UK CLOUD SNAPSHOT SURVEY 2017

ANALYSIS

Dan Smith
doogheno

serviceteamit

Cloud Snap Shot Summer 2017

The adoption of cloud has been rapid and its use has enabled traditional businesses to fast transform into digital businesses. In ten years cloud has gone from managing limited workloads for early adoptors to running extremely large and complex workloads over many geographic regions. In February 2017 the Cloud Industry Forum survey reported that cloud adoption rate for UK businesses had reached 88%, with the majority, 68% using hybrid clouds (Mcafee 2017).

However these are just broad, headline figures. To get a true picture of the status of cloud adoption in the UK across multiple industries we carried out a combination of in-depth interviews and a large sample survey. The Cloud Snapshot Survey was completed over a four-week period between the 14th of July and the 11th of August 2017. The sample size of over 1,100 people responsible for IT decisionmaking ensured that valuable and insightful information was collected.

We asked about challenges, current infrastructure and services and plans for the next 36 months. This report looks at the answers we received and explores the impact of external challenges that businesses face in 2017 and beyond, such as Brexit, GDPR and the rise of cyber-crime.

We examine the impact of the uncertainty surrounding Brexit. While the Government begins to plan and negotiate, the much-repeated comment by the Secretary of State for Exiting the European Union, David Davis, "Clearly there's a lot left to talk about" seems increasingly to have been a huge understatement.

The introduction of GDPR will not have escaped the notice of any IT or business management professional. It replaces the 1998 Data Protection Act, and updates the legislation to make it more fit for purpose in our digital world. Giving people more control over how data about them is held and businesses a clearer understanding of what their responsibilities are is ultimately the goal but there is a lot of work to do to get there.

"We're all going to have to change how we think about data protection." Elizabeth Denham Information Commissioner

UK businesses face an unprecedented level of threat from cyber-security attacks. The new National Cyber-Security Centre (NCSC) contended with 480 major incidents in its first 8 months of operation, from global ransomware outbreaks to smaller breaches at British businesses. And the pace shows no sign of slowing.

"No longer the stuff of spy thrillers and action movies, cyber-attacks are a reality and they are happening now. Our adversaries are varied – organised criminal groups, 'hacktivists', untrained teenagers and foreign states." Ben Gummer Cabinet Office

The results of the survey and our conversations give a snap shot into cloud adoption in the UK in the summer of 2017.

We asked initially about external factors affecting IT strategy. Responses showed that the top three concerns were GDPR, Brexit and the increase in cyber crime.

General Data Protection Regulation (GDPR) is clearly the largest external focus for companies in the lead up to its introduction in 2018. The survey showed that it was the largest single external influencing factor for 62% of respondents.

GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. The Regulation mandates considerably tougher penalties than the current Data Protection Act, organisations found in breach of the Regulation can expect administrative fines of up to 4% of annual global turnover or €20 million – whichever is greater. Fines of this scale could very easily lead to business insolvency. Data breaches are commonplace and increase in scale and severity every day. As Verizon's 2016 Data Breach Investigations Report reaffirms, "no locale, industry or organization is bulletproof when it comes to the compromise of data", so it is vital that all organisations are aware of their new obligations so that they can prepare accordingly.

GDPR replaces the Data Protection Act of 1998. The digital landscape in 1998 was a completely different. Pre-Google, we searched the internet using Yahoo, Lycos, or AltaVista from our Netscape or Internet Explorer browsers. Social media didn't exist as we understand it today, was limited to the likes of Geocities, and only 20% of people had been online in the last 12 months. GDPR makes data security fit for purpose in our digital world of 2017 and beyond.

The GDPR changes the historic understanding of what data privacy and data security compliance mean. No longer is it purely a checklist ticking exercise. Now the journey to compliance is more risk management focused. Risk calculations and appropriate privacy protections, as well as data security, are up front and central in all aspects of personal data management.

The GDPR places onerous accountability obligations on data controllers to demonstrate compliance. This includes requiring them to: (i) maintain certain documentation, (ii) conduct a data protection impact assessment for riskier processing, and (iii) implement data protection by design and by default, e.g. data minimisation.

GDPR needs to cover technology, process and policy and needs buy in and sponsorship from the senior management in all companies.

"The General Data Protection Regulation (GDPR) is the biggest change to data protection law in a generation." "I see this as good news for the UK. One of the key drivers for data protection change is the importance

Data breaches are commonplace and increase in scale and severity every day. As Verizon's 2016 Data Breach Investigations Report reaffirms, "no locale, industry or organization is bulletproof when it comes to the compromise of data", so it is vital that all organisations are aware of their new obligations so that they can prepare accordingly.

and continuing evolution of the digital economy in the UK and around the world. That is why both the ICO and UK government have pushed for reform of the EU law for several years...The digital economy is primarily built upon the collection and exchange of data, including large amounts of personal data – much of it sensitive. Growth in the digital economy requires public confidence in the protection of this information." Elizabeth Denham Information Commissioner

While 6% of companies believe that Brexit will halt GDPR, the government has made it very clear that GDPR will be adopted fully and will remain law after Brexit.

