



# **BEYOND THE CLOUD**

## **UK TECHNOLOGY RESEARCH 2018**

### **CONTEXTUAL ANALYSIS**

# INTRODUCTION

British business is facing a period of prolonged uncertainty. Brexit, new regulations, and emerging technologies are offering up both challenges and opportunities. How British companies react and adapt will dictate how well they and the economy do, and technology will be at the heart of this period of transformation.

During the summer of 2018, ServiceteamIT, in conjunction with Doogheno, carried out their second annual technology adoption survey of 1,100 UK companies. The survey gives a snapshot of British business at this time of change. The survey was completed over a three week period between the 14th of June and the 7th of July 2018. The sample included over 1,100 people responsible for IT decision making, which ensured that valuable and insightful information was collected.

The survey asked about challenges, current infrastructure and services, and plans for the next 36 months. This report looks at the answers received and explores the impact of external challenges that businesses face in 2018 and beyond, such as Brexit, GDPR and the rise of cyber-crime.

***“The more clarity we have on the future trading relationship, the easier it will be for business to plan ahead.” Stephen Martin, Director General of the Institute of Directors on Brexit.***

We examined the impact of the uncertainty surrounding Brexit and companies' plans for readiness. While the Government continues to negotiate, business is no clearer about an outcome and the possible implications on regulation and trading conditions.

The introduction of GDPR will not have escaped the notice of any IT or business management professional. It replaced the 1998 Data Protection Act, and updated the legislation to make it more fit for purpose in our digital world. The twin goals of the GDPR are to give people in general more control over the way their data is held, while also giving businesses a clearer understanding of their responsibilities. Compliancy is not a one off event and we look at companies' ongoing efforts to remain compliant.

UK businesses face an unprecedented level of threat from cyber-security attacks. Cyber security and data protection have been upfront in the news all year, with Facebook/ Cambridge Analytica, potential Russian interference in elections and direct cyber attacks such as the WannaCry event that effected the NHS.

The survey looked at the use of technology in UK business, from preferred cloud providers through to the overall use of emerging technologies, including Artificial Intelligence, Blockchain and IOT.

This paper explores the resulting data, and aims to put those results in context.

# GDPR

In our previous 2017 survey, 62 per cent of respondents said GDPR was going to be the biggest external factor affecting their business. And clearly it has been a major disruptive change in how many businesses operate. For some it has meant business as usual as they follow best practice throughout, for many others though it has been a wake-up call bringing their responsibilities as a data curator into sharp focus. The onslaught of emails in April announcing the arrival of the GDPR legislation arrived in every inbox and we chose to opt out or in of email communications from many organisations that we'd forgotten we ever engaged with... but GDPR isn't a one off YK2 incident. GDPR is not going away and email consent was just the tip of the iceberg. Very few companies are completely compliant, there is a high level of misunderstanding of the regulation and it will be a few more years before rulings and judgements provide definitive clarification.

The misunderstandings around GDPR have been fuelled by self-appointed experts in consultancy companies taking the opportunity to exploit incoming regulation. A prime example of this was the GDPR training given to MPs in the House of Commons where MPs were told to delete all casework information from before June 2017. Another example is the pub chain JD Wetherspoons who deleted all customers email addresses, saying,

*"We felt, on balance, that we would rather not hold even email addresses for customers. The less customer information we have, which now is almost none, then the less risk associated with data."*

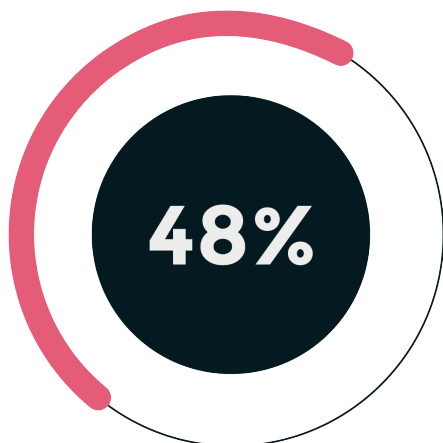
Most companies have not taken such extreme action, and have been conscientiously acting to become compliant, and this is an ongoing activity with 18 per cent of respondents to the 2018 survey saying they expect GDPR to be the largest external factor affecting their business in the coming year.

The Royal Mail's warning that annual addressed letter volumes could drop more than expected due to the potential impact of the General Data Protection Regulation is just one example of how GDPR is changing behaviours of companies, in this instance those using direct marketing. Changes to Whois data as a result of GDPR is affecting the way that cybersecurity professionals protect companies, Whois data empowers everyday security capabilities such as domain and IP risk assessment and spam protection and removing the ability to identify owners of domains and websites is predicted to hamper the ability of professionals to protect their companies with it becoming far harder to discern the persons or organisation behind a website. Cybercriminals are aware of this and may exploit it to take advantage of unsuspecting users online.

