Inside Track Research Note

In association with

Cloud Security Temperature Check

A question of visibility, governance and management

June 2015

In a nutshell

It is increasingly common for users and business groups to drive their own adoption of cloud services. But even where IT is involved, as organisations ramp up their use of cloud, activity is often uncoordinated. Pulling the threads together across service silos to manage risks effectively can be a challenge. The right strategy and governance processes, a well-thought-out hybrid cloud architecture, appropriate monitoring and management tooling and suitable operational procedures are all important to success.

About this Inside Track

The research upon which this Inside Track is based was independently designed and analysed by Freeform Dynamics Ltd. Data was gathered via an online survey executed in collaboration with a mainstream IT news site. 296 responses were gathered from business and IT professionals across a range of industry sectors, geographies and organisation sizes. The study was sponsored by Dell.

The democratising effect of cloud is a double-edged sword

Reports of the imminent demise of the corporate data centre might be somewhat exaggerated, but if you work in IT, the chances are that you are seeing more use of cloud services across your organisation. Software as a Service (SaaS) has lowered the barriers to adoption for many business applications. Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), meanwhile, are increasingly seen by developers and operations staff as important keys to streamlining application delivery.

The benefits of rapid cloud adoption often come at a price.

Whether you are an advocate or sceptic, there is no denying that cloud services in their various forms have a strong democratising effect. If it's IT teams, departments within the business, or even individual users, acquiring what they need from 'the cloud' can be a simple case of 'sign up and go'.

The danger is that the organisation ends up accumulating a sprawling mishmash of services.

But while this ease of adoption is highly convenient and great for flexibility and responsiveness, the benefits of rapid cloud adoption often come at a price. The danger is that the organisation ends up accumulating a sprawling mishmash of services that don't work well together and collectively create a significant data and application management headache. Disjoints between 'cloud silos' can even undermine the very efficiency and flexibility gains that were sought in the first place.

In a recent online survey in which responses were gathered from almost three hundred IT and business professionals, we investigated the related set of challenges and risks arising from fragmented cloud adoption in the area of security.

Challenges begin right up front

Cloud computing is simply an alternative model for application deployment and storage of data. You can dress it up as a huge transformative force in the industry if you like, but fundamentally it's about getting someone else to take care of one or more layers in the service delivery stack.

Some think of cloud as a kind of magic; indeed it's not uncommon to hear people mistakenly talking as if it somehow makes all your technology-related problems disappear.

But some think of cloud as a kind of magic; indeed it's not uncommon to hear people mistakenly talking as if it somehow makes all your technology-related problems disappear. From a user perspective, it can even create the illusion that IT is no longer relevant – the magical cloud will deliver everything you need without those irritating IT staff with their tedious rules and tendency to say "no" needing to be involved. All IT does is complicate every simple decision and slow everything down.

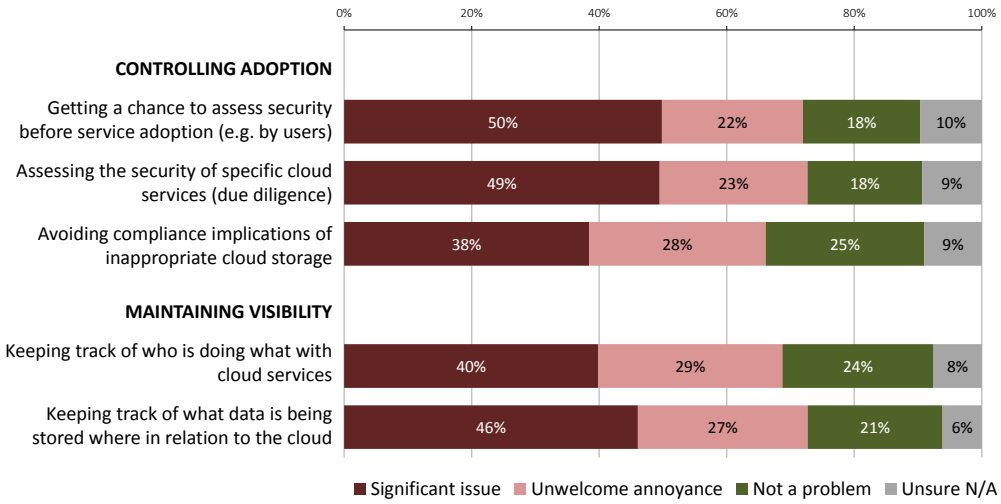
End-users or even well-meaning business managers, may believe their familiarity with consumer technology gives them the knowledge they need to make good decisions.