"The GDPR introduces obligations for data controllers and processors in several areas," minister of state for digital and culture Matt Hancock told the House of Lords EU Home Affairs Sub-Committee on 1 February.

"It strengthens the rules for obtaining consent. It strengthens the need for breach notifications and it emphasises self-assessment in the management of data. We have said that the UK is going to implement GDPR in full, and there's two reasons for that.

"The first is because that thanks to some significant negotiating successes during its development we think that it is a good piece of legislation in and of itself. That's the first thing.

"And the second is we are keen to secure the unhindered flow of data between the UK and the EU post-Brexit, and we think that signing up to the GDPR data protection rules is an important part of helping to deliver that"

GDPR is seen in most companies as an IT department issue but in companies of over 250 employees, a Data Protection Officer is required as a part of the incoming regulation.

The effects of GDPR on an organisation will largely depend on their existing data policies. Many companies have not had to pay too much attention to this area before outside of the general good business practice processes. However, GDPR changes this, not just because of the risk of heavy fines but also because it will make customers more aware of the rights that they have to see what data is being held and find out how that data is going to be used. In a July poll by SAS of over 2,000 people 64% welcomed 'the right to access' (e.g. get a copy of personal data held about them) with the 45- to 54-year-old age group is most likely to issue a request, with just over one in five (21%) thinking they will activate their new rights in the first month. That figure may be a shock to many companies who believe they can continue as they have been up until now.

Many companies have disparate systems that have grown up over years through expansion, acquisition and mergers and they simply do not know where all the data is stored. The impact of such an issue on IT is not being ignored by most companies with a large slice of companies' IT budgets being allocated to data storage projects to address this very issue.

Many companies have disparate systems that have grown up over years through expansion, acquisition and mergers and they simply do not know where all the data is stored.

For other companies that provide services to third party companies, there is the additional challenge of complying to other companies interpretations of GDPR, this could result in running completely separate storage and retention policies for these sets of data.

The focus on GDPR was found to be universal across all the verticals that were surveyed. With the volume of information about GDPR and implementing process policies and technology to ensure that a company is compliant, most companies are already a long way down the road in their process of becoming compliant. Nearly every respondent to the survey stated that they felt that they would be compliant by the 25th of May, 2018. However, this positive information must be tempered with the results of a Veritas survey that showed just under one-third (31%) are worried about reputational damage from poor data policies.

The new National Cyber-Security Centre (NCSC) contended with 480 major incidents in its first 8 months, from global ransomware outbreaks to smaller breaches at British businesses, and the pace shows no sign of slowing.

Cyber-security

UK business, infrastructure and government face an unprecedented level of threat from cyber-security attacks. The new National Cyber-Security Centre (NCSC) contended with 480 major incidents in its first 8 months, from global ransomware outbreaks to smaller breaches at British businesses, and the pace shows no sign of slowing.

Over 1/3 (34.3%) of the respondents said they had experienced an increase in cyber-attacks, also reporting that the nature of these incidents had changed. Attempts to encrypt data and charge a ransom had been experienced by many of the respondents. When asked about barriers to further cloud adoption the biggest response was security at 45%.

Cyber-security is now a significant priority for the British government.

"*This increase in major attacks is mainly being driven by the fact that cyber-attack tools are becoming more readily available, in combination with a growing willingness to use them*,"

John Noble, a Director of Incident Management NCSC

The NCSC director also revealed 451 incidents the agency responded to were lower level attacks typically related to a single organisation. However, 29 were classified as C2-level attacks, demanding more attention alongside a "cross-government" response.

The most prominent incident which almost triggered a top-level (C1) attack was WannaCry, a ransomware pandemic that spread to hundreds of thousands of unpatched computers in more than 150 countries in May. In the UK, it caused widespread disruption at the National Health Service (NHS).

In The first month of operation, the NSSC responded to 70 hacking incidents, 10% of which included ransomware.

Earlier this year the NCSC revealed the UK was being hit with around 60 significant cyber-attacks every month. Ciaran Martin, head of the NCSC, told The Sunday Times some of the incidents involved state-sponsored hackers targeting political institutions.

"There has been a step change in Russian aggression in cyberspace," he said at the time. "Part of that step change has been a series of attacks on political institutions, political parties, parliamentary organisations and that's all very well evidenced by our international partners."

In August 2017 the Government announced that British organisations could face fines of up to £17m, or 4% of global turnover if they fail to take measures to prevent cyber-attacks that could result in major disruption to services such as transport, health or electricity networks.

In August 2017 the Government announced that British organisations could face fines of up to £17m, or 4% of global turnover if they fail to take measures to prevent cyber-attacks that could result in major disruption to services such as transport, health or electricity networks.

The digital and culture minister, Matt Hancock, said: "We want the UK to be the safest place in the world to live and be online, with our essential services and infrastructure prepared for the increased risk of cyber-attack and more resilient against other threats such as power failures and environmental hazards."

The Department for Digital, Culture, Media and Sport said it also wanted to see action to detect attacks, develop security monitoring and raise staff awareness, as well as ensuring incidents were reported immediately and that systems were in place for recovery. Workshops will be held where organisations can give feedback.