While GDPR is already in place, companies' responses to it are still evolving and what is in place now will change. In many instances, it clearly needs to. An analysis of policies from 14 of the largest internet companies showed they use unclear language, claim "potentially problematic" rights, and provide insufficient information for users to judge what they are agreeing to. Privacy policies from companies including Facebook, Google and Amazon do not fully meet the requirements of GDPR, according to the pan-European consumer group BEUC.

The Information Commissioner's Office's statement that they are "not going to be looking at perfection, we're going to be looking for commitment" will provide some comfort.

The awareness of GDPR by the general public is high and people are exercising their rights, with the Information Commissioner's Office stating that it had received 1,106 data protection complaints in the three weeks following the GDPR's introduction, and reporting that data breach notifications, which are mandatory under the GDPR for most data security breaches, had also increased. The survey found that while data breaches had remained stable in the previous year, 22 per cent believe they will have to report more breaches to the ICO in the coming year. In 2017, 15 per cent of the respondents stated they had reported a breach.



**Have NOT allocated budget for increased overheads for GDPR, such as access requests and minor data breaches**

From SME to the largest of Enterprises, data breaches continue to be commonplace, and with data breaches come fines. These were limited under the previous legislation and for many businesses were seen as little more than a nuisance. The £500,000 fine Facebook has faced for its dealings with Cambridge Analytica, par example. However the fines are set to be far higher under GDPR. They could be 4 per cent of global turnover, which would make even Mark Zuckerberg think twice about being so blasé with customers' data. Other high profile breaches include British Airways, British Telecom and the University of Greenwich.

In the lead up to the legislation, GDPR was often seen as an IT department problem, one that could be fixed by implementing technology. The reality is that data breaches happen because people do not do what they are supposed to do. Or because they do things they are not supposed to do. No amount of IT infrastructure can eliminate the human error factor, and no system is foolproof against a well-equipped fool. 38 per cent of the survey respondents have concerns about GDPR compliance within their company outside of the IT department. It is a requirement that staff should receive awareness training for GDPR and companies should look at what this means for their own staff. Salespeople with shadow IT copies of databases, marketers contacting mailing lists, customer services operatives taking customer details to help resolve queries, there is personally identifiable data at many touch points within a company that the IT department have little visibility of.

Over half of the respondents, 52 per cent, said their companies had assigned budget in the coming year to help respond to GDPR related requests and potential breaches.

GDPR will remain in place no matter the outcome of the Brexit negotiations as it will be incorporated into UK law. However, if the result is a no deal Brexit with no agreement and no transition period, all Union primary and secondary law will cease to apply to the United Kingdom from 30 March 2019. The United Kingdom will then become a third country. This will lead to many issues, but here we will concern ourselves with Chapter V of the GDPR. The GDPR imposes restrictions on the transfer of personal data outside the European Union to third countries or international organisations and the UK will be subject to the restrictive provisions governing transfer of personal data outside the EU's geographical boundaries. The immediate effect would be that data transfers that are currently carried out daily, would be subject to additional scrutiny and may become prohibited altogether.

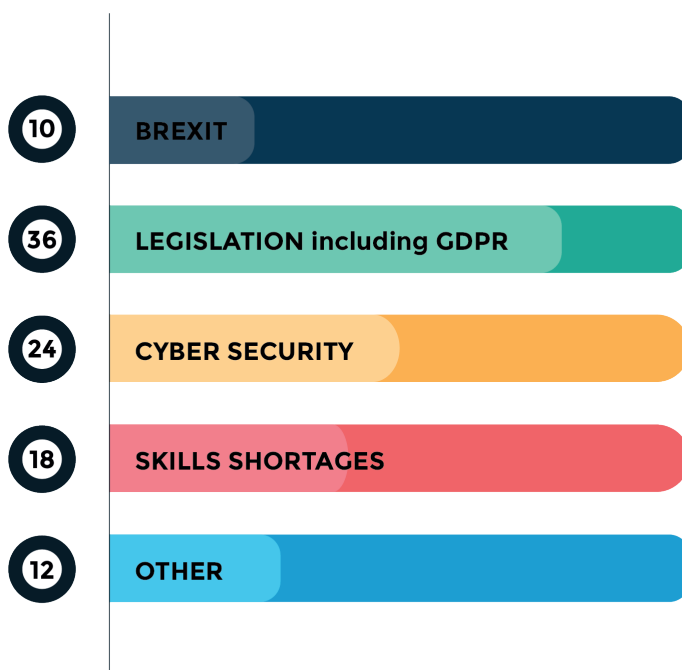
***“When we do need to apply a sanction, fines will not always be the most appropriate or effective choice,”***

***Elizabeth Denham. Head of ICO***

# CYBER SECURITY

Cyber security has moved on a long way from Firewalls, anti-virus and anti-spam. Concerns about cyber security go from the very top with interference in elections by foreign states, to smishing on teenagers phones. In a connected world where there are more mobile devices than people, the importance of cyber security has never been so great and with significant fines for data breaches, no company can be complacent regardless of their sometimes sizeable investment in software, systems and procedures.