The trouble is that IT professionals do a lot more than take care of the physical aspects of systems, and if they are cut out of the equation, some important considerations can easily be overlooked. End-users or even well-meaning business managers, may believe their familiarity with consumer technology gives them the knowledge they need to make good decisions, but they are usually not equipped to evaluate the security, governance and compliance implications and requirements.

The truth is that even if you have the necessary knowledge, it can be hard enough to evaluate the inherent security of a cloud service, and figure out how to implement it in order to stay safe and compliant. It is telling, however, that one of the most common challenges highlighted in relation to cloud is getting the chance to assess things like security before a service is adopted (Figure 1).

Figure 1

How would you characterise the following challenges in relation to your organisation's use of cloud services?



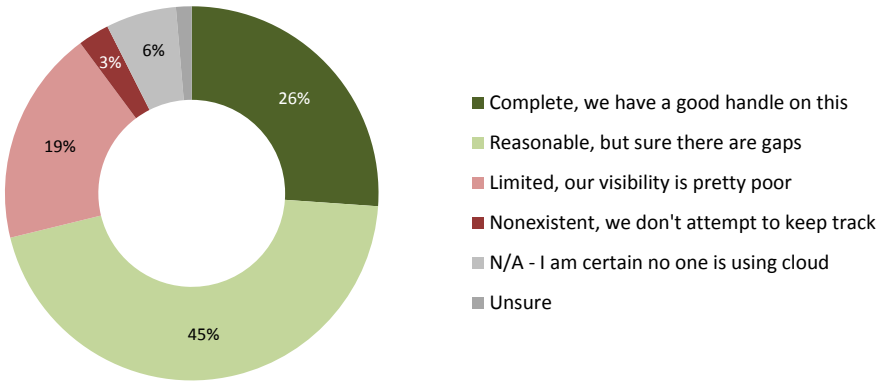
Many are clearly struggling to keep track of who is doing what with cloud services.

If we zoom out from thinking of individual services to the bigger picture, the other set of challenges that come across in the above chart are to do with visibility. Many are clearly struggling to keep track of who is doing what with cloud services, along with where and how data is being stored.

Despite the fact that many IT pros are undoubtedly making the effort to stay on top of this, the difficulties frequently lead to gaps in the IT team's knowledge. In fact, only around a quarter of those participating in our survey claimed to have complete knowledge of where and how cloud was being used across the organisation (Figure 2).

Figure 2

How would you describe the IT team's knowledge of where and how cloud services are being used across your organisation (including those adopted directly by users)?



You can't secure what you don't know exists.

The obvious problem here is that you can't secure what you don't know exists, but this is not the only challenge.

Distributed and inconsistent landscapes create more problems

Security challenges can arise around trying to coordinate security and identity across boundaries.

As a result of the cloud-related acquisition behaviour we have been discussing, both within the business and within IT, security challenges can arise around trying to coordinate security and identity across boundaries (Figure 3).

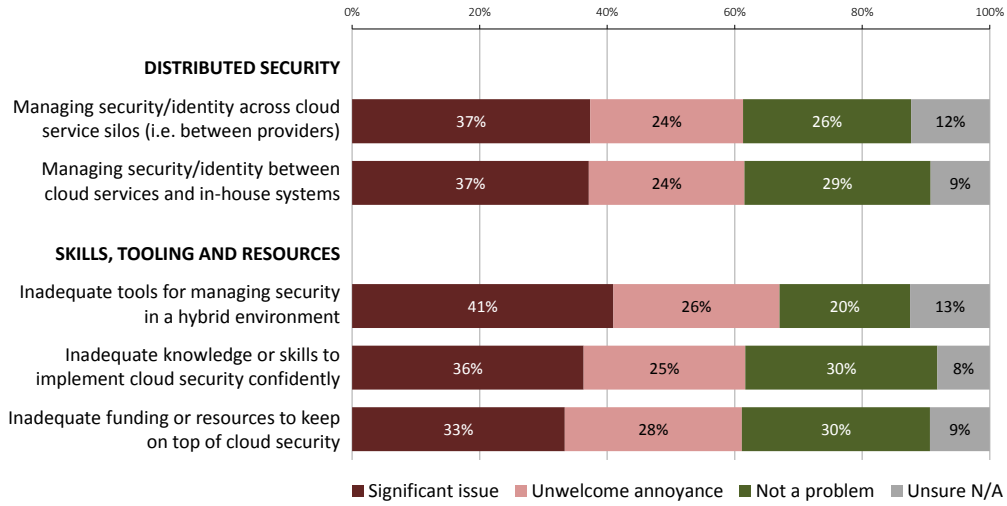


Figure 3

How would you characterise the following challenges in relation to your organisation's use of cloud services?

Many still don't feel properly prepared.