The consultation is on the Network and Information Systems directive to be implemented from Spring 2018, which is part of a £1.9bn national cyber-security strategy.

The Department for Digital, Culture, Media and Sport said it also wanted to see action develop security monitoring to detect attacks, and raise awareness, as well as ensuring any incidents are reported immediately and that systems were in place for recovery.

Ciaran Martin, the chief executive of the National Cyber-Security Centre, said organisations needed to do more to increase cyber-security. "*The NCSC is committed to making the UK the safest place in the world to live and do business online, but we can't do this alone,*" he said. *"Everyone has a part to play and that's why since our launch we have been offering organisations expert advice on our website and the government's Cyber Essentials Scheme.*"

The threat is real and it isn't just an IT problem causing minor disruption. The financial impact is vast. A study conducted by Oxford Economics found that companies' share prices fall by an average of 1.8% on a permanent basis following a severe data breach.

This means a typical FTSE 100 firm is worse off by an average of £120m after a breach, according to the study. It looked at 315 breach events with a focus on 65 "severe" and "catastrophic" breaches occurring since 2013 across seven global stock exchanges. The analysis showed that investors have lost at least £42bn due to severe public domain cyber-security incidents since 2013.

"*Once a breach has occurred, the clock is ticking and a business will only have a short period of time to instruct cyber specialists, lawyers, PR managers and insurers, while at the same time react to fulfil its regulatory obligations and position itself in the best way possible to respond to, and mitigate any potential regulatory investigation and media scrutiny,*" Andrew Gilchrist, a senior associate at international law firm K&L Gates LLP *"Experience shows us that the real threat to UK businesses is not necessarily a fine from the Information Commissioner's Office (ICO). This is a drop in the ocean compared to the bad press and loss of customer confidence that often follows a cyber-hack."*

The idea of cyber-crime being carried out by script kiddies in hoodies has been replaced by criminal groups attacking financial institutions and state sponsored cyber-attacks with the potential to influence elections.

Cyber-security threats will have an impact on every business, whether they are an organisation that has carried out a full digital transformation program or they are just a small business with online banking. The threats are varied and adaptable. They range from high volume, opportunistic attacks where technical expertise is bought, not learned, such as DDOS attacks to highly sophisticated threats involving bespoke malware created to compromise specific targets.

The idea of cyber-crime being carried out by script kiddies in hoodies has been replaced by criminal groups attacking financial institutions and state sponsored cyber-attacks with the potential to influence elections.

The past year has seen cyber-attacks on a scale and boldness we have not seen before. These include the largest recorded cyber heist, the largest DDoS attack and the biggest data breach ever being revealed. And the attacks on the Democratic National Party, Ukrainian energy infrastructure and Bangladesh Bank demonstrate that no organisation is safe.

The Effects of Brexit

The only thing we can be sure of with Brexit is that we cannot be sure of anything.

The predicted immediate economic slump has not materialised but there are growing signs that the uncertainty around Brexit is having a detrimental effect on UK business.

Brexit was identified as the third most pressing issue for respondents to the survey after GDPR and cyber-security. Brexit will have no impact on GDPR as all existing laws as of March 2019 will become UK laws.

We will not attempt to address the rights and wrongs of Brexit here or make predictions but we will simply look at the business sentiment and evidence as it stands now. It is hard to find neutral authoritative data or comment on this matter, however we have tried to keep this factual and balanced.

The UK is still in Europe and nothing has changed since Theresa May triggered Article 50 in March. As of the end of August, the Government has published 5 position papers to ensure that trade of goods and services can continue after March in 2019. These proposals have been welcomed by business with CBI saying that position on trade was a "significant improvement" on EU proposals that would create a "severe cliff edge".

At this point, there is little other clarification of the British Government position or that of the EU member states. And there lies that biggest problem, for it is uncertainty that stops businesses taking risks, it is uncertainty that holds back investment and it is uncertainty that favours the sentiment that much of business relies upon.

And the Chancellor Philip Hammond said "It is absolutely clear businesses where they have discretion over investment, where they can hold off, are doing so - you can understand why. They are waiting for more clarity about what the future relationship with Europe will look like"

"UK businesses need to know soon what arrangements will be in place after March 2019, to be able to plan, make investment decisions and have confidence that an orderly and carefully managed approach to Brexit is under way, if they don't have that assurance there will come a tipping point, sometime in 2018, when boards in the UK and elsewhere will need to make decisions based on the state of the negotiations at that point." Engineering Employers' Federation chief executive Terry Scuoler

Companies are reluctant to make new hires according to UK largest recruitment firm Hayes:

"*There is no long-term investment in any of the sectors, People are very focused on the next 18 months until we get some sort of clarity.*"

And the Chancellor Philip Hammond said "It is absolutely clear businesses where they have discretion over investment, where they can hold off, are doing so - you can understand why. They are waiting for more clarity about what the future relationship with Europe will look like"

However, we have not fallen off that cliff edge yet.

On 5 January 2017, Andy Haldane, the Chief Economist and the Executive Director of Monetary Analysis and Statistics at the Bank of England, admitted that forecasts predicting an economic downturn due to the referendum were inaccurate and noted strong market performance after the referendum.

