



# Trust and security in the cloud

## The myths and realities of hosted applications

*Andrew Buss and Dale Vile, Freeform Dynamics Ltd, February 2011*



*in association with*



The delivery of cloud based application functionality via the Software as a Service (SaaS) model frequently sparks a vigorous debate on security-related concerns. It is common to hear IT professionals question whether service providers can be trusted to look after critical and confidential business data. But while the concerns may be real, are they justified or is it a case of being wary of the unknown while overlooking the shortcomings of internal systems?

## KEY FINDINGS

### **Many companies could do much better when it comes to in-house security**

Many companies implement security reasonably well, but there is a widespread gap in the tools and policies they have in place with the result being that their security capability is some way off where they would like it to be. Additionally, there is a significant risk of data loss through end user devices and services, which is amplified by a general lack of attention to security by the workforce.

### **SaaS adoption is limited currently, but there is increasing interest from the business**

SaaS is not yet part of the mainstream, but interest is increasing. While it might be expected that demand is driven by individuals or departments, the biggest driver in fact is felt to come from business leaders as well as senior IT management. This demand means that IT departments will increasingly be under pressure to consider and deploy SaaS as part of the service delivery portfolio.

### **The biggest impediment to SaaS adoption is a perception of security issues**

There is a widespread belief that SaaS represents a considerable step backwards in security and privacy in comparison to on-premise capabilities, and that this is a sufficient reason not to adopt SaaS. Additionally, SaaS providers are seen by the respondents as broadly similar when it comes to security and privacy regardless of their actual capabilities.

### **Companies with experience of SaaS are positive about provider security**

There is an understandable attitude amongst those companies that have limited or no experience of SaaS that what is new or unknown represents a risk. However, when it comes to companies that use SaaS extensively, most view provider security as either equal to, or better than, their on-premise capabilities. This changes the outlook completely, with SaaS security moving from being a blocker of SaaS to being an enabler of adoption.

### **SaaS is likely to help with shortcomings of on-premise security capabilities**

Given the security gap that exists for many companies, which is especially marked for departmental and collaboration applications, SaaS can help to raise the overall level of security. But it needs to be evaluated impartially using the same criteria as on-premise solutions since providers differ with regard to capability, culture, service and cost.

Freeform Dynamics independently designed and executed the study upon which this report is based in collaboration with The Register news and information site. Feedback was gathered via an online survey of 510 business and IT professionals from the UK, USA and other geographies. The study was sponsored by Google.



## Introduction

---

Software as a Service, or SaaS as it is commonly abbreviated, has been getting a lot of attention over the last few years as one of the vanguards of the 'Cloud' wave. Whatever the potential advantages that this approach may bring, adoption has been slow with security and privacy concerns often cited as inhibitors to business use. Increasing interest from senior management in SaaS is focusing the spotlight once again on security in the cloud.

In this study, we set out to see whether this is an accurate understanding of the concerns of IT and business professionals, as well as investigating the motivations behind such concerns. As a foundation for our discussion we'll be using input gathered via a research study completed in January 2011, during which feedback was gathered from 510 respondents through an online survey.

Those who participated in the study were mainly business and IT professionals from a range of organisation sizes and industries. Representation was predominantly from the UK and USA, coupled with a number of respondents from other geographies (see Appendix for more details). The study was designed and executed on an independent basis by Freeform Dynamics Ltd. ([www.freeformdynamics.com](http://www.freeformdynamics.com)) and conducted in association with The Register news and information site ([www.theregister.com](http://www.theregister.com)).

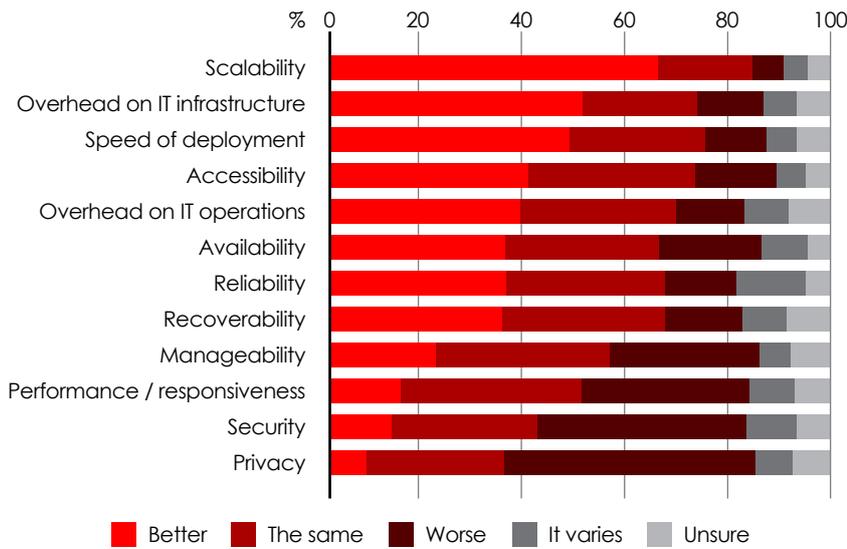
Based on this feedback, we review where organisations are on the road to SaaS, and what fears and doubts they have around using these services. We examine the views of senior IT and business managers, technical decision makers and IT professionals to determine what the reality is today. We also consider what the future holds for companies considering the implications of security and privacy when adopting SaaS. In many respects, it really is a case of myth versus reality and a wariness of the unknown.

## Security and privacy are real concerns for most companies

---

When we look at the prevailing view of SaaS in the mainstream IT professional community, we can see that there are a lot of perceived benefits, particularly around the issues of scalability, resiliency and the ability to reduce the overhead on IT operations and infrastructure. Many of these are strongly weighted in favour of SaaS over an on-premise solution. Crucially though, we can also see that security and privacy come very much at the bottom of the list, being viewed as significantly worse than on-premise solutions (Figure 1).

**Does the SaaS model represent an advantage or disadvantage compared to traditional on-premise solutions for the following?**



While SaaS is generally recognised as offering potential benefits, security and privacy are big sticking points for many.