The other telling observation from this chart is that many still don't feel properly prepared. Inadequate tools, skills shortfalls, and a general lack of funding and resources to improve the situation are all frequently cited.

Tools are available to help, but they aren't always used

Most know what they should be using, but they are frequently not acting on this knowledge.

When it comes to security tooling, the survey suggests that most know what they should be using, but they are frequently not acting on this knowledge (Figure 4).

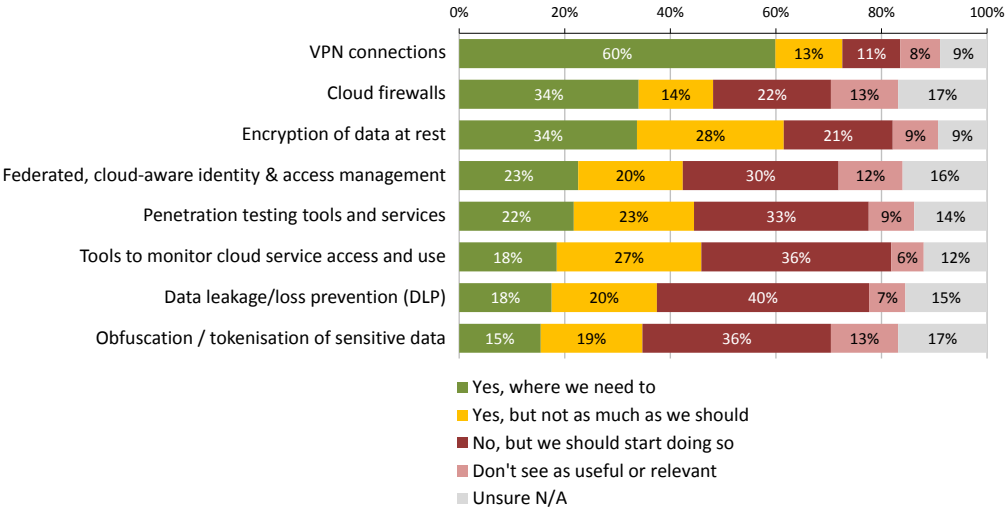


Figure 4

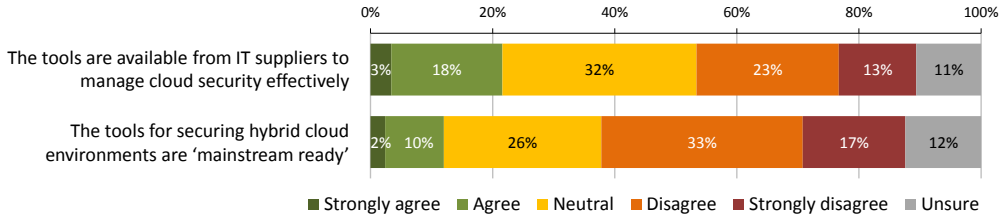
Do you make use of solutions in the following areas to deal with cloud service security requirements?

Suppliers have some work to do.

As we can see, even where tools are in place, they are not always applied as broadly as they should be. But this raises the question of the availability and readiness of the security solutions on offer. Here it would seem that suppliers have some work to do to either improve their offerings, or to convince IT professionals that they can actually handle the requirements of today's complex cloud environments (Figure 5).

Figure 5

How much do you agree or disagree with the following statements?



But while technology is undoubtedly important to ensure safe use of the cloud, we should not forget one of the most prominent sources of risk.

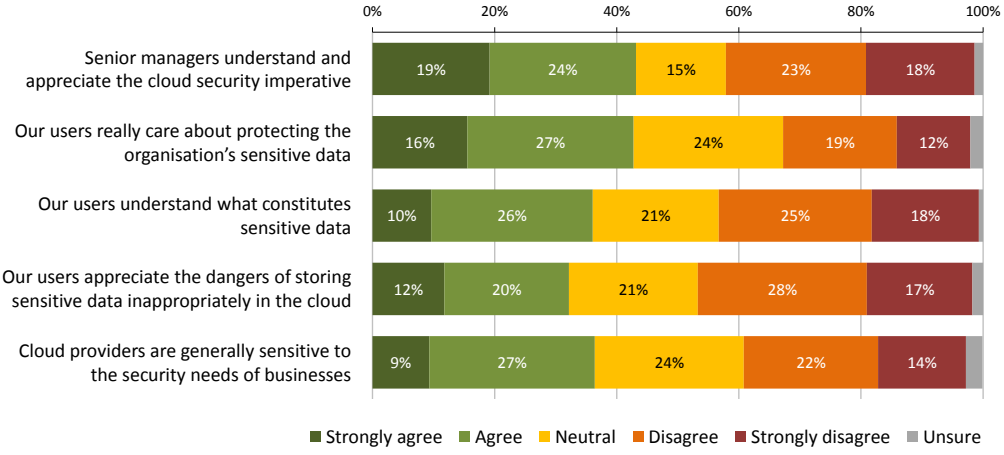
Familiar people-related issues remain a problem for many

A frequent lack of understanding and appreciation of the cloud security imperative among senior managers is evident.