And business has to continue, companies cannot and will not stand still for the next two years. Some companies see Brexit as an opportunity, some as a real threat.

Removing all trade tariffs and barriers would help generate an annual £135bn uplift to the UK economy, according to a group of pro-Brexit economists. A "hard" Brexit is "economically much superior to soft", according to Professor Patrick Minford, the lead author of a report from Economists for Free Trade. He says eliminating tariffs, either within free trade deals or unilaterally, would deliver huge gains. The report - Project Fear to Project Prosperity, is due to be published in the autumn. Minford argues that the UK could unilaterally eliminate trade barriers for both the EU and the rest of the world and reap trade gains worth £80bn a year. The report foresees a further £40bn a year boost from deregulating the economy, as well as other benefits resulting from Brexit-related policies.

This is not a view universally shared.

Other economists say cutting barriers sets off a "race to the bottom".

Economist Dr Monique Ebell from the National Institute of Social and Economic Research (NIESR) says Prof Minford "ignores decades of evidence on how trade actually works".

So while the economic impact is still very much unknown we do know that business regulations will remain the same, at least for the foreseeable future as a result of the Great Repeal Act and the biggest impact of legislation, GDPR will be enshrined into UK law.

And one more thing that we can be fairly clear about is that Brexit will have an impact on data sovereignty, with only 37% believing that it will have no impact. It is possible that the UK could impose rules similar to those that exist in Germany, stating that data must be held within the UK currently, for example. The law stipulates a number of things, such as the need to have data stored in the UK if it is financially sensitive. A survey from Vanson Bourne backs up our own findings suggesting that 86% of respondents felt it was important to locate their data in the UK. And in the Autumn of 2016 a 4D survey found 63% said Brexit has intensified their concerns surrounding data location and sovereignty even further.

Sovereignty of data is of great importance to all businesses, primarily because the laws governing access rights differ greatly from country to country. A good example of this is the United States where access to data held in country, even if stored by an international business, can be freely gained by federal agencies through their Patriot Act.

Amazon, Microsoft and Google have all opened UK data centres for their cloud offerings and while they say this is to serve local markets better it also helps UK businesses after Brexit with data sovereignty.

So while the economic impact is still very much unknown we do know that business regulations will remain the same, at least for the foreseeable future as a result of the Great Repeal Act and the biggest impact of legislation, GDPR will be enshrined into UK law.

We asked about cloud platforms and the services and applications being delivered.

The survey asked what platforms were being used for delivery of cloud based solutions, and the responses supported the belief that most UK companies are working with a hybrid cloud approach and with multiple vendors, in combination with in house data centres.

63% of respondents have in house data centre or hosting resource that makes up an element of their cloud solutions. These include legacy systems as well as the strategic deployment of hardware. The interviews showed divided opinion about in house hosting, with an even split between those who believe that data is always going to be more secure if it is directly under their control and those who feel that large scale platform providers have a level of resource that results in a higher level of security than can ever be delivered in house.

It is estimated that around 60% of organisations globally have adopted either Office 365 or Google apps.

Half of the respondents use third party data centres for collocation of server and network equipment.

38% of companies are utilising Amazon AWS closely followed by Microsoft Azure at 36%, Google cloud was down at just 12%. The battle of the large scale platforms is hotting up, the Microsoft Azure share of the market is growing at a rate faster than AWS but is safe to say that currently, globally AWS has the largest market share at around 40%, with Azure, Google and IBM making up just 23% combined (Synergy Research Group)

In April 2017 Amazon, Microsoft and Alphabet all reported quarterly results on the same day. Amazon was the only company to present clear numbers for its infrastructure business showing an annualised run rate of $14.6 billion. Microsoft bundles its Azure business into the Intelligent Cloud division, which includes various other servers and cloud services. In total, that business grew 11% to $6.8 billion. While Microsoft does not split out Azure's revenue, it does give a growth number. In the quarter ended March 2017, sales increased by 93%. Giving Microsoft a Commercial Cloud business with annualised revenue of $15.2 billion, including Office 365 and not just the Azure infrastructure service. Alphabet did not provide a figure for the Google Cloud Platform, including it only in the $3.1 billion figure left after removing advertising revenue from their $24.5 billion quarter. Other providers of cloud platforms such as HPE Helion and Oracle Cloud made up 9% of the total cloud platform used by the survey respondents.

We sought to discover which applications were being used on these platforms and also which applications were provided in the cloud model. As the survey did not cover areas such as farming or manufacturing and most responses to the survey were companies with largely office based staff it is not surprising that most of the companies said that they used cloud based productivity tools such as Microsoft Office 365 or Google Apps. 77% of respondents said they used either one or both of the productivity suites. It is estimated that around 60% of organisations globally have adopted either Office 365 or Google apps and according to Gartner, the split between enterprise adoption of Office 365 over Google apps

is around 2:1. There is crossover between companies who use both sets of productivity applications, due to third party application integrations and avoidance of disruptive change within a base that is familiar with certain products.

