

As much as people enjoy playing battle royale games such as Fortnite and Playerunknown's Battlegrounds, discovering Epic's mistake was not Google Project Zero's most important disclosure over the last year. That was to be reserved for a discovery that would shake the IT world to its core. In January 2018, months after alerting manufacturers, Google's security researchers disclosed details of vulnerabilities affecting almost all processors manufactured by Intel, ARM, and AMD over the last two decades. Under pressure from shareholders for incremental improvements and fulfilling projections foretold under Moore's Law,

chip manufacturers started to look increasingly towards software-based measures to improve processing speeds, using principles such as speculative execution, out-of-order execution, and caching on CPUs. In the age-old battle of function and performance in conflict against security, this was one where the former had to eventually be sacrificed for the latter, with patches against Meltdown said by many to negatively impact microprocessor performance. Despite the trade-off, at least a fix was possible, with Spectre being purely hardware-related and therefore not truly patchable in the same way.

INCIDENT DISCLOSURE - HEARD IT ON THE GRAPEVINE >

Discussions around breach disclosures have been ongoing for years among security professionals; should firms be forced to announce breaches, what's an acceptable timeframe for a disclosure to occur, and what's the risk associated with disclosing a breach before the attack vector can be addressed. The onset of GDPR enforcement provided an answer to this dilemma, making a notification to regulators and affected individuals within 72 hours from the point of discovery.

The general consensus around disclosure is that it should be done responsibly and at the right time, not so soon that the organisation is opened up to further attack through the same methods, but not so long that those affected are at risk of compromise themselves. There is also a belief that in most instances disclosure will not be met with resentment or scorn from the public, and there is often an element of sympathy and good will to those who have fallen victim to a cyber attack.

These are not opinions shared by executives at serial courters of controversy, Uber, who in 2016 paid off hackers to the tune of $100,000 on the condition that they not disclose the breach to the public and delete all the information they obtained[51]. With 600,000 drivers, and 57 million users having been affected, the firm opted to bury the truth for over a year from regulators as well as those affected.

In reality the data set lost, although extensive in size was relatively limited and at least did not include payment card data. Undoubtedly the outrage caused at the cover up is far greater than it would have been in response to the initial incident, although perhaps the fine of $148m agreed as part of a settlement package which also included breach disclosure and corporate integrity commitments[52], will go some way to fostering a sense of justice.

Facebook, another organisation who are no strangers of their own to controversy, hit headlines in 2018 as details of their third party data sharing practices became public. Those who have experienced Facebook as a business user have been somewhat privy to the trove and variety of information that Facebook is able to group target audiences by, and perhaps it should not have come as a surprise when political consultancy Cambridge Analytica (CA) sought to use this data to provide insights in to political allegiances and influence voting intentions[53]. Following revelations from CA-employee turned whistleblower Christopher Wylie, it became apparent that the agency had been harvesting data from those who had taken a survey called 'thisisyourdigitallife' about political affiliations setup by a Cambridge University researcher (though not on behalf of the university); this included not only the data of those who completed it but of their connections too.

The scandal served as an interesting precursor to GDPR entering the public consciousness and raised the subjects of data privacy and protection as mainstream conversation topics, if anything Facebook have arguably done more in that regard than the new EU regulation. Many learned the valuable lesson about the monetisation of data within free services and the extent of the social network's data-sharing agreements. At every turn, Facebook and its founder Mark Zuckerberg have denied any intentional wrongdoing, played the role of victim, and declared relative ignorance about the nature of their own operations. The social network has taken to penning open letters to users about their use of data and other areas they have courted controversy in (also see: fake news, hate speech, and Facebook Live deaths) and taking up display adverts in public places,

making declarations such as 'Data misuse is not our friend'; the opportunities for defacement pretty much wrote themselves[54].

THIRD PARTY - BRING YOUR OWN BREACH >

Despite being implicit in their own scandal and therefore diminishing any hopes for public empathy, Facebook were also effectively victims of a third party incident. They were not alone in getting caught up as a result of others' malpractice, negligence, or straight up bad luck. This year we received further reminder (see: Cellebrite incident of January 2017) that those who provide cyber security solutions and services are not themselves immune to attack. In independent incidents, both Fox-IT and Deloitte came forward to announce that they had been breached and as a consequence small amounts of customer data had been compromised. Dutch firm Fox-IT, part of the NCC Group, demonstrated a calm and measured response which drew praise for its speed and transparency; proving to the aforementioned executives at the likes of Uber and Equifax, that being hacked doesn't necessarily need to result in a PR disaster.

Having clear incident response and disaster recovery plans in place can mitigate much of the damage that might be expected in the fallout of a breach. It is perhaps for this reason why we have seen an increased demand for digital resilience and disaster recovery professionals over the last year, as well as those helping to drive and improve incident handling and security operations processes, particularly in financial services and telecommunications.

One of the largest third party breaches in recent times saw access of data on effectively all of Sweden's citizens and some military information was revealed to unauthorised personnel in supplier IBM. Of particular concern was that some of the data was moved to servers in Serbia due to their government's close links with counterparts in Russia; Sweden has a strained relationship with the Russians who previously simulated carrying out nuclear strikes on their Nordic neighbours and frequently test sovereign boundaries by making incursions in to Swedish airspace and waters[55].

The issue came about through a lack of governance and alignment to legislative requirements, as such senior resignations took place within government including ministers for infrastructure and home affairs[56].

Often when a company has experienced a breach you will find them wheeling out terms such as "unavoidable", "sophisticated", and "unprecedented" to discuss the incident and distance themselves from blame. In the context of Magecart victims Ticketmaster, British Airways, and NewEgg some of this is true at least. Code insertions (of 8-20 lines only) made by the Magecart group in to ecommerce forms with the intention of hijacking payment card details, indicate bespoke attacks on third party suppliers and/or the companies directly, and the complexity was further highlighted by the fact stolen data was transmitted in an encrypted state and with the use of a Comodo security certificate to avoid triggering alerts[57]. With those responsible still at large and likely to run more attacks, the industry has received a reminder of the importance of third party assurance and web application security; Ticketmaster were breached through a customer support tool, British Airways lost 380,000 card details in an attack that lasted 15 days[58], and retailers Stein Mart and Title Nine have been hacked through analytics upplier Annex Cloud[59].

LOOKING FORWARD - PREDICTIONS 2018-2019

In considering what we are likely to see unfold in our industry over the coming year, there are of course the unavoidable and inevitable areas that have been and will continue to be topics of concern, the conversation around skills shortages and diversity issues will not be leaving us any time soon. Nor should they, despite their obviousness, these are problems.

Cyber security always has an inane ability to shock us, and 2019 (and the remainder of 2018) will certainly be no different. We will learn of multinational organisations with impressively underwhelming security controls, nation states will continue to probe each other's cyber readiness, and someone is going to get hauled over hot coals by the ICO to the soundtrack of record-breaking fines.