So it is no surprise then that nearly a quarter, 24 per cent, of survey respondents said that cybersecurity events were the biggest external factor currently affecting their business.



Perceived impact of external factors on businesses 2017-2018

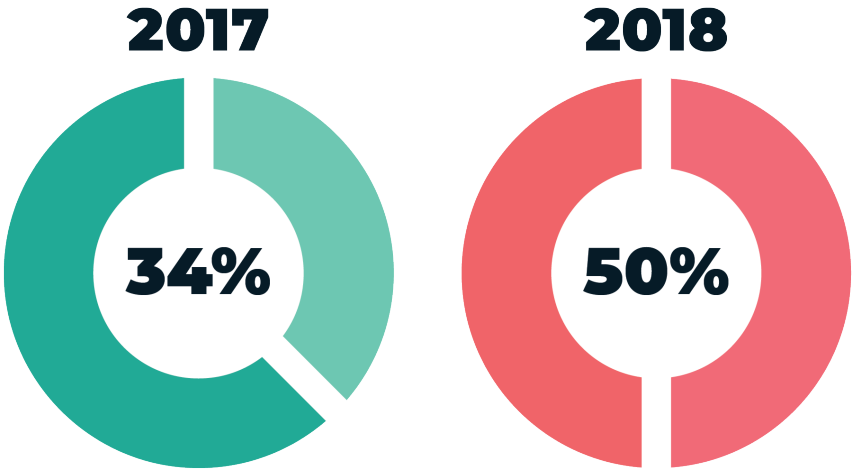
The motivation for cybercrime is both financial and political.

Financial fraud crimes and Cyberextortion are common. A recent email based attack used passwords from the 2012 LinkedIn breach in the body of the email which lead many recipients to believe that their machine had been compromised and the attacker did indeed have compromising browsing and webcam information which would be released unless a large sum was paid in Bitcoin. An unsophisticated DDOS attack using a botnet of 1,000 workstations can cost as little as £5 per hour to run but the estimated average cost to the recipient is over £35,000 per attack in lost business and productivity plus mitigation costs. The cost of cybercrime is hard to truly state, many incidents are covered up and few companies want to go completely public with the impact but just within the UK legal sector, £11 million of client money stolen due to cybercrime over the last 12 months with 60% of law firms reported to have suffered information security incidents last year.

Politically based attacks can be Cyberterrorism or Cyberwarfare. Cyberterrorism intimidates or coerces a government or an organisation to advance their political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them. But it is Cyberwarfare that we will focus on.

22 per cent of our contributors reported that they had experienced attacks originating in Russia, overwhelmingly the largest single originating country for attacks. While we cannot conclude that these attacks were all state-sponsored, it is clear that Russia does use sophisticated cyber-attacks on countries to influence their own agenda. Whether using bots on social media to influence elections, infiltrating core infrastructure providers such as energy companies or disrupting commerce in countries by hitting their business the state-sponsored attacks are considered the single largest cybersecurity threat there is and the disruption is very well funded. There is an argument to say it has been used to influence our own democratic processes. While this is yet to be proven, incidents in Estonia, France, Germany and the Ukraine would indicate that there is a pattern of such actions. And in the US this year, the United States Computer Emergency Response Team released an alert warning that the Russian government was executing “a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities’ networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks.”

Within all business sectors surveyed, there was a reported increase in cybersecurity incidents, with overall 49 per cent of respondents reporting an increase in cyber security incidents. 16.5 per cent believe this will be their biggest problem in the coming year.



**Businesses reporting an increase in cyber security incidents in the last 12 months**



As the criminals carrying out the attacks become more sophisticated so must the ways that companies protect their data and employees. While brute force attacks and denial of service are still very much commonplace, the combination of technology and social engineering of spear phishing attacks are growing, and they are far harder to mitigate. At the 2018 Winter Olympic Games in Pyeongchang attackers spoofed the email address of the National Counter Terrorism Center South Korea to send emails to the Olympic organizations with the subject line “Organized by Ministry of Agriculture and Forestry and Pyeongchang Winter Olympics.” The victims received an email purporting to be an anti-terrorism drill, asking them to find instructions within the malicious document. The criminals used different approaches to launch the attack successfully without being caught, including embedding malicious code in the documents and hidden images, hidden Visual Basic macros, and custom Powershell codes.

