The Plan B SaaS Adoption and Resilience Report May 2016

Executive Summary

This latest report from Plan B Disaster Recovery looks at Software as a Service (SaaS) and asks IT buyers which areas of their business they are considering expanding these services in to. We assess the concerns they have over running their data on software in the cloud, and what level of business assurance they receive from suppliers to ensure continuity of service should unpredictable events such as platform outages and financial insolvency occur.

Should IT buyers be more concerned about the risks of having business critical systems in the cloud and would a better understanding of how to protect against these risks be beneficial to ensure better continuity of service and mitigation of risk?

Research Demographics

This research was carried out by surveying a sample of 100 companies from a range of sectors that attended the Cloud Expo 2016 event. All contacts interviewed were within an IT or decision making function of their business, with businesses ranging from SME to Enterprise.

1. Which areas of your business do you use SaaS for?

Across the board, SaaS is a highly adopted strategy, with nearly 50% of people using it for operational, financial and sales and marketing functions of the business.

Logistics and supply chain departments have the lowest utilisation of SaaS, along with the lowest potential for growth or adoption, demonstrating this function keeps their systems locally under their own control. This could, however, be because scalability isn't such a requirement for this software and the benefit of moving to SaaS doesn't make it viable.
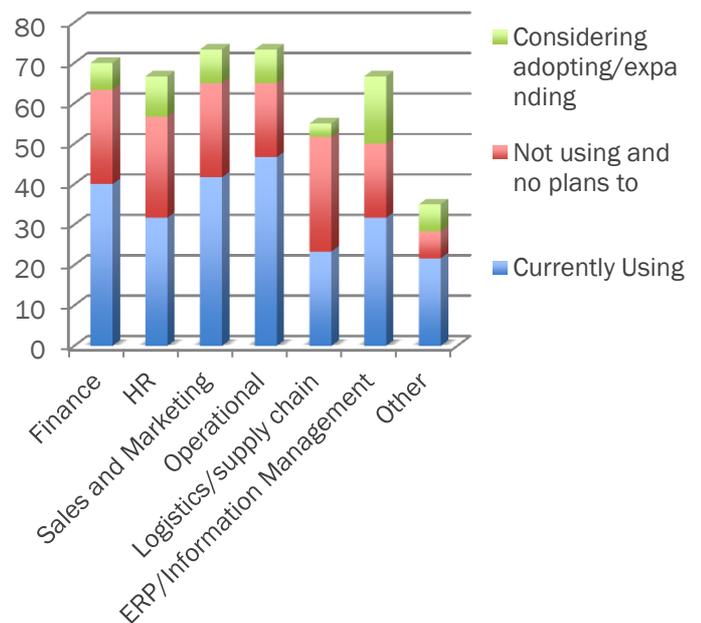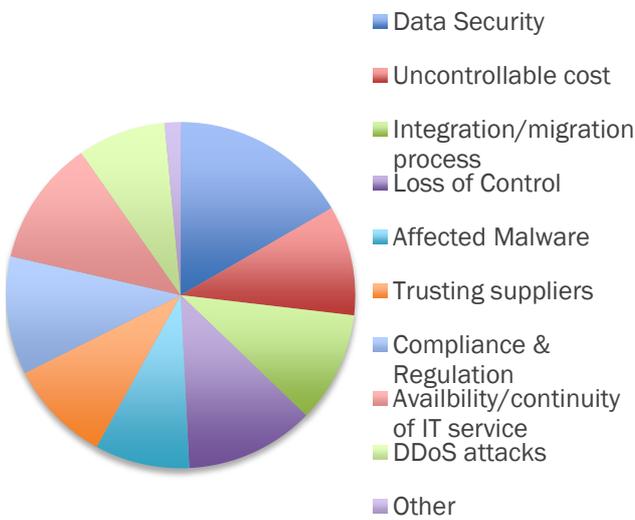
There was a surprising number of businesses that don't have Software as a Service anywhere in the business and wouldn't entertain the idea of adopting it in the foreseeable future, perhaps because they see the risks as being too great.

The greatest opportunity for growth of SaaS is in the ERP/Information Management function with 16% of companies researched considering adoption or growth of SaaS in this department.