SKILLS SHORTAGE – MEAT MARKET

"Easy access to offensive cyber capabilities, such as ransomware or DDoS, has allowed individuals and groups to have an impact disproportionate to their technical skill."[60]

Although from last year's version of the NCA and NCSC's joint report on the risks and impact of cyber attacks to the UK, the assertion remains starkly true. Upskilling as a cybercriminal is depressingly quicker and strewn with fewer barriers to entry than breaking in to cyber security. What's more, little in the way of skill base is required to operate many of the exploits and attacks that are prevalent across hacker communities, getting started as a script kiddie is easier than it ever has been with many tools featuring extensive guides or straightforward GUI controls. For all the schemes, funds, and noise, we are not making sufficient progress quickly enough by comparison in bringing new talent in to the industry. Many of the issues are of our own making, the necessity for now is unrelenting, and we repeat the mistakes of the past more often than we should

Many recruiters don't help matters, and nowadays there are so very many of them working the security market. At their worst, they pariah clients and regale candidates with toxic tales of woefully insufficient packages; they struggle to keyword match loosely defined industry buzzwords rather than resourcing capabilities; and claim expertise when they're three months in to their careers. The cyber security skills shortage is gold to the recruitment industry, and like the noisiest of magpies they are drawn to its lustre; perpetuating the myth for as long as they can milk the cattle, before moving on to cryptocurrency, blockchain, or whatever kind of virtual/augmented/digital reality sounds like it might sell well next.

Do not believe tales of 0% unemployment, no matter how credible the source; at any given time we can speak to a number of competent and experienced security professionals who find themselves out of work. As an industry our problem is indicative of, but not made of, a skills shortage. Rather the problem is a hiring shortage.

There are obstacles and patterns of behaviour that prevent us from being able to hire effectively. These are broad and disparate in origin, and worthy of a report in their own right. Issues arise through multiple sources and reinforce the argument for risk assessing your hiring process for security roles. Engagement with line management throughout the recruitment process helps to ensure screening is effective and accurate, while fostering engagement with potential hires. With the market particularly competitive for permanent employees, factors such as speed-to-offer and engaging candidates with the security roadmap, can become decisive. A well-defined role with a vision for the medium-term is an essential part of attracting and retaining security professionals. Given the importance of the industry and the responsibility attached that comes with the job, it is only right that we understand the situation, strategy, and commitment of any employer.

GENDER GAP – UNEQUAL PAY FOR EQUAL WORK >

The good news is that we're headed in the right direction, the percentage of women in the cyber security workforce is up from 11% in 2013, to 20% some 5 years later[61]; the bad news is there is still a long way to go, and we are not doing enough to be inclusive as an industry.

Through a lack of gender diversity we limit the development of the industry as a profession and undermine it if we cannot make proper progress in equality. Cyber security has its problems, many of which are not unique and are indicative of underlying societal issues, yet the responsibility is ours and only we can create fair, representative, and inclusive environments and communities; no matter how unpleasant the reflection, it is vital we look in to the mirror and hold ourselves to account.

That tales of sexual indiscretions and inappropriate behaviours can reverberate around major industry events in 2018 is not just utterly unacceptable, it's abhorrent. In a society unfolding the narrative of the #MeToo movement, it seems that many remain entrenched in lascivious conduct, hard-wired objectification, and an inherent propensity for outmoded innuendo.

As an industry, if we cannot overcome this imbalance we risk not only driving away those already in industry, but also deterring the next generation of female cyber security professionals. And rightly so. If we cannot facilitate safe working environments for all then we are not representative of the societies we strive to protect.

Women are traditionally under-represented in STEM subjects in education and IT is no different, in America which would perceivably be among the more progressive societies we could consider, only 27% of students enrolling to study a Computer science degree are female, with this falling to only 18% to the point of graduation[62]. This may be a snapshot in the broader context, but given that then fewer may be tempted to follow this vocation in to working life, the problem of diminishing returns at every juncture becomes apparent.

Between a combination of factors like STEM stereotypes, pay gaps, and discrimination in the workforce, it is no surprise that we are failing women as an industry and a society.

In security we are fortunate that we have, broadly speaking, acknowledged there is a problem; and with the aforementioned skills shortage, we have the motivation (should further be needed) by which to overcome it. There are already a number of excellent membership organisations and groups discussing about and campaigning for equality, and to increase the numbers of women entering the profession. It is imperative that these are treated as mainstream rather than fringe movements, that men heed the concerns and advice raised, and that women are given an appropriate forum through which to launch diversity efforts. Yet this is not something that women should have to solve alone for men are the root of many of the causes, and so a shift akin to cognitive reprogramming is almost necessary in some instances. We must champion equality; be brave in calling out discriminatory and toxic behaviours no matter how innocuous they may seem; and take measures in our own teams and organisations to ensure both genders are hired, developed, treated, and rewarded as equals. It might take a legal change like the one made in Finland, indoctrinating equal gender pay in law, but we cannot wait idly for such a moment of societal change, we must be the change.

BREXIT – THERESA MAY PRESENTS 'DEAL OR NO DEAL' >

At this point we are still waiting to see what the UK's divorce settlement from the EU might entail. On one hand we may achieve an agreement that allows for free trade and movement of labour, conversely we may find ourselves at a point where no legislation is in place to facilitate any trade or movement of labour at all. In reality despite talks of cliff edges and mass exodus of migrants, we can fairly reasonably presume that EU nationals living and working in the UK will be protected and able to continue doing so.

One area that is very much likely to present itself as an issue is the movement of data rather than people. In the past, the EU has been accused of utilising data protection adequacy determinations as a negotiation tool, and so New Zealand have one (see also Jersey, Guernsey, and the Isle of Man) while Australia do not, despite both providing effective data protection legislation and meeting the requisites around human rights. Recent guidance issued by the ICO around the matter suggests that the processing of personal data might be one such cliff edge moment in the event of "no deal" being reached, with the EU effectively refusing to begin the process or preliminary discussions until the point that that UK becomes a third nation (i.e. not in the EEA)[63].

So does that mean that come March 2019 that UK businesses will no longer be able to process personal data of EU nationals; in a word 'no'. It does mean however that companies will have to mirror GDPR in to standard contractual clauses and may be required to appoint representatives overseas in the EU. In the event of no deal being reached, UK-based DPOs and data controllers are going to find themselves as busy as they were in the build up to 25th May.

In the long-term the consideration is more likely to be whether the UK remains an attractive destination for European professionals and if trade agreements will remain commercially attractive enough to continue to draw organisations to base themselves here. Deal or not, new agreements and legislation will come eventually, so any worse case scenario is likely to be temporary. The UK will continue to host international companies, and we will (for now) continue to be Europe's biggest data market (second only to the US globally)[64] and many data centre operations will remain based here. In a logical world, security teams should typically be based where the data is and you would expect companies to continue to use the infrastructure and personnel they have invested in where possible.

STATE COMMITMENT – SIGNING UP FOR THE RACE >

Entering the latter stages of 2018, we find ourselves in a rapidly developing cyber arms race. Much like the aspirations for armament of the Cold War, we find many of the same players involved now. Cyber has already become an integral part of intelligence gathering operations and governments are keen to develop their offensive capabilities alongside protective ones. The £1.9bn commitment to the National Cyber Security Strategy and GCHQ's recent announcement outlines the UK's desire to be at the forefront of the digital world. Over the last 12 months Acumin have experienced substantially increased demand from the public sector as part of government security transformation programmes to support digitisation initiatives across multiple departments.

As global cyber capabilities grow, digital frontlines will become increasingly common. Given the scale of impact attacks on critical infrastructure could have for civilians, there is likely to come a point where internationally-agreed rules of engagement are required, which might forbid certain targets and ban specific methodologies or tools.