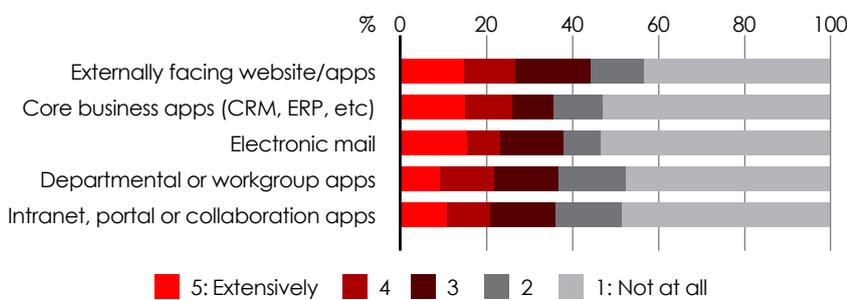
**Figure 1**

These fears concerning the security and privacy of SaaS are certainly felt in a very real way, but if we look at the underlying issues, are they justified? The first thing we need to do is look at the situation from a 30,000 foot view to see just what use is made of SaaS, and from this to see what differences there are in attitude to SaaS security based on the extent of SaaS experience.

**SaaS adoption is limited today, but there is growing interest**

When we look at the adoption of SaaS, it is clear that many companies are not using it at all and have no direct, hands on experience. A good number are really just dipping their toes in the water or using SaaS in a piecemeal or tactical way. What is telling is that a significant number of companies in the survey have overcome their security and privacy concerns and are using SaaS in an extensive manner. It is worth recognising that when SaaS is broadly used, it is not relegated to niche areas or departmental applications, but is used across all of IT from mainstream applications to critical business systems (Figure 2).

**To what extent is SaaS actually being used in your organisation in the following areas?**

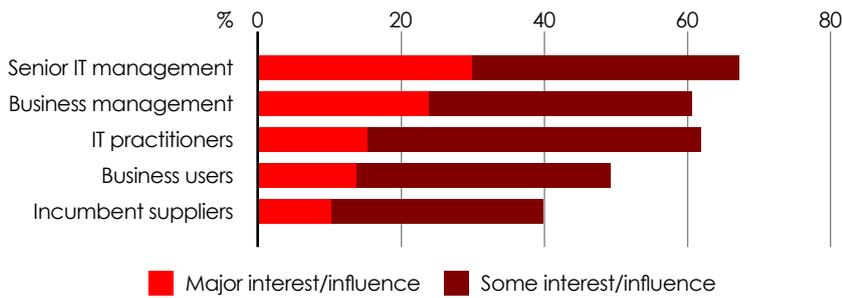


While a significant number of companies are actively deploying SaaS, most organisations lack real hands on experience.

**Figure 2**

Another trend to note is that more organisations are likely to be considering SaaS as time goes on. We see a lot of interest from senior managers, both from the business and in IT, attracted by some or all of the benefits that SaaS is perceived to provide (Figure 3).

### Where in the business is the drive or interest for SaaS services coming from at the moment?



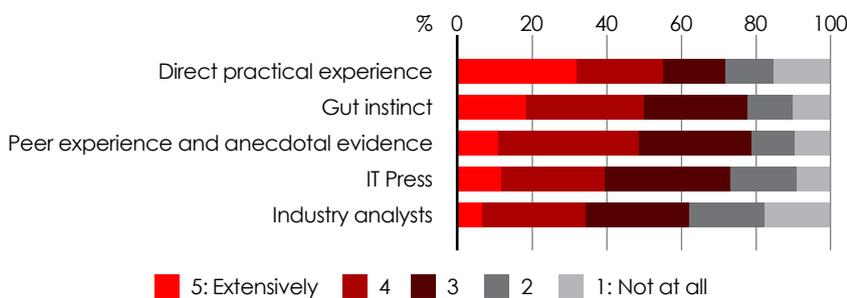
Interest in SaaS is coming from senior management in both the business and IT.

Figure 3

This growing interest is likely to increase the pressure on IT to consider SaaS options to meet the needs of the business, and reinforces the motivation to explore what's behind the security and privacy issues that are likely to hold back the adoption of SaaS if they are not addressed.

In order to understand why so many IT professionals have such deep-rooted concerns about security and privacy in the cloud, it is necessary to examine what is most influential in shaping their views. We see the expected influence of the press, analysts and vendors along with input from peers. However, the top two influences are very telling. Direct experience trumps all other influences, and if this does not exist, IT pros follow their instincts (Figure 4).

### How much have the following shaped your opinion of SaaS?



Practical experience is most effective at shaping opinions of SaaS, but there is still a lot of confusion and guesswork going on.

Figure 4

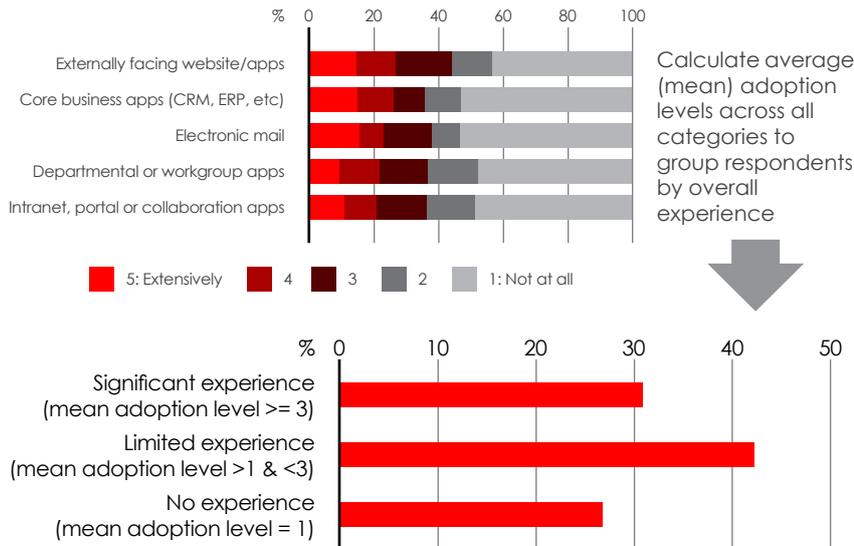
This is an important trend because, as we saw earlier, a significant proportion of respondents are not using SaaS in any shape or form. They therefore have no direct experience on which to form an opinion. Even more telling is when we look in more detail at these respondents it is clear that they generally do not utilise peer experiences either, and their main influence is their gut instinct. Those with extensive experience of SaaS tend to make use of all resources open to them, with gut instinct still forming a good part of their view, but with hands-on experience and peer advice the main sources of influence.