The threat of disruption from a cyber-attack is recognised at the highest levels as very real and very damaging. Over the last year, we have seen a significant increase in the scale and severity of malicious cyber activity globally. In the UK, we have seen the impact of major cybersecurity incidents, such as the WannaCry attack that affected 48 NHS Trusts. To meet this challenge, the government has put in place our National Cyber Security Strategy 2016-2021, supported by £1.9bn of transformational investment. There is also the NIS Directive which is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU. It creates a culture of security across sectors which are vital for our economy and society, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority.

***“Would-be criminals no longer need to be computer experts to conduct cyber crime, because they can buy in the various components they need as easily as online shopping.”***

***Surrey University criminologist Michael McGuire***

# BREXIT

Much has been written about Brexit, though the debate over whether its right or wrong has little relevance to the reality as it stands. The government did trigger Article 50 so at the end of March 2019 we will leave the EU and this will impact business. We could still have frictionless trade with the EU with access to new trade deals around the world, however it is highly likely that whatever the outcome it will be disruptive to business. While only 10 per cent of survey respondents felt that Brexit had already had an impact on their business, 31 per cent believed it would be the largest single external threat facing their business in the next year.

There are a number of possible outcomes of the ongoing Brexit negotiations. At the time of writing, it is not clear which one we will end up with. Here are some ideas.

**Norway Style Brexit** - effectively remaining a member of the EU without influence and voting rights, still working under EU law, accepting freedom of movement and having frictionless trade with Europe. While technically this would deliver Brexit based on the terms of the referendum it is very unlikely that the government will pursue this approach as it crosses multiple of the red lines set out for negotiation.

**Bespoke** - The government's preferred solution is to have a deal like no other, given our unique relationship with Europe. This is the hardest to negotiate and is why it seems that little progress has been made. It is highly complex and even if a broad stroke agreement is reached it may take years of negotiation to define all the elements. The government is under considerable internal party pressure not to have an extended transition period, but an extended transition period could reduce the impact of Brexit on businesses and citizens of both the UK and the EU. Increasingly likely is a no deal Brexit but with a transition period where the UK would abide by EU law. This would free the UK to open trade deal talks with other countries while having space to plan Brexit without it being likened to falling off a cliff. For business, this would mean a smoother transition but it would also extend the period of uncertainty about what rules and regulations they would need to operate under and hamper planning for the coming years.

**No Deal Brexit** - If the UK and the EU fail to come to any agreement, then there is a high possibility of a no deal Brexit or hard Brexit. In this worst-case scenario, the UK would have no access to the EU market, there would be no recognition of mutual laws and regulations and the UK would be the only country in the world without a single trade deal. If a no deal Brexit is looking likely then it is possible that the UK and the EU may agree to extend the negotiation time. As no deal would impact both parties this is becoming an increasingly likely scenario. While it will ultimately allow for a better outcome it does also mean an extension to the period of uncertainty which will result in a decision making paralysis for many businesses.

OR

**Restart the whole process** - There are increasing calls for a second referendum, or a people's vote on the final deal. It is possible that parliament may not have the stomach to pass a deal which they know is not in the best interest of the country and defer their decision making again to the people of the country. This could also happen in the form of a general election. While this outcome is highly unlikely it could result in business as usual with Europe, although the political fallout would undoubtedly be disruptive.

As the final outcome is unknown businesses should now be planning for the worst and hoping for the best.

20 per cent of the survey respondents said their businesses are already planning for multiple possible outcomes from the Brexit negotiations. 35 per cent said their companies were currently taking no action at all and 45 per cent were unsure what their business plans to do. It is clear that British business is unprepared and this is largely because it is uninformed.



**NO Contingency plan in place for possible outcomes of Brexit negotiations.**

A number of companies have come out and made very clear statements about their planning, Airbus, for example, have said they are starting to stockpile parts which are normally just in time, 50 London-based banks have approached eurozone banking regulators about relocating key services and BMW have said they may have to stop production entirely in the UK. While some of the statements by business have been politically motivated, such as Amazons warning about civil unrest within 2 weeks of Brexit, much of it is industry experts understanding the full impact of the disruption to their businesses.