Part of a holistic government approach to protecting businesses and citizens online must include investment in law enforcement. The police are simply not being supported to process and investigate the massive influx of cybercrime and digital fraud cases, a strategy reliant on volunteers is not capable of scaling to the extent required or providing a long-term solution. Additional funding must be made available sooner rather than later to ensure crimes can be reported and investigated properly, and annual prosecutions improve past their current levels.

DIGITAL DEMOCRACY – POLITICAL HACKS >

Electronic voting machines are becoming increasingly prevalent as governments seek to move the process of democracy in to the twenty-first century. With over a dozen countries having introduced EVMs or online voting, some doing so permanently and others on a pilot basis, the security of such systems has come under close scrutiny.

Given this it is no surprise that they wold become an object of focus for DefCon, with the 2017 event featuring a whole section providing attendees with the opportunity to try and compromise a variety of machines; security was found universally lacking[65] with the protective measures on some devices falling over in minutes.

Adoption means that a sufficient percentage of the electorate in some regions or nations will be using digital means of voting; that they could strongly influence the outcome. If the security and privacy of these votes is undermined then so too could be the results. Such systems due to their high profile nature would require substantial investment in protective measures, and so the merits of introducing them in the first instance must be justified. If it becomes a mainstream option for UK voters then public scrutiny will dictate an investment in infrastructure and staff, creating further employment for security and privacy professionals in the public sector.

A high profile incident or controversial outcome as a result of electronic voting in the coming years will lead to other countries either abandoning such projects or investing in them to ensure they are not easily compromised. The ongoing entanglement of life with technology means digitising electoral systems will be a logical move for many governments despite the risks associated, further reinforcing the role cyber security plays in protecting society.

RECRUITMENT CHALLENGES

As one of the oldest UK service providers to this industry, it is important in this report to reflect on the activity within recruitment services and their impact on the organisations they support.

Whilst we are all mostly aware of the major events that have occured in the cyber security industry over the past 12 months, pressures on the labour market and the mobility of labour are also important to cover.

The skills gap is of course, the biggest influence at play here - but how internal HR functions and external recruitment service providers manage this can still make all the difference in the impact of the gap in the upcoming years.

How we hire, and the skills we are looking for are all processes that are increasingly being looked at from a recruitment industry perspective, and HR and recruitment functions will certainly have to undergo innovations to remain responsive to organisational and societal expectations of fair human resource management.

CLUTTERING

The amount of recruitment agencies acting within the market has grown, and the competition for the top spot increasingly ruled by marketing budget, not reputation for effective delivery within the market.

Recruitment agencies choosing to add cyber security to their tagline do so with considerable risk, but greater opportunity for reward. Cyber Security professionals are set to be some of the most affluent contributors to our society, with a REED report naming 'security architects' within the top 10 highest paid jobs[66].

Whilst this increases the choice for clients looking to employ a recruitment service, it does not necessarily correlate to quality of service improvements. Recruiters acting without a base level of understanding on the nuances between individual job titles and how role specs differ between organisation type and size risk creating white water in an already limited fishing pond. We often hear of how candidates within our own network have been contacted by multiple agencies about a specific role.

In this case, recruitment firms with the right background are able to pull ahead in securing the best talent, but for those organisations relatively green to hiring cyber staff knowing which agency to engage with is challenging. On one agency search website, there were over 300 recruitment agencies able to support IT security role requirements[67].

Some resources are slightly more comprehensive in assessing those with the right credentials, such as this list from Cyber Security Ventures that lists the top search firms globally with cyber experience – nicely naming Acumin 3rd, and the top of the list from Europe [68].

It is likely that the amount of recruiters in the market will increase further in the next few years, and demand in the industry very unlikely to die of for the long term. Those looking to instruct an agency need to consider due diligence before engaging, understanding current client lists and recent placements is a good place to start.

DIVERSITY >

As we mentioned in the context of gender earlier, diversity within the STEM industries is increasing, slowly. Over recent years education directives to try and help the gender imbalance on the uptake of certain subjects have increased, and schools are now engaging with more and more tech based skills development initiatives.

In solving the immediate issue of a lack of diversity within UK cyber security teams, and globally for that matter, we are still woefully behind. Whilst groups supporting women within this sector thankfully keep rising, inclusivity efforts supporting other minorites are not gaining as much traction in the sector.

Diversity ought to be addressed on several fronts; not least in engaging minorities to take up posts, promoting inclusivity and safe networking environments for minority professionals, and contributing to a diversity and inclusivity agenda on a wider corporate level. This is not a challenge that the cyber security industry should be addressing alone, it is an economy issue affecting most organisations to some degree. Hiring managers can work to overcome this by working in harmony with HR and marketing teams to ensure that the right message is being sent out to attract people from various backgrounds.

Diversity is coming more and more into the fore of the industry event circuit, with multiple talks and content being released on the issue. If the predictions about the imposing skills deficit are true, it's imperative to look outside what the culture of staff has organically developed to be. Diversity is challenging, because it is not necessarily born out of intentional exclusivity. Hiring managers need to be especially careful of overcompensating too quickly, and becoming guilty of positive discrimination in a bid to appear as an ally to diversity strategies.

CAREER CHANGES >

As demand for cyber security staff grows, professionals from other disciplines are increasingly beginning to see the benefit in migrating across to IT security.

Take the advent of GDPR as a recent example, non-technical candidates can see an opportunity to within reason, easily upskill on new legislation and look for a new role within wider corporate compliance and security. Technical security can be daunting to try and

attempt an entry into, knowledge of complex languages and systems is required for the most part.

Equally, more general IT staff may be inclined to make the jump into IT security, taking a strain on organisations if too many employees make the jump from NOC to internal (or another organisation's) SOC. In this case individuals may have more suitable skills to help bridge the talent gap.

With money comes popularity in most cases, and employers need to understand ways in which they can support increasing supply of non-specific staff looking for cyber roles.

As we mentioned earlier, recruiters in some cases don't help this issue both internally or in an agency context. Understanding someone's true skill-set and ability to do the role required of them when referring to complex job specs littered with buzzwords. Those intending to make a move into cyber security should do so with complete transparency of direct experience, and employers should be grateful of the opportunity to mould individuals with the right aptitude in the skills required for their organisation.

There should be a subsequent industry discussion on how we need to be driving for the highly demanded skill sets and what alternative backgrounds would be considered applicable. The responsibility for recruitment marketing should not be exclusively down to the organisation, for security purposes. And maybe there is room in the future for recruitment partners or other agencies to have a role in driving interest into cyber security as a profession from the available labour market.

MARKET SPECIFIC CHALLENGES

This final secion of the report addresses some of the sector unique recruitment challenges affecting our industry.

Every organisation has its pressures and demand generators impacting their recruitment efforts, but this is nothing comparitive to situational factors effecting verticals or sectors. At Acumin, we split the market into four key sectors:

- End Users (Banks, Telco's, retailers, utilities etc)
- SI's and Consultancies,
- Vendors
- Public Sector (both local authorities and central departments)

We have referred to our own recruitment consultants responsible for leading services to each of these areas their direct experience of, and learned market intelligence of factors effecting recruitment. Despite all these areas being somewhat dependant on each other, there are many different motivators between organisations and their role in the cyber security industry - and how they deal with human resource represents those differences (not least in the skills sets they recruit for).