## Experience leads to a security revelation

Picking up on the question of experience, we can explore the effect that this has on the perception of SaaS security and privacy if we group the respondents according to the level of SaaS activity that they report in their organisation (Figure 5).

### Segmentation of respondents by SaaS experience

To what extent is SaaS actually being used...



Most companies have a very limited exposure to SaaS applications.

Figure 5

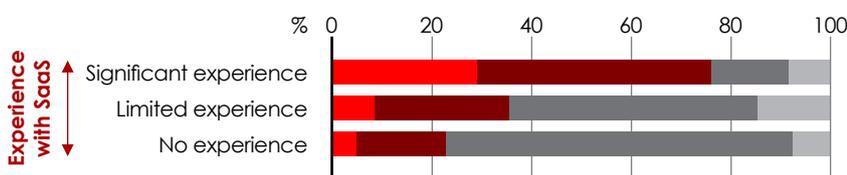
If we base this on the mean adoption level of SaaS across the different areas of IT, based on 1 being no adoption in that area, and 5 being extensive usage, we can identify three distinct segments:

- **No experience** - mean adoption level = 1
- **Limited experience** - adoption level >1 and <3
- **Significant experience** - mean adoption level >= 3

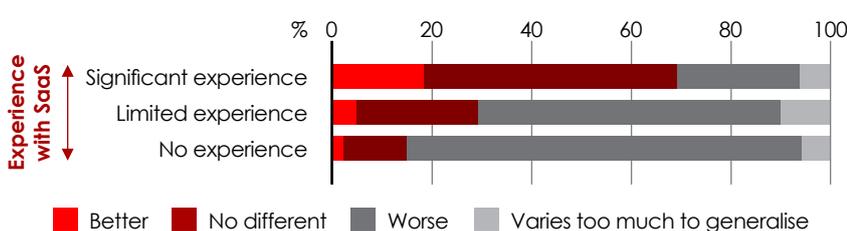
Looking at how the perception of SaaS security changes with the level of experience is striking. For those with limited or no experience of SaaS, the general consensus is that security and privacy are both significantly worse than on-premise solutions. For those with extensive experience, a different picture emerges. Most believe that SaaS capabilities are at least equivalent to their on-premise solutions. Even more importantly, there is a big jump in the proportion of respondents that believe SaaS security or privacy is better than on-premise (Figure 6).

### Opinions vary based on experience

Is SaaS better or worse than on-premise with regard to **security**?



Is SaaS better or worse than on-premise with regard to **privacy**?



Opinions on SaaS security reverse once significant experience is gained.