With 25% of survey respondents predicting that they will be heavily affected by skills shortages over the next year, removing the rights for European workers to work in the UK would be potentially damaging and while other trade deals will no doubt include working visas, making it easier to employ people from other countries, these will not be in place immediately

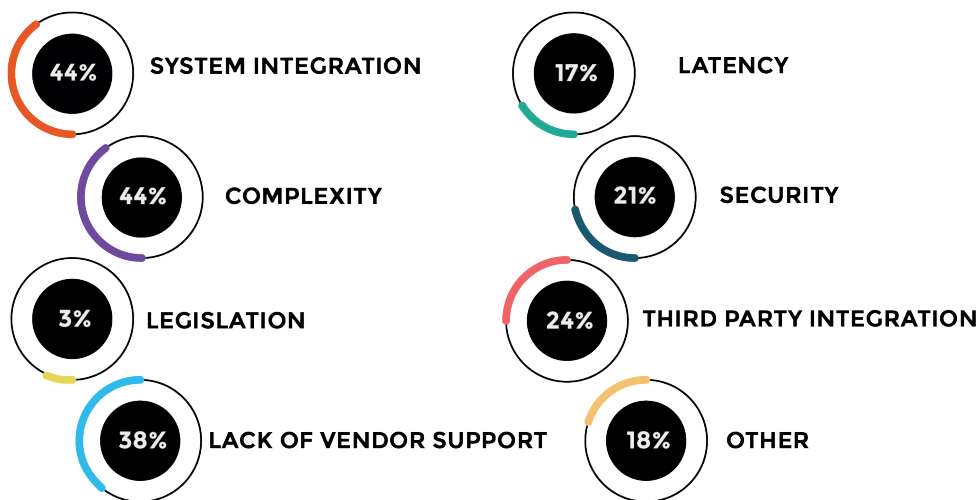
The UK government is releasing guidance to its business and citizens about the possible impact of a no deal Brexit. The EU has also issued 60 preparedness notices that layout its position if the negotiations result in no deal. The effect of the no deal positions is far-reaching, covering aviation, agriculture and industry sectors including technology.

The impact on technology goes from the fairly trivial such as revoking .eu domain names too far more complex such as the transfer of EU citizens data to a third country. The UK would become a third country at the end of March 2019. And while GDPR would be incorporated into UK law the European Commission would need to make an Adequacy Decision for data to be transferred without additional, meaning that it considers that the third country in question ensures an 'adequate' level of data protection. Understanding the potential impact of such rulings is the responsibility of business both in the UK and the EU and it should be undertaken immediately.

# CLOUD COMPUTING

A decade ago cloud computing was in its infancy, even the term cloud had not become synonymous with the technology we think of now. Terms such as internet as a platform, computing on demand, applications as a service or what is now a subset of the cloud software as a service were all terms being used to describe what we would now know as cloud computing. And for once a Gartner prediction, that cloud computing would be as influential as e-commerce, has proven to be accurate. Only 6 per cent of respondents said they had no significant systems in the cloud. The ubiquity of cloud computing could lead one to believe that everything is now delivered from the cloud but anyone working in IT knows that there are many workloads that are not suited for the cloud and that on premises is sometimes the only way to provide the performance, security and service levels demanded by the business and its users.

In the survey, 48 per cent of respondents said they had workloads that couldn't or wouldn't move to the cloud. This has resulted in many hybrid deployments, some through choice and some through necessity. 21 per cent said they hadn't moved specific workloads and data to the cloud because of security. While it is reasonable to say that cloud solutions, including public cloud, offer higher levels of security than can be reasonably achieved by a small and medium-sized business, the same is not true of more sophisticated enterprise setups managed by teams of experienced engineers. And when there is a data breach on a cloud based system, whether that be LinkedIn or Yahoo, the argument for in-house systems that can be controlled and monitored gains strength. While in some organisations the requirement for data to remain in-house may be for compliance issues for many others it is through choice. Governments, security contractors and financial organisations all use the cloud but the maturing of the reality of the cloud means that organisations now have realistic expectations of what can be delivered by what platform.