END USER >

There is no need to pretend as if cyber security is a junior issue to the board now, but the ways in which organisations respond to risk differs massively. The threats organisations face are constant and evolving, and understanding the ways in which criminals approach and exploit network vulnerabilities requires in most cases, unrealistic and exponential amounts of resource. How successfully companies manage these

risks varies greatly, causing inconsistencies in best practice processes both internally and more widely throughout the industry.

A major influence on the success rate of mitigating risks comes from the allocation of specialist staff active within the organisation. Every company has its own unique challenges that a standardised first aid kit will not heal. The ways in which organisations approach hiring in order to prevent cyber crime often doesn't match up to market realities however. The skills gap is extremely prevalent and at no risk of changing for the better in the upcoming years. Competition for experienced candidates leaves some organisations high and dry, and this is only set to worsen.

Candidates understand the upper hand they have when it comes to negotiations whilst job hunting, and salary expectations are continuing to rise (if not plateauing slightly from the recent few years of super charged growth we've noticed). This puts particular strain on medium sized organisations and larger organisations acting in the charity and third sector, who may not have the budget for decent staff, nor the budget to offer a candidate to effectively manage the business's cyber security requirements. Over the next few years we can expect to see certain verticals fall foul to cyber crime as they fail to up the budgets for cyber.

GDPR has also created less of a splash in terms of end user recruitment strategies as expected, as the ways in which the legislation is managed is company specific. As GDPR can be managed by differing company silos including compliance, security or legal depending on resource/ need. Security teams need to ensure GDPR remains on the radar of the exec board for the years to come, and for it to be firmly part of corporate governance processes in order to mitigate risks of breaches. GDPR also offers an opportunity for non-technical professionals, internal schemes to promote within to ensure the legislature is being well managed within organisations has allowed for more exposure to security and compliance processes. Multiple training courses available on the market also create an upskilling momentum in other areas of the business who handle sensitive data, such as HR and marketing. This in turn slowly can nurture better internal cultures of security within organisations, a benefit for the cyber security professionals active within these end user organisations.

So whilst there hasn't been as much demand for extra GRC professionals in the market as perhaps expected at this point last year, we can hope that at least some organisations are taking other strategies to improve data handling at an individual level.

SI AND CONSULTANCIES >

The factors effecting Systems Integrators (SI's) and Consultancies have not vastly developed from our findings reported in last year's survey.

An expectation that brand value is a significant factor in recruitment efforts for the Big 4 still stands, and isn't likely to change unless a major incident unfolds. Large consultancy companies consistently value roles below the market rate, but working for such an organisation is not doubt a great 'cv builder' for candidates actively searching for work. For as long as corporate reputation is intact, these organisations are set to dominate the market both in business and in candidate attraction.

Consultancies are also beneficial to the wider cyber security industry, as one of the only verticals consistently offering entry level and graduate opportunities. The ability and proclivity of these organisations to retain these candidates depends on something quite separate to capability of the candidate. However, this is arguably well understood, with graduate schemes in particular still prioritising nature over core competencies, most likely under the logic that you can teach processes but not internal drive.

Like so many professionals within this sector working for consultancy organisations, career success depends on durability of nature as much as it does on technical ability. Consultancy work

provides great variety and autonomy, but with that also an increased risk of pressure and stress. Burnout is still a factor effecting consultancy staff, like so many professionals in different industries. Statistics of consultancy workers migrating to end user organisations would be interesting to see, but there is no question for some consultancy workers the increase in pay alone is a big driver in shifting career paths.

Service-led propositions have been a particular growth area, with consultancies and SIs looking to further develop their offerings, while vendors have also looked to add value through the development of managed services. Indeed, many of the disruptive vendors providing solutions around areas such as threat intelligence, seem to be as reliant and focussed on services as they do product. This is further echoed by traditional service providers making strategic acquisitions in order to individualise their offerings and demonstrate differentiators, one only need look at the investment made by the likes of BAE Systems in creating a product-set to piggyback services on. The rapid development of the security industry, confounded by staff shortages, has seen end user organisations increasingly look to take on professional and managed services to act as stop-gap measures in addressing such shortfalls. As such the EMEA market is currently highly attractive for organisations looking to grow their service footprint across the territory. We have seen a number of efforts to land and expand here from US-headquartered consultancies which have been driven through acquisition of smaller local consultancy capabilities over the last decade. More recently, antimalware vendor F-Secure doubled down on the services market with its acquisition of MWR InfoSecurity, and cloud MSP Six Degrees entered the security market by picking up CNS Group. These represent a fairly safe strategy in that the customer-base, brand, partnerships, and delivery model is already established, however these existing structures can also prove limiting.

In 2018, we saw announcements about ambitious investment and growth plans from US-based firm Optiv, who have already made significant inroads in developing their presence in Europe; this approach to organic growth, is not only encouraging for the future scale and quality of security service providers but also positively disruptive in much the same way next-gen antivirus has caused the established players in that space to adapt and improve.

The presence of large American companies and the investment they bring with them in local infrastructure and personnel can only help to mature the industry and improve the services offered to end users, as well as ensuring that solutions are best-of-breed and competitively priced.

PUBLIC SECTOR >

The UK Public sector has a lot to compete with from the private sector if its intention is to secure the best talent. With salary bandings greatly limiting the buying power of some government departments, demand is easily outstripping supply. Permanent vacancies are open, in a few cases for years before a suitable candidate signs on the dotted line. Existing cyber security teams are not at fault here, the way in which government group salaries in terms of contribution versus remuneration means that salaries are far below market rate.

This leaves hiring managers with two options in how to manage talent requirements internally.

First, roles are more likely to be filled on a contract basis, where daily rates can be better matched to industry averages. Hiring on a contract basis is great because it gives departments the flexibility they need - paying for requirements rather than position. However, contract rates are by far inflated to what the department would normally pay, and departments are not upskilling for the long term. Critical information is also at risk of being lost from within the department, if there is a high turnover of individuals doing contract work in expense of a single permanent role.

The second option is to continue the attempt for hiring individuals on a permanent basis, but having to requalify the essentials of the job description to match on salary, rather than internal need. Senior cyber security positions within the public sector are paid less, but

especially as the budgets they would be working with is also constrained. In the case for having to do more for less, employers will always struggle to find the top of the talent pool willing to take the challenge on. This then means, that department hiring managers have to consider hiring for ability and not experience. Providing a promotion opportunity for the new hire, means that they may find people within budget. This certainly helps the upskilling of the labour market in the long term.

Career hungry cyber security professionals have the opportunity to work for complex organisations, but departments need to consider the risks associated with this approach.

VENDORS >

The market is busier than ever before with billions of dollars of VC funding being invested into new companies aiming to solve an increasingly complex and damaging level of threats. Often these solutions require significant technical knowledge, especially when starting in a new region which has resulted in demand for high performing sales engineers and new business enterprise sales outweighing supply.

Traditionally start-ups would hire entrepreneurially minded SE's and EAM's from larger vendors offering higher salaries and equity options to counteract the increased risk moving to a smaller company. Over the past 12 months we have seen more established businesses significantly increasing packages to retain technical sales staff, due to the shortage of talent in this area.

The volume of new market entries and start ups has meant an increasing number are unsuccessful, particularly with unrealistic revenue demands placed on a new region, which results in an increasing number of short tenures on CV's. We are however now seeing a growing number of start-up vendors IPO or get acquired which proves that the reward is still there, but the risk is higher.