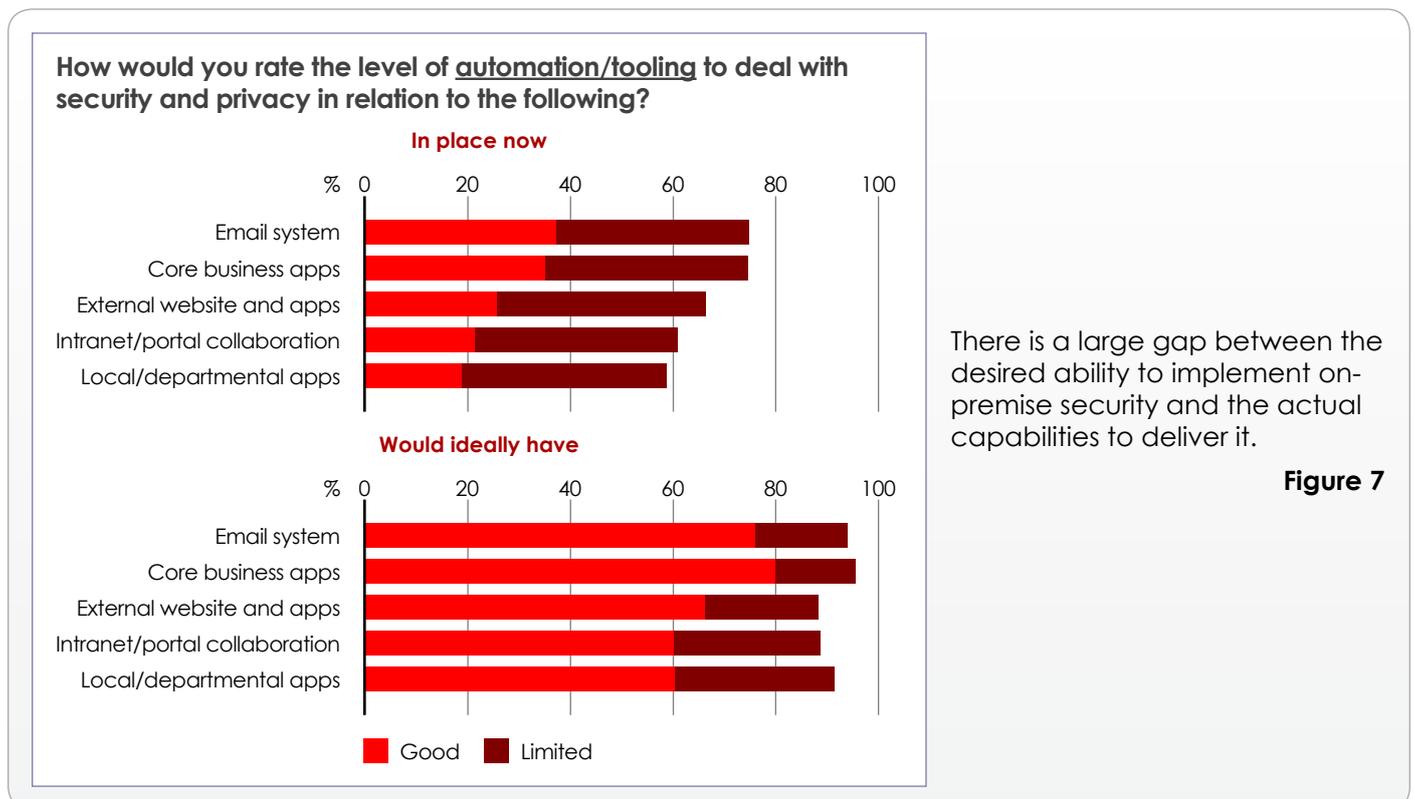
Figure 6

This suggests that a big gap exists between perception and reality in these areas, with SaaS in practice being nowhere near as risky as those with limited or no experience think it might be. Cautious IT professionals are undoubtedly equating 'unknown' to 'risky'. This is a natural and understandable reaction given that cloud hype, which is often so obviously dubious, has tended to create issues of confusion and trust. It's also important to recognise that the perception doesn't really change until significant use is made of SaaS. This has the implication that many companies will start out slowly until experience and trust is gained before ramping up the adoption of SaaS.

## On-premise security is no bed of roses

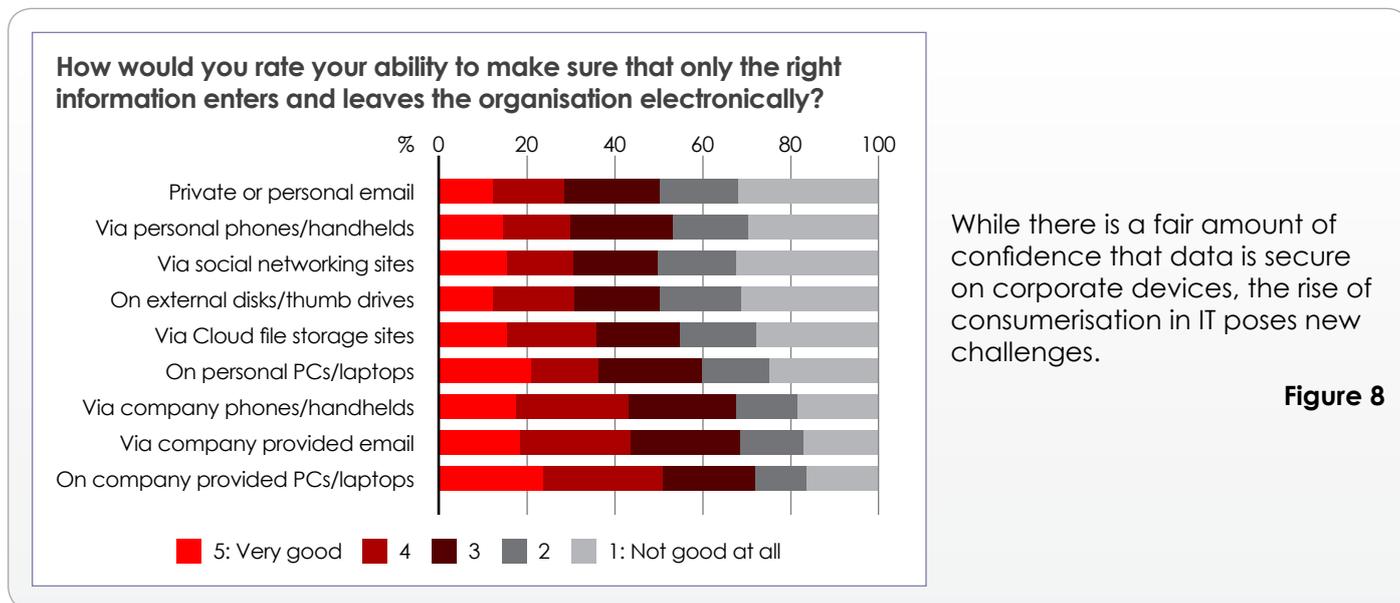
The difficulty with asking about SaaS security in isolation is that the focus is placed squarely on the potential challenges associated with this model. What we tend to forget is that there are also limitations on the capabilities of current on-premise IT security, and these have a tendency to be glossed over. So let's remind ourselves about the reality of in-house IT security.

There is a tremendous amount of system complexity and information that exists in most IT organisations today. When combined with the rapidly changing nature of the security landscape and diminishing budgets, security is a moving target that is difficult to keep on top of. Effective security management can be helped to a large extent by automation and tooling. However, few respondents felt that they had a good implementation for this, and many respondents reported large gaps between what they would ideally like to have compared to what is actually in place (Figure 7).



Further confirmation of the difficulties that IT faces in securing systems and data become evident when we look specifically at the question of data leakage. This is a hot topic due to the continuing number of high profile incidents of data loss as well as the increasingly stringent regulations that are coming into force. Respondents were most confident that they had a handle on data leakage with company provided equipment, although there is obviously still a lot of improvement that could be done in this area.

An even bigger problem is looming however, as the consumerisation of IT leads to a proliferation of personal mobile computing, portable storage devices and the use of online services to access, store and propagate corporate information. What's clear is that whatever IT does to secure company issued devices, they face a new challenge when it comes to tackling the security of this new wave of consumerisation (Figure 8).