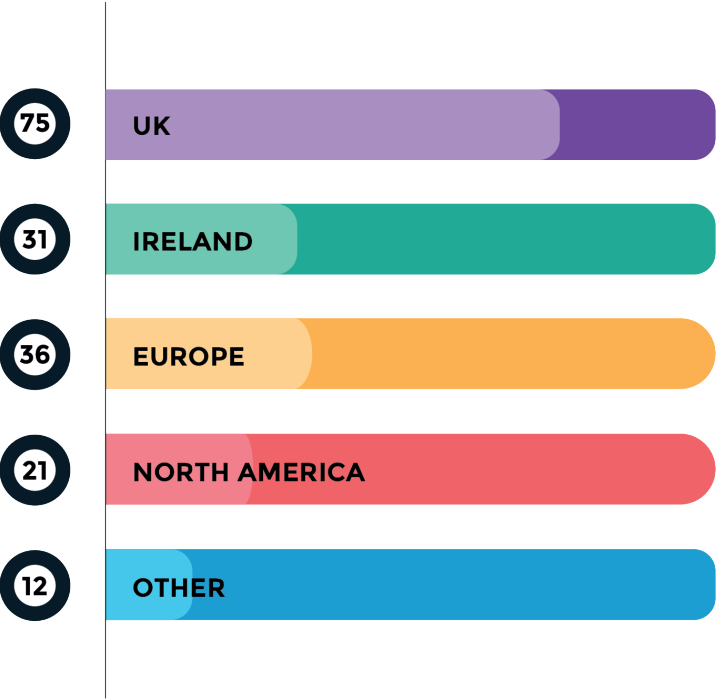


## Reasons for problems moving applications to the cloud

For many, keeping services running in-house is not a choice but a result of the complexity of moving the applications. 44 per cent of respondents said that this is the reason why they are still running systems in-house and 38% said that the vendors did not provide enough support to help them move these legacy applications. Anyone who has tried packaging applications for the cloud will have come across things that should on paper work but they simply do not run in the new environment.

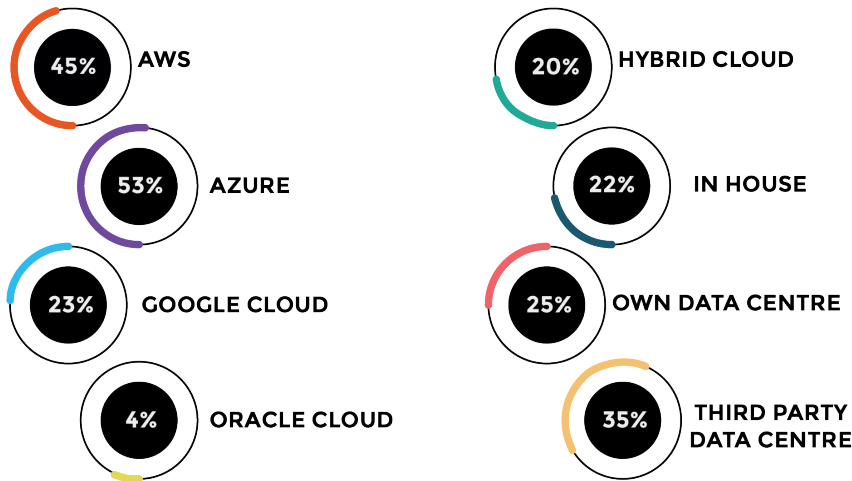
There are solutions that use machine learning to analyse and identify the code that is stopping the application to be migrated but for many teams, this is added complexity and cost that they do not have the appetite to indulge. Companies running legacy applications, that are often no longer supported and patched by the vendors are running risk of failures and security breaches, it is not uncommon to find an almost fabled server that hasn't been switched off since 2005 because it's running a service still used by someone in a company and the IT team are not confident in ever getting it working again if they tried to move it.

Earlier in this analysis, we raised the potential issue of data sovereignty. 75 per cent of respondents have hosting within the UK, 36 per cent within Europe and 32 per cent specifically in Ireland. As a part of Brexit preparedness, companies should look at where their hosting is and access whether it is potentially at risk of causing disruption to their business and their customers in the event of a no deal Brexit.



Cloud service hosting locations

Over the past year, Microsoft has gained market share for cloud services. Our survey showed that 53 per cent of companies are now utilising Azure, slightly ahead of AWS at 46% and Google at 23 per cent. Globally the overall market share of AWS has dropped by 8 per cent and Azure has 20 per cent usage. Many organisations are using more than one cloud provider and have looked at what workloads are best placed for which platform, with many using traditional colocation or in-house data centres as well. 46 per cent of respondents host some services in-house and 36 per cent use third-party data centres.



With the hybrid approach being very common, we asked how companies were connecting to the cloud services they use. Over half, 51 per cent, are using the public internet. This is used typically to connect to software as a service applications such as Salesforce, rather than core systems. 67 per cent of organisations are using VPNs and 29 per cent of companies have adopted direct connections to provide lower latency and higher levels of security.

Ten years after the adoption of the term cloud computing, the adoption of cloud services has overcome much of the original resistance and fear and it could be said that it has surpassed the expectations of all but the most evangelical of cloud enthusiasts. Only 3 per cent of respondents were dissatisfied with the outcomes of moving their services to the cloud, with the majority satisfied and 36 per cent very satisfied. During this decade the quality of these services has addressed many concerns and it has brought things such as geographic diversity into the reach of a wider audience. The arrival of AI as a service based on cloud platforms is an example of the next phase of cloud adoption, opening up services to businesses of all sizes. Cloud computing has now been accepted and will be used as the basis for many of the new wave of technology that business will be adopting over the next decade that would not or could not exist without the cloud.