SALARY SURVEY DATA

Now, to the numbers. Acumin pull this data together from quantitive and qualitative research reviewing our own network and expansive database. We bring in our recruitment consultants to review and bring insight into realistic salary packages based on the extensive client experience they have.

The intention, is that clients can use this data to set realistic salaries for roles they are working on, or forecasting a need for in the upcoming 12 months. We also hope that this data can be used as a educational resource and to help candidates manage their own expectations for this position in the market.

It's important to mention that salary is just one part of the equation.

With unprecedented levels of competitive tension in the market place organisations are becoming increasingly creative with the over-all make up of their salary and benefits packages.

For example, large sign-on or guaranteed bonuses, commission guarantees and generous car allowances are the norm, especially in commercial roles. Equity participation for more senior level positions is especially common in high growth and earlier stage ventures. These are on top of the standard benefits such as pension, health and medical benefits, however companies are even looking at innovative ways to make these more generous and flexible to suit individual's needs. Remote working and flexible hours are also being offered very much as a benefit.

KEY:

EU This role is available in End User firms
SI This role is available in SI& Consultancies
PS This role is available in the Public Sector
V This role is available in Vendor businesses

£XX -£XXk This is the permanent salary rate. (OTE shown in most cases)

£XXX £XXX a day This is the contract rate shown.

This shows the mean average of the salary range has remained static over the past 12 months.

This shows the average salary value for the role has fallen. A % will demonstrate the extent.

This shows the average salary value for the role has increased. A % will demonstrate the extent.

Security and Risk Management

Risk Management roles are vital for organisations to keep control of the threats upon them, and roles within organisations heavily depend on factors such as size of company, teams and the sector in which the company sits.

Information Security Officer

Contributes towards and implements information security and risk management systems, including standards, policies, procedures, and controls guidelines.

EU/SI/PS

1.5%

£55-£80k

£400 £550 a day

Security Project Management

Coordinates project teams, manages budget, and allocates resources across all security initiatives and any projects throughout the business where security is a concern.

EU/SI/PS

£75-£95k

£500-£750 a day

Security and Risk Consultant

A broad business-facing role with internal stakeholder engagement. Conducts assessments around security and risk to identify gaps and make recommendations for remediation.

EU/SI/PS

6.7%

£60-£90k

£500-£700 a day

Security Analyst

Focussed around the operational use of information security controls that support the execution of the ISMS.

EU/PS

13%

£45-£70k

£350-£500 a day

Information Security and Risk Manager

Within a small organisation often the leader for security, setting strategy and implementing it. As part of an enterprise team, owns the ISMS and often security risk register. The salary of this role is heavily dependent on the size of the organisation, the range can be higher.

EU/PS

6%

£70-£100k

£500-£700 a day

Awareness Manager

Separated as a role in organisations with larger user bases typically. Responsible for designing and rolling out a security education, user awareness programme, and materials.

EU

20%

£60-£90k

£325-£550 a day

BISO

The BISO is a blended executive title, and comprises of ensuring that security is embedded into business practices, and that security and business needs are aligned.

EU/SI

£70-£100k

£500-£700 a day

CISO

The CISO is a broad job title, reflected in the variance in salaries on offer. Can be a managerial, executive leadership or board level role.

EU/SI

10.5%

£125-£400k

£800-£2000 a day

Regulatory

Regulatory roles are necessary functions, the responsibilities of professionals is mainly targeted towards governing and setting compliance processes and procedures on behalf of the organisation. Seniority can depend upon amount of experience and the types of certifications candidates possess.

Risk and Compliance Auditor

Typically focussed around conducting audits and gap analysis to ensure the as-is state aligns with frameworks, standards, policies and procedures.

EU/SI/PS

8%

£50-£75k

£450-£510 a day

Governance and Compliance Manager

Responsible for ensuring the ongoing compliance and effectiveness of the business in regards to information security and risk management.

EU/PS

6.5%

£65-£100k

£450-£650 a day

Security and Policy Assurance

Provides consultancy to internal projects and stakeholders across the business to identify, mitigate and accept information security risks, and embed security controls as appropriate.

EU/PS

3%

£65-£95k

£450-£700 a day

PCI - QSA

Accredited by the Payments Security Council to assess and advise an organisation on the effectiveness of their handling of payment card data against 12 key control requirements.

SI

7%

£55-£85k

ISO27001 Lead Auditor

Conducts audits for the ISMS against the requirements for compliance or certification towards ISO27001. Coverage will include risk assessments, business continuity, and effectiveness of continous improvement plans.

EU/SI

18.5%

£65-£90k

£450-£575 a day

Data Protection Officer

Independent internal adviser ensuring compliance to data protection and privacy legislation.

EU/PS

10%

£50-£95k

£550 a day

CESG Certified Professional

SC or DV cleared individual who assesses public sector bodies against the requirements of government accreditations. Work can range from RMADS to ISMS to high level security architecture.

EU/SI/PS/V

13%

£75-£95k

£500-£750 a day

Penetration Testing/Intelligence

Finding vulnerabilities and gathering intelligence is a career path that appeals to many within the realms of information security. The penetration testing market is highly competitive and roles are varied in both the end user and supplier side. Penetration tester salaries vary significantly depending on the complexity and depth of experience.

Infrastructure Penetration Tester

Conducts ethical hacking against an organisation in order to identify weaknesses in network security infrastructure and will often put forward recommendations for improvement.

EU/SI

4%

£40-£90k

£400-£650 a day

Application Penetration Tester

Performs ethical hacks against applications and associated architecture (e.g. web app servers) to identify gaps in security measures. Also concerned with secure coding practices.

EU/SI/V

7%

£45-£110k

£450-£700 a day

CHECK Team Member

Security-cleared and certified hands-on penetration and vulnerability tester within a CHECK Scheme organisation.

SI

£50-£85k

CHECK Team Leader

Senior-level penetration tester who will act as a manager and mentor of CHECK Team Members. Employment of a CTM is essential to maintain CHECK Scheme Green Light status.

SI

£85-£120k

Threat and Vulnerability Manager

Technical and analytical management role responsible for overseeing the company's threat research and intelligence, inputting in to service design, and ensuring timely vulnerability detection and mitigation.

EU/SI

6%

£75-£95k

£450-£625 a day

Security Analytics/ Data Scientist

Close analysis of data generated by analytics technology such as SIEM and IDS solutions. Will apply multiple principles such as packet capture, behavioural analysis, and threat research to identify trends and technical risks.

EU/SI

6%

£65-£110k

£550-£800 a day

Technical Security

Careers in technical security are focused on developing technical controls to enforce security policies and procedures, and can develop to become particularly lucrative as roles grow in management responsibility. The salaries reflect the ranges once could expect depending on experience and size of the organisation.

Security Administrator

Broad role offering operational support to the security function performing duties like user access management, change requests, and patching.

EU/SI/PS

6%

£35-£55k

£400-£450 a day

Security Engineer

Some involvement in developing technical standards and solution, with the focus of the role being to implement the technical controls required to enforce the ISMS.

EU/SI/PS/V

3.5%

£55-£95k

£400-£600 a day

Security Architect

Technical roles with something of a management overview, will focus predominantly on High Level Design looking at the workflow and broad controls. Will translate the security policy into technical specification.