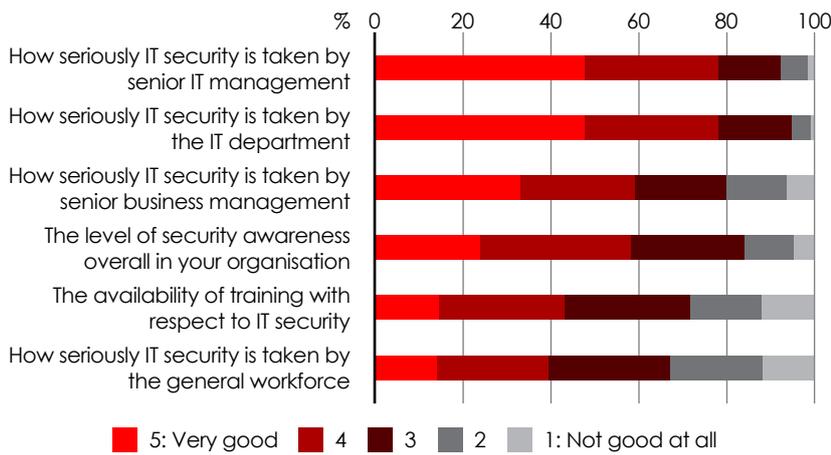
The upshot of this is that whatever concerns respondents may have about using SaaS services, there is a pressing problem that needs both recognition and attention. Compounding this challenge, respondents to the survey reported serious concerns about the attitude and awareness of the general workforce when it comes to security and privacy.

## Users are a weak link in the security chain

A central concern is how little security is appreciated and taken seriously by the general workforce. Even more worrying is that this lack of focus has not really improved over the past number of years despite the high profile security breaches and the improvements that many IT vendors have incorporated into their products to increase the default levels of security

A primary reason why this remains the case is that when it comes down to making sure employees know what is expected of them, we commonly see a reluctance to invest in the required level of education and training to make this happen (Figure 9).

### How would you characterise the following?

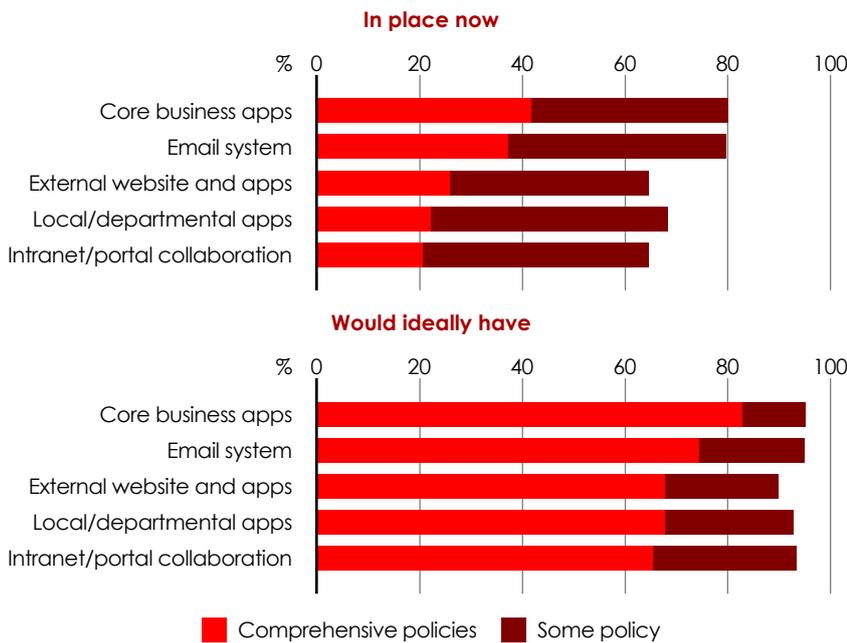


Although management is increasingly concerned with IT security, there is a lack of investment in training to change the culture of the workforce to match.

Figure 9

Of course, appropriate workforce behaviour and effective training are, to a large extent, dependent on the clear definition of security and privacy policies coupled with an awareness of how the workforce use systems and data. Yet as with the investment in tools and automation, we see a significant gap between the security ideal and what is really done in practice (Figure 10).

### How comprehensive are the policies and procedures that you have to deal with security and privacy?



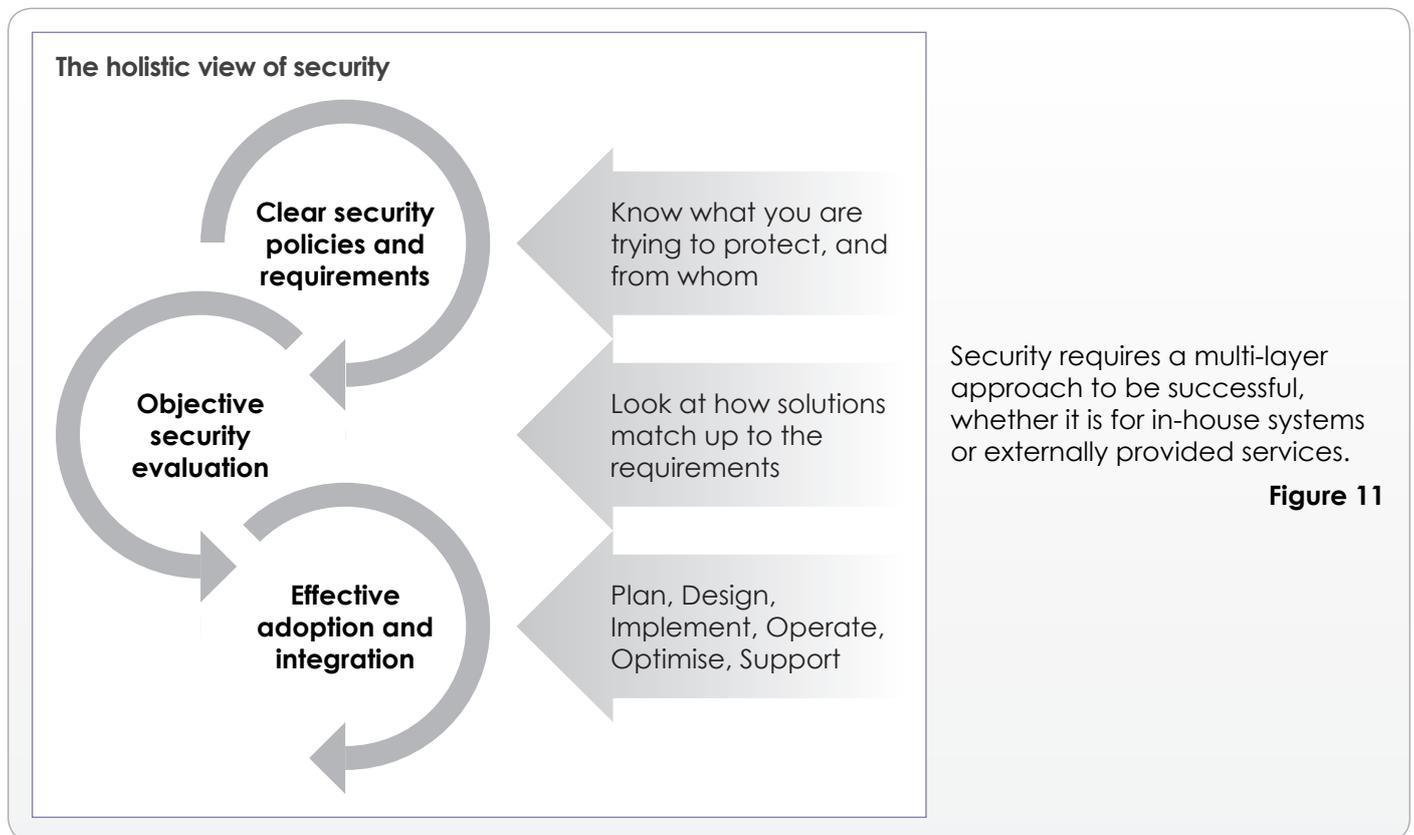
The general workforce doesn't pay much attention to IT security because policies are insufficient to guide their behaviour.