With storage costs being as low as $0.02 per GB per month most companies are utilising cloud based platforms for storage. With increasing consolidation and projects to simplify data policies in a post-GDPR Britain the use of cloud based storage will only increase. 60% of responding companies said they used cloud based storage. Security concerns over safeguarding stakeholders' information and private data majorly restrains the cloud storage deployment in certain verticals but for most small to mid-sized businesses, the cost benefits outweigh some of those concerns. Storage is a large part of the hybrid solutions used by many companies. Services such as Microsoft OneDrive, Dropbox and Google Drive were not included in the answers to this question.

56% of companies use databases on cloud platforms. These combine the benefits of running a database on a VM or database as a service (DBaaS) such as Amazon Relational Database Service or Microsoft Azure SQL Database. The global DBaaS market is highly fragmented due to the presence of many large and small vendors. Cloud-based Database market size is predicted to maintain the average annual growth rate of 24% as companies move an increasing amount of databases to the cloud to benefit from the relative simplicity of deploying resilient data base services.

Legacy security solutions are no longer as effective at providing protection, and on-premises hardware often lacks the sufficient scale and performance to protect Internet-facing application infrastructure as it grows.

Legacy security solutions are no longer as effective at providing protection, and on-premises hardware often lacks the sufficient scale and performance to protect Internet-facing application infrastructure as it grows. Over 1/3 (37%) of companies responding to the survey have adopted cloud based security services such as Multi-Factor Authentication and Single Sign-On. Cloud security providers typically have greater visibility of attacks and attack patterns than any individual company. They make real time threat intelligence available as well as threat updates to companies, including through improved web application firewall rules, new attack signatures, customer-facing threat advisories and better internal response processes. By defending against attacks directed at multiple organizations, cloud security providers develop significant expertise and experience, on which they can draw when mitigating future attacks to help reduce customer impact and the time to resolve the instance.

The promise of business insight from Big Data through quality analytics is now a reality in most businesses. Cloud analytics is a service model in which elements of the data analytics process are provided through a public or private cloud and it has been adopted by a third of the survey respondents. Gartner defines the six key elements of analytics as data sources, data models, processing applications, computing power, analytic models and sharing or storage of results. Gartner states that any analytics initiative "in which one or more of these elements is implemented in the cloud" qualifies as cloud analytics. From Oracle to Microsoft Power BI it is clear that the use of cloud analytics will grow larger over the coming year.

Part of the consumerization of the enterprise is the adoption of enterprise grade cloud applications such as Oracle and Salesforce.com. One large change that has been observed over the past year is a growth in consumption of enterprise cloud applications. There has been an increase in both the number of applications moving to the public cloud marketplace as well as increasing the ease of consumption of these enterprise cloud applications. In the past, enterprises needed to open up conversations with the vendors, complete an RFP process and then work through the process to select and deploy an enterprise software solution. Today, an organization can go to a public cloud marketplace and, with just a few clicks, spin up an instance of Microsoft Dynamics, SharePoint or other business applications. Overall 35% of respondents said they were using cloud based enterprise applications, in the Scientific research section this was nearly every company, however, in the insurance sector, it was just 14% of the respondents, this may reflect the more traditional nature of the insurance markets.

In the past, enterprises needed to open up conversations with the vendors, complete an RFP process and then work through the process to select and deploy an enterprise software solution. Today, an organization can go to a public cloud marketplace and, with just a few clicks, spin up an instance of Microsoft Dynamics.

Managing the public cloud estate, hybrid estate or enterprise applications requires the use of cloud based management tools such as Amazon CloudWatch, CA Unified Infrastructure Management or Cisco CloudCenter (formerly CliQr). Other smaller companies have arrived to provide cloud management services such as Cloud Ranger and Dynatrace. Some of these are very powerful and very easy to adopt. Nearly a quarter (23%) singled out cloud management tools as a key application they use across their platforms as they give them far greater visibility and control over their infrastructure than could be achieved in traditional computing.

Cloud may be the heart of many companies' infrastructure but it would be nothing without the veins of connectivity that keep the data flowing. The survey asked what connectivity companies use to access their cloud solutions. This was split out from their normal office connectivity unless they relied on an open public cloud connection.

40% of respondents use VPNs. VPNs are quick and simple to deploy and can encompass remote sites and users as well as the main corporate location connecting through encrypted tunnels to the cloud infrastructure, or connecting two separate cloud platforms. Nearly a third (32%) use the public internet. This is mainly being used for cloud based applications such as Salesforce.com CRM rather than accessing corporate infrastructures. The use of the public internet could also be the cause for some of the reported concerns regarding the security of the cloud and latency. 28% use direct connections such as Microsoft Azure Express Route and AWS Direct Connect. Direct connections provide a more

secure solution to cloud access and can deliver lower latency. Often direct connections are perceived as more complex to set up and less flexible than VPNs, however, this is no longer the case and they can also offer higher bandwidth for a lower cost. The direct connection use will grow as more companies understand the technical, operational and cost benefits.

We asked where the data centres were.

Over two thirds (69%) of the companies surveyed had data centres in two or more countries.