2. What are your biggest concerns about having your data in the cloud?

- Data Security
- Uncontrollable cost
- Integration/migration process
- Loss of Control
- Affected Malware
- Trusting suppliers
- Compliance & Regulation
- Availbility/continuity of IT service
- DDoS attacks
- Other

Although Data Security came out at the top of IT buyer's concerns when considering SaaS, there is a remarkably even spread of concerns around having data in the cloud, as the results demonstrate.

Contacts were asked to list their concerns in order of importance from 1-5, with 1 being their biggest concern. Points were awarded accordingly e.g. 5

points were awarded for every 1, 1 point awarded for a 5 etc.

Companies therefore have very different views on what's important to them when reviewing SaaS providers, and the protection of their data.

3. Does your SaaS Provider store runnable copies of your data in a secondary location?
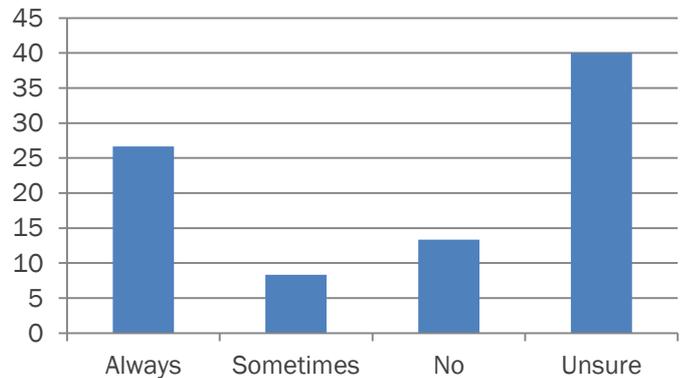
40% of people were unsure as to whether they have runnable copies of their data in a secondary location. This lack of knowledge implies that companies aren't doing enough due diligence when selecting a SaaS provider. In order to achieve high availability, companies should ensure that there is a runnable copy of their data in a secondary location that has been tested on a recovery platform and certified as recoverable. There is still some way to go in achieving this level of resilience.

4. Do you have any continuity plans should your SaaS provider cease trading or get taken over?
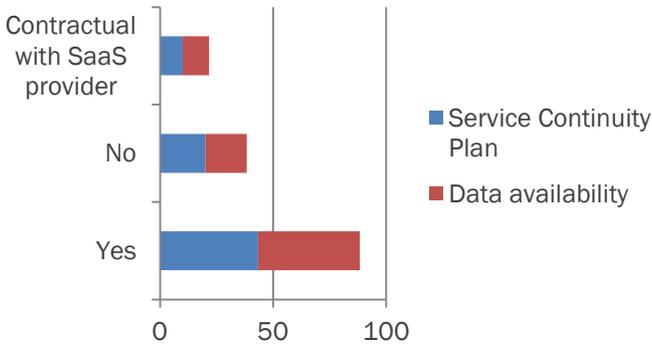
A very small percentage of businesses (10%) have contractual service continuity agreements with their suppliers. More worryingly, only 12% have contractual data availability contracts, which means that should your SaaS provider go into insolvency, there is an 88% chance that you won't be able to access your data and could therefore suffer complete data loss. Whilst 43% of providers have a service continuity plan, and 45% have a data availability plan, these are useless if there is no contract and your SaaS provider has gone TITSUP (total inability to support usual performance).

The upshot is that businesses should start demanding more contractual service and data continuity agreements to protect business critical systems.

5.   Was a continuity plan offered to you by your SaaS provider?

36% of SaaS providers are now automatically offering continuity plans with their services, which is a good start but could be improved. It would be good to see 100% of SaaS providers offering their customers a robust service assurance and continuity plan, and even better for 100% to automatically offer contractual guarantees of continuity. It may require buyers to start asking for them for this shift to happen though.
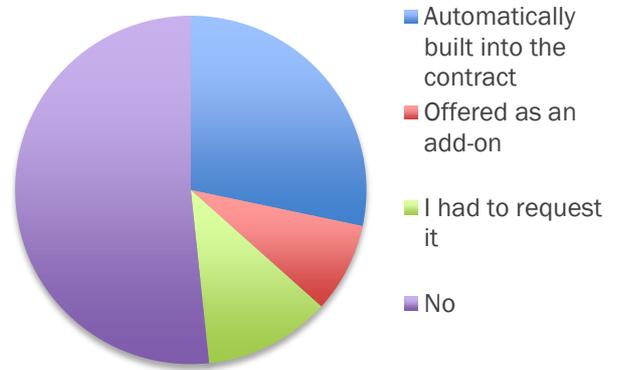
Of the businesses that offer service continuity plans, 58% are automatically building them into the service contracts, showing that many SaaS providers deem service continuity highly importance to the quality of their service. These providers should be favoured over those that do not offer a continuity plan.