EU/SI/PS

8%

£75-£130k

£500-£700 a day

Security Solutions Architect

Senior yet hands-on role which encompasses developing technical solutions, identifying security controls, and creating design documentation. Will help embed security in to projects throughout the business.

EU/SI/PS/V

8%

£75-£130k

£500-£800 a day

Enterprise Security Architect

Proven track record of developing security architectures and acting as technical design authority cross enterprise-scale infrastructures. Ability to understand deep technical topics from a top-down and management perspective.

EU/SI

5%

£90-£135k

£550-£800 a day

Application Security Specialist

Responsible for architecting security controls around all aspects of the application environment, from secure development, server stacks and web app firewalls.

EU/SI/V

2%

£80-£150k

£650-£800 a day

SecDevOps

Responsible for developing applications securely. Will have thorough knowledge of Java and agile development practices.

EU/SI/V

£60-£90k

£400-£550 a day

Detection/ Investigation

Detection and Investigation roles reflect a niche set of skills that appeal to those who are inquisitive and analytical. Salaries depend on the complexity of work and the type of organisation and sector the individual works for.

Security Investigation

Some overlap with forensics professionals but more likely to take ownership of the investigation and evidence collection. Concerned with the extent and cost of the breach as opposed to the 'who' and the 'how'.

EU/SI

£55-£80k

£400-£450 a day

Digital Forensics

Technical role focussed on identifying exactly what has occurred during a breach. This will include indentifying the point of entry, any vulnerabilities,

EU/SI/PS

£40-£65k

£350-£600 a day

Security Operations Analyst

Sits within a SOC focussing on monitoring systems for intrusion detection and prevention; will often act as the first line of incident response/escalation.

EU/SI/PS

6%

£55-£80k

£400-£800 a day

SOC/ Security Operations Manager

Oversight of atechnical intrusion monitoring and response team. Technical background with some risk/assurance oversight and will input in to strategy and solutions, as well as mentoring colleagues within security operations.

EU/SI/PS

5%

£85-£110k

£600-£800 a day

Incident Response Analyst

Expert incident handler who will manage the technical response to a security breach. Some input in to intrustion response procedures.

EU/SI/PS

7%

£65-£90k

£475-£600 a day

Sales Engineering & Product Management

Sales Engineers support the sales function of an organisation and provide technical expertise in a customer facing environment. Salaries reflect the level of experience of the individual, market area and location of the organisation.

Pre Sales Consultant/ Sales Engineer

Supports the sales function through the delivery of technical presentations, responses to bid/tenders, and developing proof of concept installations. Works closely between the client, and product management and support teams. OTE shown (typically 80:20 split)

SI/V

5.6%

£70-£120k

Senior Pre-Sales Consultant/ Sales Engineer

Supports the sales function through the delivery of technical presentations, responses to bid/tenders, and developing proof of concept installations. Works closely between the client, and product management and support teams. OTE show (typically 80:20 split)

SI/V

9.5%

£80-£150k

Product Manager

Review of technologies to input in to their ongoing development as a stand alone product and as part of broader solutions. Works closely with sales and marketing, responsible for channel communications, and acts as an escalation point on large scale deployments.

SI/V

3%

£55-£110k

Product Director

Responsible for architecting security controls around all aspects of the application environment, from secure development, server stacks and web app firewalls.

SI/V

2%

£100-£130k

VP Product

Responsible for managing product life cycle from the onset of strategic planning and solution development, through to leading the execution. Will often have overview of a portfolio of products and value-add services, working to coordinate the collaboration of commercial and technical teams. Base shown.

SI/V

£140-£180k

Security Evangelist

A champion for all things security, driving cultural improvement. The face of organisation's security posture, focused on best practice above all else.

SI/V

6%

£110-£150k

Sales & Marketing

Sales and Marketing roles are tasked with relationship building, generating leads and driving revenue on behalf of their organisation. The salaries typically include bonus and commission - based on performance to achieve an OTE.

Inside Sales Rep

Responsible for lead generation activities.

SI/V

£25-£50k

New Business Sales - SME

Responsible for winning new clients within the SME market. OTE shown.

SI/V

8%

£110-£150k

New Business Sales - Enterprise

Direct sales role focussed around mid-corporate and enterprise level organisations. OTE shown.

SI/V

3%

£120-£220k

Regional Account Manager

Responsible for working with existing customers as well as an element of new business acquisition. Main function of the role is to grow existing business.

SI/V

£120-£160k

Major Account Management

Responsible for working closely with several large existing high-value customers to deliver a consultative and focussed client experience. Typically 2/3rds new business and 1/3rd account management. OTE shown.

SI/V

3%

£160-£200k

Channel and Alliance Sales

Selecting, recruiting, managing and supporting a partner network, consisting of VAR's, systems integrators and MSSP's. OTE shown.

SI/V

3%

£140-£180k

Marketing Executive

Responsible for the operational execution of the marketing strategy through the use of digital and print media, events and enabling the sales function.

SI/V

22%

£35-£75k

Marketing Manager

Will work closely with senior sales colleagues to set regional direct and channel marketing strategies, and lead implementation activities.

SI/V

17%

£75-£115k

VP Marketing

Responsible for setting the marketing strategies at a global level, for the products and/or services within the organisation.

SI/V

£100-£160k

Executive Management

Executive Management roles include the most senior of the roles within the industry, both in the end user and vendor markets. Those who hold such titles usually represent diverse experience across both technical and commercial domains. The sector in which the organisation sits, alongside the size of the organisation have a direct effect on the range of salaries available.

Operations Director/ General Manager

Responsible for overseeing process, compliance, corporate governance, international operations, and support divisions for the entirety of the business.

SI/V

21%

£175-£250k

Regional VP

An executive management role with territorial oversight for a particular region. Typically reporting into VP EMEA/APAC/US. OTE shown.

SI/V

£200-£275k

Pre-Sales Director

Responsible for leading technical sales capabilities and will input into wider commercial solution development. OTE shown.

SI/V

£150-£200k

Sales Director/ EVP

Commercial business leader with management responsibility across sales, marketing and operations. OTE shown.

SI/V

10%

£250-£300k

VP EMEA

Regional business lead with responsibility for strategy and execution of sales, marketing and operations. Will have some input in to product/ service development. OTE shown.

SI/V

4.5%

£280-£400k

Marketing Director/ CMO

Develops international marketing strategies whilst overseeing the marketing activities across the organisation. OTE shown.

SI/V

13%

£150-£190k

Chief Technology Officer

Board level technical role concerned with the ongoing development of soft and hardware based products, services and solutions.

SI/V

9%

£155-£215k

Security Director/ Head of Information Security

Overarching responsibility for all information security and risk concerns in a SEM to mid cap corporate.