Over two thirds (69%) of the companies surveyed had data centres in two or more countries. 71% of the companies have data centres within the UK. These include hosting in house and third party data centres. Nearly two thirds (63%) hosting in Europe with 32% hosting in Ireland. The location of the data centre is still largely dictated by the speed of traffic back to the users and Ireland has offered local options for UK businesses before Amazon, Microsoft and Google opened up UK data centres. 26% of companies said they used North American data centres and 2 % said they used data centres in Asia Pacific.

The issue of data location will become more relevant after Brexit, while initially, we will continue to host in Europe it is very possible that the UK adopts a German style data hosting policy regulated by the Federal Data Protection Act which is more stringent than the European wide laws. While companies can host elsewhere it is easier to comply by hosting in Germany, boosting German digital economy. The companies were asked if they felt that Brexit would introduce data sovereignty issues. Just over a third (37%) said no. 21% said they believed that it would cause data sovereignty issues but the largest group 42% were unsure. Again this is another example of the uncertainty around Brexit and its knock on effects to IT operations and planning.

However, in the Governments Position paper published at the end of August, it is indicated that the intention would be to maintain the current arrangements.

"Estimates suggest that around 43 % of all large EU digital companies are started in the UK, and that 75 % of the UK's cross-border data flows are with EU countries. Analysis indicates that the UK has the largest internet economy as average of GDP of all the G20 countries...

...Any disruption in cross-border data flows would, therefore, be economically costly to both the UK and the EU. Taking EU-US data flows as a comparator, external estimates suggest that if cross-border data flows between the EU and the US were seriously disrupted, the EU's GDP could reduce by between 0.8 and 1.3 %. Therefore, placing restrictions on cross-border data flows could harm both the economies of the countries implementing these policies, as well as others in the global economy...

As well as ensuring that data flows between the UK and the EU can continue freely, the UK also wants to make sure that flows of data between the UK and third countries with existing EU adequacy decisions can continue on the same basis after the UK's withdrawal, given such transfers could conceivably include EU data. The UK is, and will remain

after the point of withdrawal, a safe destination for personal data with some of the strongest domestic data protection standards in the world. For this reason, the UK does not see any reason for existing data flows from third countries to the UK to be interrupted.

The UK will liaise with those third countries to ensure that existing arrangements will be transitioned over at the point of exit…"

The large providers are however securing their position no matter what happens.

Amazon, Microsoft and Google have all opened UK facilities. Amazon opened its first of five UK data centres in London in December 2016. Microsoft who have data centres in Cardiff and London have used these to secure government contracts such as providing Parliament with Office 365 and the Metropolitan Police. And while it has been reported that a big factor in the move to the UK for Google was being able to offer customers assurances over data sovereignty when Brexit finally happens, Google denied this.

The spokesman said the decision to open the "region" was not caused by the Brexit vote to leave the EU in June 2016 because it "had been taken well before the Brexit vote".

In March 2017 the Cloud Industry Forum (CIF) revealed that the overall cloud adoption rate in the UK now stands at 88%, with 67% of users expecting to increase their adoption of cloud services over the coming year.

We asked why companies had moved to the cloud and whether they were satisfied with the results…

Only 14% of respondents have gone "all in" for the cloud with between 81 and 100% of their services and applications delivered from the cloud. The largest section of respondents at 40% had moved less than 20% of their applications to the cloud. So while every respondent is running some cloud based services many are still running in more traditional IT infrastructure models, and we will look at why later in this paper. Around a quarter (22.8%) have moved between 21 and 40%. There is a jump from just 7% moving 41-60% to 16% moving 61-80% of their applications and services to the cloud.

In March 2017 the Cloud Industry Forum (CIF) revealed that the overall cloud adoption rate in the UK now stands at 88%, with 67% of users expecting to increase their adoption of cloud services over the coming year. These figures are borne out by our own research.

There are an increasing number of applications being adopted by business that are born in the cloud and not based on existing applications, but businesses do have many legacy applications that either do not have a cloud delivery option or simply are workloads that are not suited to the cloud.

We looked at why companies had adopted cloud. Across the industry, vendors tend to lead with the message of flexibility and cost savings. Flexibility and scalability of IT resources certainly are considered the largest driving factors to cloud adoption within the survey base. 55% of respondents said this was their primary reason for adopting cloud within their business. The adoption of cloud has been partly driven by the uncertain economic conditions of the past decade. Businesses are no longer able to predict their growth and direction with the same accuracy because of ever changing external factors and we can be no more sure of our business futures now than five years ago.

Disaster recovery and business continuity have become far easier to achieve and far cheaper to deploy, with cloud ensuring high availability and eliminating data loss for business-critical applications, without the cost and complexity associated with traditional application-level clustering.

Disaster recovery and business continuity have become far easier to achieve and far cheaper to deploy, with cloud ensuring high availability and eliminating data loss for business-critical applications, without the cost and complexity associated with traditional application-level clustering. Nearly half (48%) said that the ability to perform live migrations and upgrades, effectively eliminating planned downtime and being able to automatically restart applications after failure occurs was a key factor in their choice to adopt cloud. 14% of respondents said that they considered the ability to diversify their IT suppliers and reduce risk played a part in their decision to move workloads to the cloud. While cloud platforms do still suffer from occasional outages they typically run at 99.99% and with more boards requiring internal SLAs IT departments can have a higher level of confidence delivering reliable services.