Figure 10

This all suggests that the weakest link in SaaS security is often not going to be the service itself, but the behaviour and attitude of the ultimate users of the service which ultimately impacts all of IT. We therefore need to think more holistically about the approach to security and the selection of a SaaS provider.

## Success requires a longer term view

Successful IT projects require careful planning, evaluation and implementation to achieve their goals and provide a return on investment. The adoption of SaaS in general, and security and privacy in particular, are no different (Figure 11).



The planning should start with knowing the requirements that any solution needs to fulfil. It is vital to be aware of just what the necessities are so that you know what needs protecting, to what level and from whom. This may be a tough task given the gap between where policies and procedures are today, and where respondents would ideally like them to be, but time and effort spent here is required to aid the objective assessment of potential solutions.

The evaluation criteria should be applied equally to all candidates, be they on-premise, SaaS, in the cloud, "hybrid" or otherwise. From IT's perspective, one of the difficulties of choosing a SaaS provider is getting to grips with the most significant part of the offering – the operational capabilities of service delivery. It's important to understand how these elements, such as culture, staff selection, scale, support capabilities, SLAs and other contract terms come together to meet requirements.

We know from our past research that the successful implementation of IT solutions can be quite hit-and-miss<sup>1</sup>. Even with the same set of raw starting ingredients, the end result may vary and a lot of this is often to do with how the project is managed and implemented. This is arguably even more important for SaaS, as it is easy to forget just how simple it is to select a service and be up and running without much thought for the bigger picture.

Most IT systems will end up interacting with other parts of the business infrastructure and processes, so there is the issue of whether the system needs to be customised to fulfil its role effectively. Then there is the thorny issue of user training and support which is often overlooked. This can help greatly not only with acceptance and use of the service, but

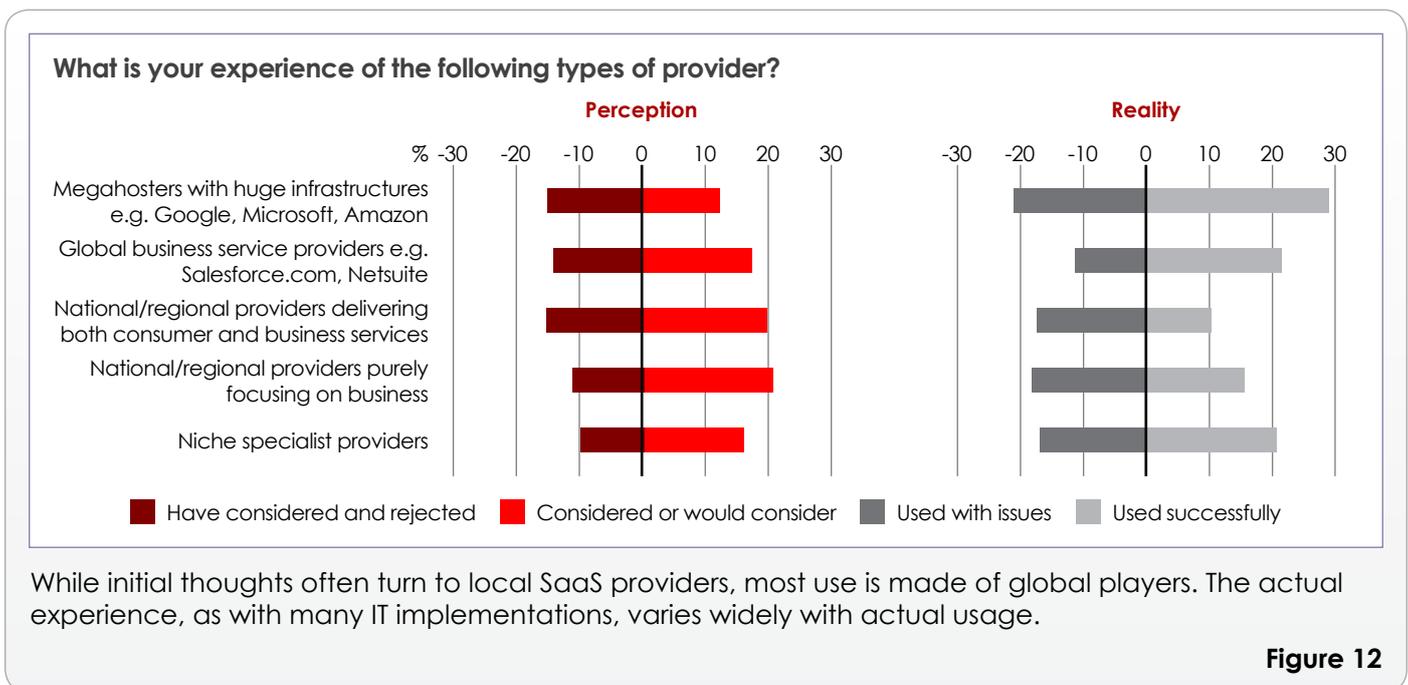
also, as we have seen, with security too.