A frequent lack of understanding and appreciation of the cloud security imperative among senior managers is evident from the survey, and this obviously goes hand-in-hand with some of the previously mentioned funding and resourcing challenges. What also comes across is a clear need in many cases to both educate and motivate users, not just on cloud specific security risks, but also on the more fundamental matter of what constitutes sensitive data (Figure 6).

Figure 6

How much do you agree or disagree with the following statements?



The last point on this chart is particularly interesting to consider. Many participating in our survey clearly have doubts about the degree to which some cloud providers are sensitive to the security needs of businesses. This will obviously be particularly true of providers with a consumer heritage. Put this together with the adoption behaviour we were discussing at the outset, and the potential for dangerous security exposure is abundantly clear.

The potential for dangerous security exposure is abundantly clear.

Research findings like this highlight that cloud security is a complex topic. Identifying and solving the technical challenges is critical, but you will only succeed in protecting the business if you tackle the governance, education, and motivation dimensions effectively too.

It's important to act sooner rather than later

It's important to develop a sustainable approach to managing security as soon as you can.

Wherever you are in terms of cloud adoption, it's important to develop a sustainable approach to managing security as soon as you can. If activity is relatively modest at the moment, you may not see this as a big imperative, but the issues escalate rapidly as you accumulate services, particularly if adoption activity is relatively uncontrolled.

In order to gain and keep control, it is important to:

- Educate senior management on the imperative so they allocate the necessary resources and provide adequate air cover as you come to an understanding with business stakeholders and users on appropriate adoption discipline.
- Define usage policies and educate users and business managers so everyone understands and is clear what constitutes safe and responsible behaviour. Back this up with a governance model to ensure sound and effective decision-making.
- Formulate a strategy and approach within IT for dealing with the realities of monitoring, managing and securing a distributed, hybrid environment. It is beyond the scope of this document to go into detail here, but you need to think through skills, systems architecture, and tooling.
- When engaging suppliers, whether IT vendors or service providers, beware of players who take a narrow view of the problem and advocate simplistic 'magic bullets'. Cloud increases diversity and complexity, which can both be managed, but only if you work with partners who embrace an inclusive approach.

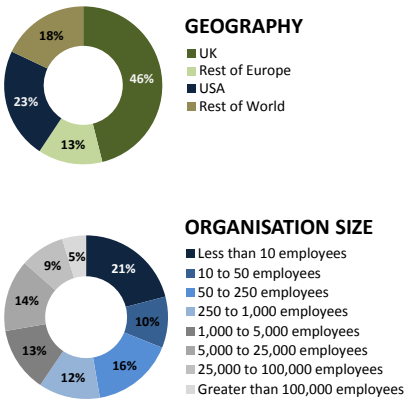
Don't fall into the trap of thinking of cloud risk management as purely an IT problem. It's a business issue, and as such ultimate responsibility lies with business executives.

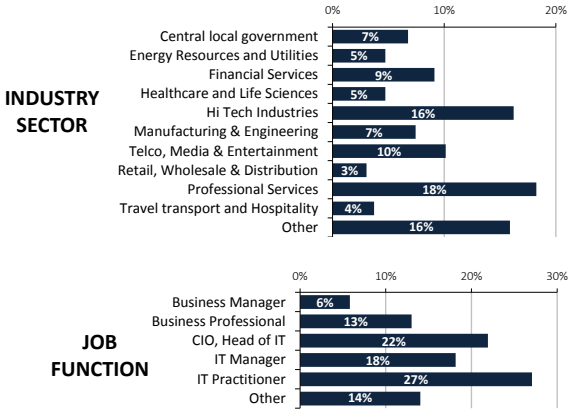
And as a last piece of advice – don't fall into the trap of thinking of cloud risk management as purely an IT problem. It's a business issue, and as such ultimate responsibility lies with business executives. You need to make sure they know this.

RESEARCH DEMOGRAPHICS

Figure 7

Online survey conducted in collaboration with a mainstream news and analysis website





About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we aim to help busy IT and business professionals get up to speed on the latest technology developments, and make better informed investment decisions.

For more information, and access to our library of free research, please visit www.freeformdynamics.com.

About Dell

Dell Inc. listens to customers and delivers worldwide innovative technology, business solutions and services that give them the power to do more. For more information, visit www.dell.com.

Terms of Use