The cloud clearly wins against traditional computing infrastructure when we look at speed of deployment. It can take over a week to order, rack and configure a server as opposed to 5 minutes to deploy the same compute and storage resource in the cloud. 46% of respondents said that speed of deployment was one of their main reasons to deploy cloud services. Deploying in the cloud also removes the capital expenditure of new hardware and software with nearly a third (32%) saying this was an important consideration when choosing cloud solutions. But simply replicating the existing infrastructure in the cloud does not automatically bring savings.

Increasing computing capacity and business performance was important to over a third (38%) of respondents. It is now reasonable to say that all businesses are digital businesses as even the local plumber runs a website and does his banking and accounting on line. In larger businesses, IT is now critical for business operations and can give companies a competitive advantage. Whether automating manual tasks, analysing data that was hitherto trapped within disparate data bases or providing more powerful tools to the internal teams, the increase in computing power has had a direct effect on business performance. However, British businesses need to become more productive through the use of technology, our productivity is currently at 35% behind Germany and 30% behind the US according to the Office of National Statistics in 2015.

10% of the companies had chosen cloud as its relative simplicity to deploy and manage has helped them address their internal IT skills shortage. According to the UK Commission for Employment & Skills, 43pc of science, technology, engineering and maths (STEM) vacancies are hard to fill. This is mainly down to a shortage of applicants with the required skills and experience.

Not all companies were satisfied that they had achieved their stated objectives when they had moved to the cloud. Overall satisfaction levels were at 70%. While some reported 100% satisfaction there was a worrying amount of companies across all sectors below 50% satisfaction. One of the largest factors causing this is the lack of strategic thinking that behind many of the deployments, either just moving workloads or a small project scaling up unpredictably. With the benefits of cloud comes the requirements of new ways of thinking and operating for the IT departments and some are yet to fully make the transition.

Nearly half the respondents (43%) to the survey said that there are significant barriers to further cloud adoption within their organisation

We asked about barriers to further cloud adoption.

While some companies are still moving workloads to the cloud, many see barriers to further adoption. Nearly half the respondents (43%) to the survey said that there are significant barriers to further cloud adoption within their organisation.

The primary concern is security, with 44% of those companies stating that this was a barrier. Views on cloud security are varied, with some respondents only trusting in-house systems, and others believing that the investment and resources that cloud providers such as Amazon put towards securing their infrastructure give them far greater protection than they could achieve themselves. In a 2008 IDC survey, 74% of respondents cited security as their biggest barrier to cloud adoption so we can see that the cloud industry has gone some way in reassuring users that their cloud services are secure but there is a long way to go yet.

The second-largest barrier is the uncontrolled cost nature of cloud services (27%). For many years, cloud was presented as cost-saving and people assumed that by simply lifting what they had into the cloud they would see a reduction in expenditure. The cloud can bring benefits such as geographic redundancy but this comes at a cost. Reengineering infrastructure to take advantage of the benefits of the cloud will not always result in a cost-saving. Outside of infrastructure cloud-based services such as Office 365 and SaaS applications bring their own challenges to cost management and has been called death by a thousand cuts. The seemingly small per user licence costs soon mount up and unless these licences are managed efficiently they can go outside of budget quickly. The role of the IT department now needs to include ongoing cost management, for example choosing the right storage class and the right platform can have a big impact on data storage costs.

Reliability and latency both had a response of 27%. There are still high profile cloud outages such as AWS in February 2017 where the company's S3 service broke down causing performance issues from thousands of companies and applications but as damaging as outages such as this are, they are a rarity. The resilience and redundancy that can be achieved on cloud based systems at a significantly lower cost than in-house systems were given by some as the reason what they believe that reliability is no longer an issue to them but for others, this is not enough for them to move all their services to the cloud.

Latency is associated with reliability and can dictate whether a workload can be moved to the cloud. 30% of the respondents were accessing cloud services over the public internet and 40% over VPNs with only 27% taking advantage of direct connections. While most of the applications accessed over the public internet are SaaS solutions some companies were accessing their own services hosted by cloud providers. Most companies had not fully considered reducing latency by utilising direct connection to their cloud platforms and hybrid solutions.

The fear of vendor lock-in is very real, with 26% reporting it. The complexities of cloud service migration can result in customers staying with a provider that isn't optimum for their needs because of disruption of migration and increased risks.

The fear of vendor lock-in is very real, with 26% reporting it. The complexities of cloud service migration can result in customers staying with a provider that isn't optimum for their needs because of disruption of migration and increased risks. There is a feeling that if you only utilise core services such as Amazon S3 or EC2 and avoid higher level managed services such as orchestration tools and databases then you will be able to move vendors far more easily. This can result in companies keeping some services in house and developing their own tools to manage these. As with much of the cloud it is less of a technology issue and more of one of governance cost control and process.

Over 20% of the respondents were concerned about the loss of control or they were tied to existing in-house infrastructure. Loss of control has been a concern for any organisation outsourcing IT services since the very early days of computing, nowadays it usually results in a company taking a hybrid approach. Lack of authentication and access control by providers is a real concern when using a third party and this security fear can be valid, understanding a vendor's policies and adherence to them is crucial to building trust but many vendors are not transparent with their policies.