We can see this in action if we step back and look at the perceptions and experiences when selecting and using SaaS from a variety of provider types.

## Experience of SaaS providers varies so careful selection is vital

Despite the general perception that all SaaS providers are pretty much alike, they vary significantly in scale, capability, execution, support and overall offering. Respondents to the survey reported a mix of good and bad experiences with all types of provider. This underlines the importance of effective supplier selection and implementation on the customer side of the equation.

There is a tendency for companies to turn to national providers first when initially evaluating SaaS. This behaviour may have its roots in a prior relationship, language, location or even an aversion to larger providers. While this may seem the natural approach when starting out with no SaaS experience, the reality is that it is the larger, more global providers that are used the most, and with the least number of issues. This highlights the fact that service providers are not all the same. The truth, of course, is that services also vary considerably within each category of provider. This makes knowing what is required as well as supplier evaluation even more critical to success (Figure 12).



When looking at the credibility of SaaS providers regarding security and privacy, the respondents in our study use a variety of means to assess offerings. Many of the attributes evaluated are not dissimilar to those for on-premise IT solutions. When considering SaaS, there is a whole new layer to consider around service delivery and the ongoing operations of the service provider, which for on-premise solutions are already part of the server infrastructure or datacentre (Figure 13).

**When looking at security and privacy, how important are the following in establishing the credibility of a SaaS provider?**

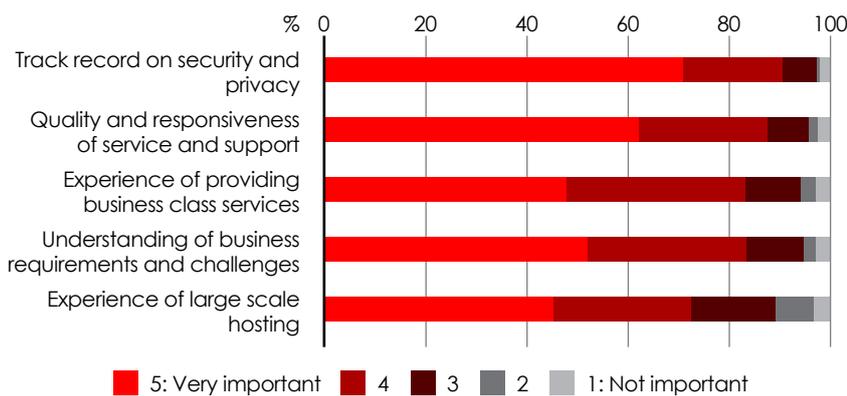


While SaaS selection involves evaluating some new criteria compared to on-premise solutions, much of what has been learned through prior procurement cycles still holds true.

**Figure 13**

Zooming out from security and privacy in particular and looking at the broader issue of trust, respondents set the bar pretty high across a variety of considerations. What potential customers seek most is a track record of security and privacy, demonstrable experience delivering business services together with an effective infrastructure to service and support customers effectively (Figure 14).

**How important are these elements in creating a feeling of trust with a SaaS provider?**



Customers set the bar high for SaaS providers when it comes to trust, arguably far higher than they set for themselves.

**Figure 14**

This is not surprising given the level of commitment a SaaS decision represents to most organisations, and perhaps a lesson here for providers looking to drive increased activity.

## Discussion and conclusion

The results of the study presented in this report indicate that SaaS adoption is starting to be used in earnest by a significant proportion of respondent companies. The interest from business management and senior IT managers looking to take advantage of a number of potential benefits is likely to increase adoption still further in the future. There is, however, also a widespread feeling that SaaS is a risky solution when it comes to security, and this is a potential deal-breaker.

Part of the problem lies in the perception of SaaS. The whole cloud computing landscape, of which SaaS is a part, is a very active and diverse area. Vendors and cloud providers have come up with many different, sometimes contradictory, marketing messages and scenarios<sup>2</sup>. Trying to make sense of the SaaS proposition and how it relates to the business is a challenge for dedicated architects and researchers, let alone time-poor IT managers.

In the midst of all this cloud confusion, the default response for many, especially those that don't have a lot of experience to guide them, is to be sceptical and rely on the intuition that years of experience provides. The end result is that most treat SaaS security as a perceived risk even though in many cases the on-premise capability is far from ideal.

This cautiousness evaporates once significant experience enters the equation. The viewpoint of the vast majority of the SaaS-experienced is that security is at least the same, if not better, than that delivered on-premise. This turnaround is not surprising. The survey respondents showed that large gaps exist internally in security tools and policies, as well as in the reliability and availability of business systems. These are areas that SaaS suppliers, provided that they are in business for the long haul and are not negligent in their service architecture and design, base their entire service offering around.

Buying into SaaS should not mean having to bolt on security and reliability as an afterthought. These are attributes that should be built into the service, and come as standard, although more advanced features may naturally come at higher prices. The providers can share the cost of the specialist investment across multiple parties, in much the same way that a golf course is more affordable when used as a member of a club, rather than constructing a course for exclusive use.

The issue then becomes one of due diligence and supplier selection. Despite the widely held belief that SaaS providers are much of a muchness, the reality is that they differ considerably in capability, culture, financial muscle, service offering and people. Different companies have markedly different experiences with providers of all shapes and sizes, both good and bad.

The upshot is, as with almost all IT projects, the ultimate success of a project is about knowing what the business requirements are, evaluating the offerings available and implementing the selected solution effectively. Because SaaS can be up and running very rapidly, the ability to quickly purchase and provision a solution is often confused with flexibility and choice. It is important to realise that few IT systems exist in isolation, and it is even more important in this age of choice to think of the longer term integration, management and support of applications and services.