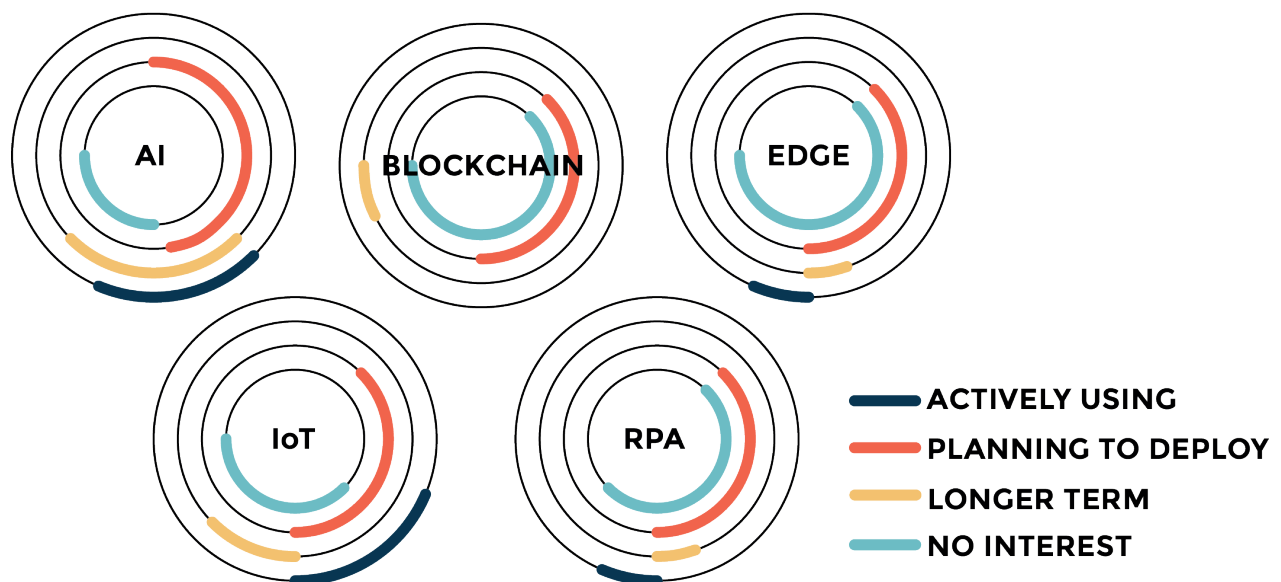
***“We are moving into a post cloud hype world when people recognise its not a panacea”***

**Pete Hulme Dimension Data**

# EMERGING TECHNOLOGIES

The technology landscape is forever changing, cloud computing and smartphones were emerging technologies a decade ago and now working without them is almost unimaginable. There are many more new technologies that in ten years' time may have found their way into almost every business and home, such as virtual and augmented reality but in the survey we looked at five technologies that are already seeing adoption and looked at their use and planned use in British business.

These technologies are Artificial Intelligence (AI), Blockchain, Edge computing, Internet of Things (IoT) and Robotic Process Automation (RPA).



Artificial Intelligence and Robotic Process Automation often go hand in hand. Businesses are increasingly looking to drive efficiencies across their organisations, to make better and faster decisions and reduce costs. 16% of the respondents had already started to adopt AI, with a further 19% looking to adopt it within the next year. Currently the UK is amongst the world leaders in AI with established companies such as QuantumBlack and start ups like Mindtrace providing real world solutions. The government recognises what could be a £232 billion boost for the British economy by 2030. The AI Sector Deal offers a fresh package of almost £1 billion in support of the sector, including new government, industry and academic contributions up to £603 million, up to £342 million from existing budgets, and £250 million for connected and autonomous vehicles. It also aims to invest £400 million into maths, digital and technical education to address the shortage of STEM skills.



Robotic Process Automation is already commonplace within the financial sector where there are large volumes of rule-based data processing to handle. Previously much of this work was offshored but with RPA's lower costs, faster speed and higher accuracy rates, this work is being brought back onshore and handled by RPA with small teams handling the exceptions. RPA was already being used by 11 per cent of respondents with a further 36 per cent planning to adopt it in the future. RPA and AI could become real challengers for people's jobs. Initially, RPA will replace low-value repetitive actions and free workers to provide high-value work for their organisation but AI will also start to replace historically middle-class jobs and that will bring its own challenges. London based Babalyon Health, who run on Azure, already have an AI triage service that is more accurate than a GP being used by 30,000 patients. Automation will come at a cost but it will come and the businesses that fail to adopt it will not be as competitive putting at risk more jobs than the technology itself.