EU/SI/PS

12.5%

£105-£165k

References:

1. Ismail, N. (2018, 4 July). What sectors are investing the most and least in cyber security? Retrieved from Information Age: https://www.information-age.com/sectors-investing-most-least-cyber-security-123473207/
2. Ernst & Young. (2018). Report - EY GISS Survey 2017-18. Retrieved from Ernst & Young: https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf
3. Wadsworth, J. et al (2016, May). Brexit and the Impact of Immigration on the UK. Retrieved from the London School of Economics: cep.lse.ac.uk/pubs/download/brexit05.pdf
4. Anon. (2017, 30 November). Net migration falls by more than 100,000 after Brexit vote. Retrieved from the BBC: https://www.bbc.co.uk/news/uk-42178038
5. Bulman, M. (2018, 28 June). Government warned of 'disastrous' impact of Brexit on economy as immigration plummets. Retrieved from the Independent: https://www.theindependent.co.uk/news/uk/home-news/brexit-uk-immigration-workers-employment-2018-latest-updates-a8420781.html
6. Curley, J. (2018, 14 June). Deal, No Deal: The State of U.K. Cyber Security Post-Brexit. Retrieved from Radware: https://blog.radware.com/security/2018/06/uk-cybersecurity-post-brexit/
7. Daniel, E. (2018, 25 June). STEM skills shortage undermining UK industry's post-Brexit prospects. Retrieved from the Verdict: https://www.verdict.co.uk/stem-skills-uk-industry-brexit/
8. Reed, J. and Acosta-Rubio, J. (2017). The Global Information Security Workforce Study (GISWS). Retrieved from the Center for Cyber Safety & Education: https://iamcybersafe.org/gisws/
9. Thompson, S. (2018, 10 June). Impact of Brexit on cybersecurity far reaching, says expert. Retrieved from the Irish Times: https://www.irishtimes.com/news/ireland/irish-news/impact-of-brexit-on-cybersecurity-far-reaching-says-expert-1.3525708
10. Manthorpe, R. (2017, 3 July). Wetherspoons just deleted its entire customer email database – on purpose. Retrieved from Wired: https://www.wired.co.uk/article/wetherspoons-email-database-gdpr
11. Hill, R. (2018, 25 May). US websites block netizens in Europe: Why are they ghosting EU? It's not you, it's GDPR. Retrieved from the Register: https://www.theregister.co.uk/2018/05/25/tronc_chicago_tribune_la_times_gdpr_lock_out_eu_users/
12. Travis, A. (2017, June 5). Simple numbers tell story of police cuts under Theresa May. Retrieved from: https://www.theguardian.com/uk-news/2017/jun/05/theresa-may-police-cuts-margaret-thatcher-budgets
13. Travis, A. (2015, 15 October). Crime rate in England and Wales soars as cybercrime is included for first time. Retrieved from: https://www.theguardian.com/uk-news/2015/oct/15/rate-in-england-and-wales-soars-as-cybercrime-included-for-first-time
14. Muncaster, P. (2018, 21 August). Cybercrime prosecutions fall again in the UK. Retrieved from Info-Security Magazine: https://www.infosecurity-magazine.com/news/cybercrime-prosecutions-fall-again/
15. Warrell, H. (2017, 23 August). Police officers should be sacked for poor IT skills, report says. Retrieved from the Financial Times: https://www.ft.com/content/d1f8f97c-8749-11e7-8bb1-5ba57d47eff7
16. Miller, R. (2018, 28 January). AWS beefs up threat detection with Sqrrl acquisition. Retrieved from TechCrunch: https://techcrunch.com/2018/01/24/aws-beefs-up-threat-detection-with-sqrrl-acquisition/
17. Desai, M. (2018, 14 February). VMWare acquires CloudCorero. Retrieved from VMWare: https://cloud.vmware.com/community/2018/02/14/vmware-acquires-cloudcoreo/
18. Dhawan, S. (2018, 28 March). VMware Acquires E8 Security: Leveraging Behavior [sic] Analytics to Secure the Digital Workspace. Retrieved from VMWare: https://blogs.vmware.com/euc/2018/03/e8-security-behavior-analytics-digital-workspace.html
19. Anon. (2018, 5 March). Oracle buys Zenedge. Retrieved from Oracle: https://www.oracle.com/corporate/acquisitions/zenedge/index.html
20. Novinson, M. (2018, 2 August). Symantec to cut staff by up to 8 percent as part of $50m restructuring. Retrieved from CRN: https://www.crn.com/news/security/300107511/symantec-to-cut-staff-by-up-to-8-percent-as-part-of-50m-restructuring.htm
21. Anon. (2018). 2018 State of the industry report. Retrieved from Shred-It: https://www.shredit.co.uk/getmedia/87b91029-abe2-4126-8eb2-fd-73c480e61a/2018-Shred-it-SoI-Report-UK.aspx?ext=.pdf
22. Bordessa, E. (2018, 16 January). The real costs of a data breach. Retrieved from IT Governance https://www.itgovernance.co.uk/blog/the-real-costs-of-a-data-breach/ (PSA: the original Ponemon Institute report has not been referenced as it includes a pre-ticked registration form.)
23. Anon. (2018, 7 July). Director GCHQ speaks at Billington Cyber Security Summit. Retrieved from: https://www.gchq.gov.uk/news-article/director-gchq-speaks-billington-cyber-security-summit
24. Anon. (2018, 24 July). Russian hackers penetrate US power stations. Retrieved from the BBC: https://www.bbc.co.uk/news/technology-44937787
25. Anon. (2018, 15 March). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved from US-CERT: https://www.us-cert.gov/ncas/alerts/TA18-074A
26. Roberts, D. et al. (2016, 27 July). Donald Trump to Russia: hack and publish Hillary Clinton's 'missing' emails. Retrieved from the Guardian: https://www.theguardian.com/us-news/2016/jul/27/donald-trump-russia-hillary-clinton-emails-dnc-hack
27. Buncombe, A. (2018, 13 July). Russians tried to hack Clinton emails same day Trump publicly asked them to, says Russia probe indictment. Retrieved from the Independent: https://www.independent.co.uk/news/world/americas/us-politics/russia-hack-clinton-emails-mueller-probe-indictment-trump-latest-a8446626.html
28. Hern, A. (2017, 26 October). NSA contractor leaked US hacking tools by mistake, Kaspersky says. Retrieved from the guardian: https://www.theguardian.com/technology/2017/oct/26/kaspersky-russia-nsa-contractor-leaked-us-hacking-tools-by-mistake-pirating-microsoft-office
29. Kastrenakes, J. (2018, 13 August). Trump signs bill banning government use of Huawei and ZTE tech. Retrieved from the Verge: https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump
30. Anon. (2018, 23 August). Huawei and ZTE handed 5G network ban in Australia. Retrieved from the BBC: https://www.bbc.co.uk/news/technology-45281495
31. Anon (2018, 17 April). China's ZTE deemed a 'national security risk' to UK. Retrieved from the Guardian: https://www.theguardian.com/technology/2018/apr/17/chinas-zte-a-national-security-risk-to-uk-warns-watchdog
32. Chapman, B. (2018, 20 July). Huawei poses security risk to UK telecoms network, British spies warn. Retrieved from the Independent: https://www.independent.co.uk/news/business/news/huawei-uk-security-risk-telecoms-network-gchq-warning-a8456006.html
33. Lynch, S. and Volz, D. (2018, 24 April). U.S. regulator fines Altaba $35 million over 2014 Yahoo email hack. Retrieved from: https://uk.reuters.com/article/us-altaba-cyber-yahoo/u-s-regulator-fines-altaba-35-million-over-2014-yahoo-email-hack-idUKKBN1HV295
34. Lunden, I. (2017, 21 February). After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B. Retrieved from TechCrunch: https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/
35. Jay, J. (2017, 10 May). Yahoo coughed up $16m in legal costs following 2013 data breach. Retrieved from TEISS: https://www.teiss.co.uk/information-security/yahoo-16m-legal-costs-data-breach/
36. Greenberg, A. (2018, 22 August). The untold story of NotPetya, the most devastating cyberattack in history. Retrieved from Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
37. Burton, G. (2017, 7 November). Maersk pins $300m cost on NotPetya ransomware. Retrieved from Computing: https://www.computing.co.uk/ctg/news/3020561/maersk-pins-usd300m-cost-on-notpetya-ransomware
38. Whittaker, Z. (2018, 23 March). A new data leak hits Aadhaar, India's national ID database. Retrieved from ZDnet: https://www.zdnet.com/article/another-data-leak-hits-india-aadhaar-biometric-database/
39. Anon. (2018, 25 September). Aadhaar security breaches: here are the major untoward incidents that have happened with Aadhaar and what was actually affected. Retrieved from First Post: https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html Anon (2018, 5 June). Security breach at MyHeritage website leaks details of over 92 million users. Retrieved from Reuters: https://www.reuters.com/article/us-myheritage-privacy/security-breach-at-myheritage-website-leaks-details-of-over-92-million-users-idUSKCN1J1308