When it comes to evaluating the security and privacy of SaaS providers, the same criteria should apply as for any on-premise solution. In fact, any criteria that are applied to the SaaS provider should also be applied to on-premise solutions as well - after all there are large gaps in the desired levels of security tooling and policy. Applying more stringent standards to only a part of the infrastructure may leave a number of risks and vulnerabilities.

Ultimately, business reasons will be the main driver behind increased SaaS adoption. Successful implementations will mean getting your act together internally to know what the business needs, performing effective supplier due diligence and selection, and implementing SaaS in a structured and organised manner rather than viewing SaaS as a set-it-and-forget-it silver bullet.

## References and further reading

---

The following documents referred to in this report are available for free download from the Freeform Dynamics website:

### **1. Risk and Resilience**

The application availability gamble

<http://www.freeformdynamics.com/fullarticle.asp?aid=373>

### **2. But is that really cloud computing?**

The problem of ill-defined terminology

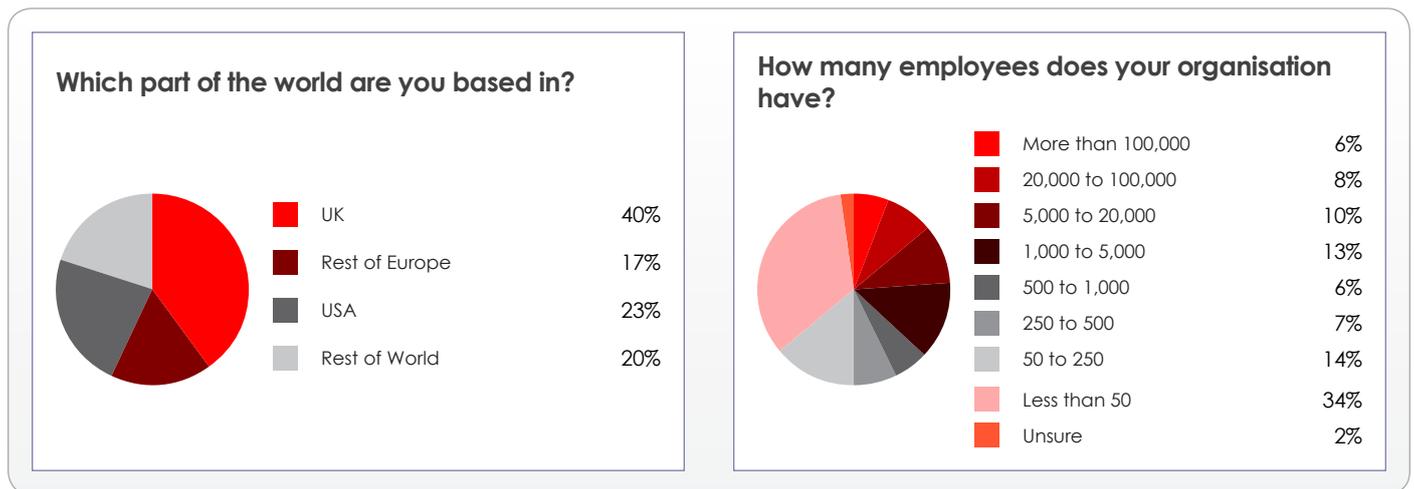
<http://www.freeformdynamics.com/fullarticle.asp?aid=1068>

## Appendix A: Sampling and Methodology

Feedback was gathered via an online questionnaire published on The Register news and information site ([www.theregister.com](http://www.theregister.com)). The respondents – totalling 510 – were largely IT and business professionals, representing a good cross section of job functions, and working in a range of different industry sectors.

The composition of the sample by organisation size and geography is as follows:

### Sample Composition



Note that the usual caveats to do with online research apply to this study, namely that respondent profiles are self-declared and the 'self-selection' sampling process is likely to have skewed the sample towards those with an interest in or knowledge of SaaS. Neither of these factors, however, can reasonably be expected to have had an impact on the conclusions outlined in this report.

### Acknowledgements

Our thanks go to all those who participated in the study, whose feedback has been invaluable in providing insights into the practicalities and opportunities in this interesting, diverse and complex area.

## About The Register

The Register started life as a daily news operation on the web in May 1998. On the first day, 300 readers visited; in 2007 more than 5 million unique readers visit the site every month.

The Register's blend of breaking news, strong personalities, and its accessible online execution, has made it one of the most popular authorities on the IT industry.

With an international team of journalists and columnists, The Register reports on the IT industry from the inside out – covering everything from enterprise software to chip developments.



## About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit [www.freeformdynamics.com](http://www.freeformdynamics.com) or contact us via [info@freeformdynamics.com](mailto:info@freeformdynamics.com).



## About Google

Google Apps is an enterprise-ready suite of applications that includes Gmail, Google Calendar, Google Docs and Spreadsheets, Google Sites, and Google Video. Google Postini services make email systems more secure by blocking spam and other intrusions before they reach email networks, and by providing encryption and archiving to help meet compliance requirements. Visit [www.google.com/a](http://www.google.com/a) for more information.



## Terms of Use

This document is Copyright 2011 Freeform Dynamics Ltd. It may be freely duplicated and distributed in its entirety on an individual one to one basis, either electronically or in hard copy form. It may not, however, be disassembled or modified in any way as part of the duplication process.

The contents of the front page of this document may be reproduced and published on any website as a management summary, so long as it is attributed to Freeform Dynamics Ltd, and is accompanied by a link to the relevant request page on [www.freeformdynamics.com](http://www.freeformdynamics.com). Hosting of the entire report for download and/or mass distribution of the report by any means is prohibited unless express permission is obtained from Freeform Dynamics Ltd.

This report is provided for your general information and use only. Neither Freeform Dynamics Ltd nor any third parties provide any warranty or guarantee as to the suitability of the information provided within it for any particular purpose.