Blockchain, especially its use in cryptocurrency has been a big story over the last year with smart investors achieving returns many times their investments, and FEWER smart investors losing a lot of money. The survey found that while there is a lot of interest, blockchain has yet to be adopted by a single respondent outside of their personal use of cryptocurrency. 35 per cent of companies said they were looking at it as a long-term solution but only 4 per cent had identified where they would be using it in their business in the next twelve months. The most common application for blockchain, identified, has been in supply chain management but there are many others being developed; Kodak has announced a blockchain based service for photography licencing to ensure that the original photographer is credited for their work and paid. It is this sort of problem-solving that will drive adoption of blockchain, while many for now still see it as a solution to a problem that does not exist.

Edge computing is usually referred to in IoT use cases, where edge devices collect data and send it to a data centre or cloud for processing. Edge computing triages the data locally so some of it is processed locally, reducing the backhaul traffic to the central repository and providing real-time information. In industry these devices are typically the machines themselves, enabling IoT to provide its true potential. 9 per cent of the respondents have adopted edge computing into their infrastructure with a further 6 per cent looking to do it within the next year and 30 per cent considering it for the future. As with all technologies here, edge computing is enabled by the cloud and the real value comes when used with the other technologies such as AI based machine learning.

The Internet of Things is more than a connected fridge telling you are out of milk and ordering it for you. In business, it is already adopted by 20 per cent of the respondents and a further 32 per cent looking to deploy it within the next year. We have mentioned its use with industrial machinery, for example, feeding back diagnostic information on an oil rig in the North Sea, but it can be used to track production, in supply chain management, track assets, provide real-time information to help financial decisions and improve the customer experience. Heavy equipment manufacturer Caterpillar, for example, is transforming its business by incorporating the IoT.

Over the past decade, the company has been outfitting its equipment with sensors and embedded connectivity. Today, almost everything Caterpillar produces, from trains and industrial generators to construction and mining equipment, can measure and communicate critical data. As a result, over 560,000 Caterpillar vehicles now collect and transmit data to their owners. This can help prioritise preventative maintenance and keep businesses running.


Transport and logistics company Eddie Stobart has adopted IoT to monitor its 2,200 vehicles, 3,800 trailers and 24 distribution centres across the UK and Europe, providing real-time information that keeps its business on the road.

Innovate UK, a non-departmental public office, has stated it is investing up to £20 million into emerging technology projects. It has already awarded £248,000 to a blockchain start-up developing a cross-border financial transaction tool. This investment could mitigate the risk for enterprise organisations in adopting solutions from small unknown companies. Securing the backing of larger organisations such as the government is vital in this. The importance and potential disruptive impact of these technologies have been recognised by many governmental entities in the UK, in particular, the All Party Parliamentary Group on Blockchain which was set up January 2018.

These emerging technologies have the power to transform businesses and British business has been adopting them to gain an advantage. But there is a real risk that this may not continue because of a skills shortage. 69 per cent of respondents felt they did not have the skills in-house to take full advantage of these technologies. Companies can be reluctant to spend significant sums on training only to have people leave after gaining experience on one project. Vendors have a part to play in this. Smart vendors realise that if there are more engineers skilled up to deliver their projects the cost per engineer will be lower and the project will be delivered faster making their solution more attractive. This approach is being used by some RPA vendors to challenge BluePrism's dominance by providing free training to engineers and the end user companies as well as deskilling the deployment by making it drag and drop rather than coding.

***“By harnessing clear domestic strengths in pure and applied science – by combining existing technologies as well as innovating from scratch – we can position the UK at the forefront of new markets, industries and delivery models.”***

***Jo Johnson UK Government***



IT can be complex. It's an ever changing world, with new technologies, new regulations and new threats. At **Serviceteam IT**, we love it. (This can make us a little boring at parties).

Ask us about the latest cyber-security trends, the challenges of data sovereignty or low latency connectivity, and we'll put the kettle on and open the biscuits.

Every company promises great service, few consistently achieve it.

At Serviceteam IT we strive always to be honest, transparent and personable at a price which is fair. Our professional team will work hard to bring you the benefit of their knowledge and experience, and our flexible, can-do approach means nothing is impossible if your pockets are deep enough. We're not the biggest, but our clients trust us, and believe we are one of the good ones.

0121 468 0101 [www.serviceteamit.co.uk](http://www.serviceteamit.co.uk) [info@serviceteamit.co.uk](mailto:info@serviceteamit.co.uk) [@serviceteamit](https://twitter.com/serviceteamit)

49 Frederick Road Edgbaston Birmingham B15 1HN

**Doogheno.com**

Working with technology companies to bring their stories to new customers.