40 Dunn, J. E. (2018, 17 September). Equifax IT staff had to rerun hackers' database queries to work out what was nicked. Retrieved from the Register: https://www.theregister.co.uk/2018/09/17/gao_report_equifax_mega_breach/
41 Anon. (2018, 2 March). Equifax expects net $200 mln in breach-related costs in 2018. Retrieved from Reuters: https://www.reuters.com/article/equifax-cyber/equifax-expects-net-200-mln-in-breach-related-costs-in-2018-idUSL2N1QK0N4
42 Anon. (2018, 20 September). Credit reference agency Equifax fined for security breach. Retrieved from the ICO: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/credit-reference-agency-equifax-fined-for-security-breach/
43 McCrank, J. and Finkle, J. (2018, 2 March). Equifax breach could be most costly in corporate history. Retrieved from Reuters: https://uk.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUKKCN1GE257
44 Levingston, I. and Surane, J. (2018, 7 September). Equifax Breach a Year Later: Record Profits, Share Revival. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2018-09-07/equifax-breach-a-year-later-record-profits-share-price-revival
45 Cohen, J. (2018, 23 March). Massive cyberhack by Iran allegedly stole research from 320 universities, governments, and companies. Retrieved from the American Association for the Advancement of Science: http://www.sciencemag.org/news/2018/03/massive-cyber-hack-iran-allegedly-stole-research-320-universities-governments-and
46 Cuthbertson, A. (2018, 24 August). Iranian hackers attack UK universities to steal secret research. Retrieved from the Independent: https://www.independent.co.uk/life-style/gadgets-and-tech/news/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html
47 Anon. (2018). The 2018 Hacker Report. Retrieved from HackerOne: https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report.pdf
48 Miller, R. (2018, 7 February). Google's bug bounty programs paid out almost $3M in 2017. Retrieved from TechCrunch: https://techcrunch.com/2018/02/07/googles-bug-bounty-programs-paid-out-almost-3m-in-2017/
49 Amadeo, R. (2018, 27 August). Fortnite's Android vulnerability leads to Google/Epic Games spat. Retrieved from Ars Technica: https://arstechnica.com/gadgets/2018/08/fortnites-android-vulnerability-leads-to-googleepic-games-spat/
50 Newcomer, E. (2017, 21 November). Uber Paid Hackers to Delete Stolen Data on 57 Million People. Retrieved from Blooberg: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data
51 Cameron, D. (2018, 26 September). Uber to Pay Record $148 Million Fine for Concealing 2016 Data Breach. Retrieved from Gizmodo: https://gizmodo.com/uber-to-pay-record-148-million-fine-for-concealing-201-1829334439
52 Cadwalladr, C. and Graham-Harrison, E. (2018, 17 March) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from the Guardian: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
53 Kanter, (2018, 17 August). Protesters are trying to shame Facebook by vandalising its ubiquitous 'not our friend' ads in London. Retrieved from Business Insider: http://uk.businessinsider.com/facebook-not-our-friend-ads-vandalised-in-london-2018-8
54 Anderholm, H. (2014, 17 October). Why Is Russia Simulating Nuclear Strikes on Sweden?. Retrieved from Vice: https://www.vice.com/sv/article/dpwk4q/why-is-russian-military-hanging-out-on-swedish-territory
55 Scott, M. and Murphy, C. (2017, 27 July). Swedish ministers resign amid data security breach scandal. Retrieved from Politico: https://www.politico.eu/article/sweden-data-breach-privacy-security-stefan-lofven/
Targett, E. (2018, 28 June). The Ticketmaster Hack is Worse Than First Thought. Retrieved from Computer Business Review: https://www.cbronli56 ne.com/news/ticketmaster-hack-latest
57 Topham, G. (2018, 6 September). British Airways customer data stolen from its website. Retrieved from the Guardian: https://www.theguardian.com/business/2018/sep/06/british-airways-customer-data-stolen-from-its-website
58 Zorz, Z. (2018, 20 September). New Magecart victims ABS-CBN and Newegg are just the tip of the iceberg. Retrieved from Help Net Security: https://www.helpnetsecurity.com/2018/09/20/magecart-victims/
59 Martin, C. and Toon, D. (2017). The cyber threat to UK business report 2016/17. Retrieved from the NCA: http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file Morgan, S (2018, 21 July). Women Represent 20 Percent Of The Global Cybersecurity Workforce In 2018. Retrieved from Cyber Security Ventures: https://cybersecurityventures.com/women-in-cybersecurity/
60 Khazan, O. (2018, 18 February) The More Gender Equality, the Fewer Women in STEM. Retrieved from the Atlantic: https://www.theatlantic.com/science/archive/2018/02/the-more-gender-equality-the-fewer-women-in-stem/553592/
61 Anon. (2018, 13 September). Guidance: Data protection if there's no Brexit deal. Retrieved from Gov.UK: https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal
62 Mirreh, M. (2018, 31 January). UK Data Market to Exceed £1.1 Billion to Become Largest in Europe. Retrieved from PerformanceIN: https://performancein.com/news/2018/01/31/uk-data-market-exceed-11-billion-become-largest-europe/
63 Weise, E. (2017, 27 July). Hackers at DefCon conference exploit vulnerabilities in voting machines. Retrieved from USA Today: https://eu.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/
64 Rolfe, A. (2018). 10 of the highest-paying jobs 2018. Retrieved from Reed: https://www.reed.co.uk/career-advice/10-of-the-highest-paying-jobs-2018/
65 Anon. (2018). Information Security recruitment agency listing. Retrieved from Agency Central: https://www.agencycentral.co.uk/agencysearch/IT/skills/security/information-security.htm
66 Anon. (2018). Cybersecurity Search Firms. Retrieved from Cyber Security Ventures: https://cybersecurityventures.com/cybersecurity-search-

About the Author: Ryan Farmer

Now in his tenth year with the company, Ryan is an Acumin veteran. As group Compliance Manager and DPO, he has used his expertise as a practitioner and a background in cyber security recruitment, to deliver opinion across multiple reports, panels, and webinars.

About the Author: Martha Tonks

Martha joins Acumin as the Marketing Manager for the wider group, writing and contributing to many pieces of industry specific content, with several whitepapers in circulation. Martha is responsible for shaping the content strategy and executing its delivery, including the annual survey..