Investment into in-house systems or their complexity borne out of many years of projects, workarounds and incomplete documentation can leave companies tied to their in-house platforms. And some people simply prefer to be able to see lights flashing and know that their systems are built to their specifications and are getting managed in their way and this will always be the case.

20% of respondents said that lack of experience and training across their team means that they do not feel that their cloud deployments would bring the benefits they desired. There is a challenge that the ever evolving cloud landscape and services mean that companies do not necessarily know what will be best for them and that existing projects preclude them from taking the time to learn without running into the risk of failure. The introduction of new services such as machine learning, AI across platforms such a Microsoft Azure, Amazon AWS and Google makes the landscape even more complex and confusing.

Conclusion

British businesses have adopted cloud over the past decade and are now expanding its use into other areas. This adoption is not going unchecked. As well as technological issues, businesses face external factors such as GDPR, Brexit and the rise in cyber-security incidents. Cloud is being used to address these external factors alongside strategic business objectives

GDPR is a legislative indicator of just how important the digital economy and data has become and how central IT is to all business functions.

GDPR is a legislative indicator of just how important the digital economy and data has become and how central IT is to all business functions. GDPR will remain a major influence on IT priorities throughout Autumn, Winter and into Spring, and for companies only now starting to address their obligations under the new regulations, the pressure may continue past the new legislation's introduction date in March. The focus on GDPR is also being driven by the vendors and IT resellers who see an opportunity to help companies become compliant, with some addressing the troublesome issues such as finding where personal data is stored across large estates built up over many years.

Brexit looms large over business and will continue to do so. Its impact will be felt for years beyond 2019. For many businesses this will be positive, opening up new opportunities, though for others, the change will be more than just disruptive, it will be destructive and they will not survive. The government is moving toward the concept of a transition period which will ease the impact but as there is currently no certainty of what the final agreement will be businesses are going to have to continue to plan without all the facts. This is already impacting recruitment and it will start to impact projects over the coming year. Perhaps the flexible nature of the cloud is exactly the right technology for these uncertain times.

Cyber-crime is not going to stop, it is the new reality in which we have to operate, it will adapt and change to every attempt to bring it under control. The threats will be larger and potentially far more damaging to more than just business with national infrastructure already being targeted. Businesses have recognised this issue but there is a skills shortage of experienced cyber-security professionals resulting in a high cost to bring these skills in house. Businesses that do not pay enough attention to the threats will be hit by ransom ware attacks. It is important that the understanding of the real risks of cyber-crime are understood at board level so that the IT team can be sufficiently resourced to mitigate that risk.

While the cloud market is undoubtedly growing, most companies have already made the move to utilising cloud services so the growth rate will not be exponential. Business is entering a second

phase, or for some companies a third phase of cloud adoption. They have moved the easiest workloads, such as productivity suites like Office 365, and virtualized large server estates. They are now addressing the more complex infrastructure projects involving legacy applications. This is driving more companies to a hybrid approach as the varied workloads are often not suited to a full cloud adoption or in some instances there is a feeling that moving everything to the cloud is a loss of control and potentially a less secure solution.

The opening of UK based data centres by Amazon, Google and Microsoft will allow some additional workloads to be moved. These data centres address the issues of data sovereignty which is predicted to become more significant over the next four years.

The rise of the digital business, made possible by cloud, has changed the role of the IT department. For many companies, the use of technology is no longer just the engine room to keep the company moving but it is now dictating the direction of the business. Many businesses have had to adapt their business model or adopt a new one to survive and grow. And so the IT department has had to adapt and grow to meet this challenge and the increased demands and expectations put upon it by the boards of directors. IT departments are now expected to deliver zero downtime with incidents being very public if this is not achieved, as was seen in the BA data centre outage. Cloud, from SaaS based applications to multi region high availability data centre deployments allow IT departments to deliver highly complex solutions at a lower cost than has ever before been achievable.

The use of cloud in UK business is widespread but some of the concerns such as loss of control and security that have been around for the last decade have still not been eliminated and some people may always hold these views. The idea that everything will be delivered from the cloud is not going to be a reality for many businesses but the idea that cloud makes up a core element of UK IT deployments is already a reality.

serviceteamit

Download more analysis and full study results at
http://serviceteamit.co.uk/survey2017
and use these free services to have a look at your current cyber-security position.

Do you know exactly where your data is stored?
Free data location map http://serviceteamit.co.uk/datasov

Get a free basic Cyber-Security Audit
http://serviceteamit.co.uk/cyberaudit

Move towards GDPR compliance with this free, branded Subject Access Request form http://serviceteamit.co.uk/gdpr

Free, secure, low latency, high bandwidth Cloud Connect port for one month http://serviceteamit.co.uk/cloudconnect

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.

ADDRESS
49 Frederick Road
Edgbaston
Birmingham
B15 1HN

CONTACT
0121 468 0101
www.serviceteamit.co.uk
info@serviceteamit.co.uk
@serviceteamit