6.   Does your SaaS provider offer the added protection of an independent Disaster Recovery provider?
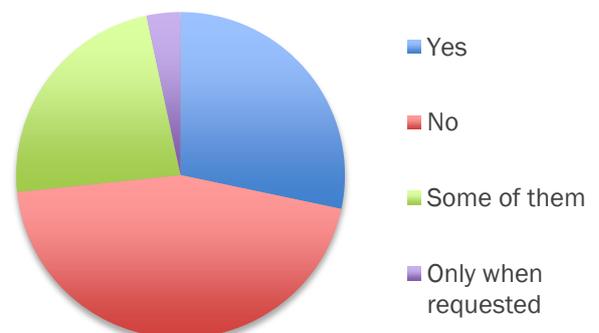

45% of SaaS providers don't offer disaster recovery via an independent provider. This leaves SaaS adopters at the risk of having all their data with one

provider. Should their provider go TITSUP then they could not only be without their systems but lose their data without the ability to get access to it.

One of the best methods of protection from the cloud is to ensure your data, and ideally systems, are not held by just one provider. You should have copies stored in a separate location (ideally runnable copies of the whole system) and through an independent provider to ensure high availability.

7.   Do you receive vulnerability reports from your SaaS provider?

Legend:
- Yes
- No
- Only if I ask
- Unsure
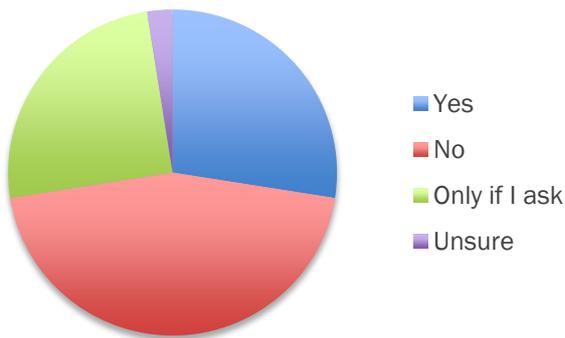
Only 18% of people receive vulnerability reports from the SaaS providers. Buyers should be requesting these more regularly so they can assess their risks and work towards safeguarding their data and the availability of their systems.

8.   Do you feel your SaaS provider could do more to protect your business from service interruption?

Whilst many buyers feel their SaaS providers should be doing more to protect their business critical software service, many didn't know what these improvements were. Hopefully this paper will

highlight areas for better due diligence that can be implemented across UK industry to improve IT resilience.
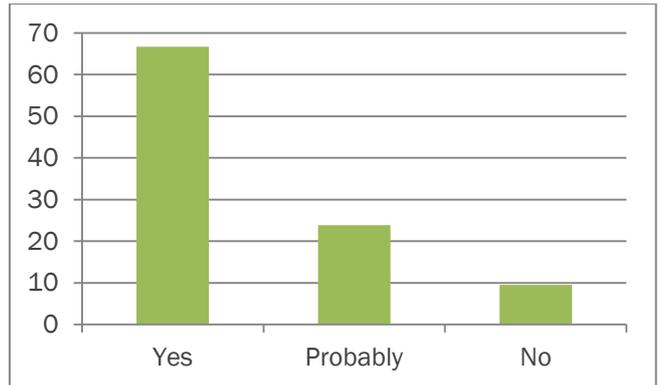
Conclusions

IT buyers would benefit from doing more due diligence when purchasing Software as a Service. They are looking for SaaS providers to offer more protection to their business, yet it is only the IT buyer asking the questions that will drive SaaS providers to step up their approach to resilience and availability of IT systems.

There is an opportunity for SaaS providers to create competitive advantage by offering a higher level of protection of their cloud via contractual Escrow services. This gives customers contractual guarantees of service continuity through an independent Disaster Recovery provider who can hold copies of their SaaS system and run them for them in the eventuality that they are needed.

It will be interesting to see how SaaS provider's offerings will improve over the next few years, as buyers become more knowledgeable of the risks of the cloud, and the options available.