quocirca
Business and IT Analysis

From NO to KNOW

The secure use of cloud-based services

July 2015

Attitudes to cloud-based services vary, but over time there has been increasing uptake as the benefits are recognised by more and more businesses. Those in the vanguard recognise that there is ground work to do; certain security measures must be put in place to enable safe use of cloud-based platforms and applications. At the other end of the spectrum there is investment in security too, as measures are taken to try and limit access to cloud-based services.

However, the days of these conservatives are numbered as digital natives move into IT-management and show the organisations they serve the value of business processes that *live in the cloud*. They must stop saying NO and move to a position where they KNOW what users are doing and where data is going, freeing the organisation they serve to benefit from cloud-based services.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: Bob.Tarzey@Quocirca.com

Rob Bamforth
Quocirca Ltd
Tel: +44 7802 175796
Email: Rob Bamforth@Quocirca.com

Executive Summary

From NO to KNOW

The secure use of cloud-based services

There are few organisations left that believe they can hold back the tide of cloud-based services flowing into their businesses. For many organisations, the use cases are now overwhelming and the choice is not whether to accept cloud-based services, but how well prepared they are for their use.

Cloud *enthusiasts*, *avoiders* and the middle ground	With regard to their attitude to the use of cloud-based services organisations can be placed in one of four broad categories. At one extreme are outright *enthusiasts* whilst at the other are *avoiders* that shun such services. In-between are *case-by-case users* that deploy cloud services in a controlled way and *supplementary users* that take a more casual approach.
Public cloud services will prevail	Since similar Quocirca research was conducted two years ago there has been a dramatic change. The proportion of UK businesses classing themselves as *enthusiasts* has doubled from 19% to 38%; *avoiders* have declined by two thirds from 23% to 10%. In-between casual *supplementary use* is giving way to controlled *case-by-case use*.
For many the case for cloud is overwhelming	The change is being driven by a number of positive use cases for cloud that make the direction of travel inevitable. These include on tap infrastructure to avoid over (or under) investment, the support for live-in-the-cloud business processes and the outsourcing of utility applications to third party specialists. If IT management does not support the move, lines of business will drive it anyway through shadow IT.
The value of knowledge and co-ordination	The confidence to use cloud-services is associated with confidence in IT security. This is driven by a number of factors including improved user knowledge and the ability to co-ordinate security policy and the response to incidents. These factors, together with investment in a range of advanced security capabilities, all have positive correlation with enthusiasm for cloud.
A wide range of security capabilities are deployed	The current research looked into the use of a wide range of security capabilities. These include general data protection measures (such as data loss prevention), user end point security and capabilities aimed more specifically at cloud use (such as secure proxies, policy-based encryption and access rights). In most cases cloud *enthusiasts* were the most likely to place the highest value of these security technologies.
Confidence in security is highest at the extremes	*Enthusiasts* of cloud services prepare the ground by investing in security on a broad front as an enabler. *Avoiders* invest too, but mainly in security measures that can block use, for example through end-point controls. *Supplementary users* are the least likely to have invested in most given security capabilities, whilst *case-by-case users*, like *avoiders*, focus in on end-point controls and secure login for the specific use cases they allow.
Motivators for investment in security vary by attitude	For all organisations, the top motivator for investment in security is regulatory compliance. However, cloud *avoiders* are most likely to cite this as the top issue, along with the insider threat. For *case-by-case users* customer compliance is high on the list, whilst for *enthusiasts* supporting external users and preventing hacking come to the fore as they expand their attack surface through their more open approach to the world.

Conclusions

The business case for the use of many cloud services is now so strong that if IT departments try to stem use, users will work their way around the measures that are put in place. IT management is there to enable the business and its role is to facilitate use through putting in place a security platform that gives them the confidence to move from saying "no" to saying we "know" who is doing what with our data.

quocirca

Introduction – characterising users of cloud services

Perceptions about public cloud computing are changing fast, as the economics become ever more compelling and the old guard are giving way to digital natives in the work place. In a recent survey Quocirca repeated a question asked three years ago where respondents were asked to choose one of five statements that most closely matched their organisation's views regarding the use of cloud-based services:

1. We make use of cloud based services whenever we can, seeing such services as the future for much of our IT requirement (**enthusiasts**)
2. We are evaluating the use of cloud based services to supplement in-house IT resources (**supplementary users**)
3. We do evaluate cloud based service on a case-by-case basis selecting them if they seem a better alternative to an in-house implementation (**case-by-case users**)
4. We avoid cloud based services (**avoiders**)
5. We proactively block the use of all cloud based services (**blockers**)

Figure 1: Which of the following statements most closely matches your organisation's attitude to cloud computing?

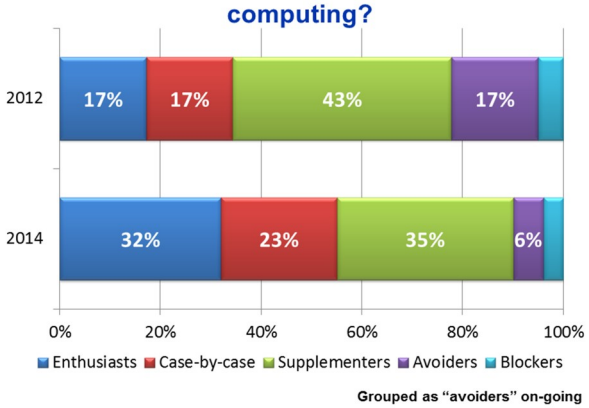


Figure 1 shows a clear direction of travel. The numbers of the most pro-active users, which Quocirca dubbed *enthusiasts*, has almost doubled from 17% to 32%, while the reticent *avoiders* and *blockers* (referred to collectively as *avoiders* on-going), has more than halved from 22% to 10%.

This report will look at the security measures enthusiasts take to enable the safe use of cloud-based services and those that avoiders take to prevent their use. The report will also look at another change that is clear from Figure 1, the drop from 43% to 35% of those that consider themselves *supplementary users* and the increase of *case-by-case users* from 17% to 23%. This change is more significant than might at first be expected as it shows a move away from casual use to more controlled access for specific use cases.

Cloud use-cases

The move from avoiders to enthusiasts will rarely be direct; such a major change can only occur if there is a radical change in IT management. However, once the benefits of cloud services have been seen through case-by-case use, the step to all-out enthusiasm is not such a big one.

There is a range of compelling use cases for the introduction of cloud services, which are hard for even the most reticent organisation to overlook. These can be considered in three categories.

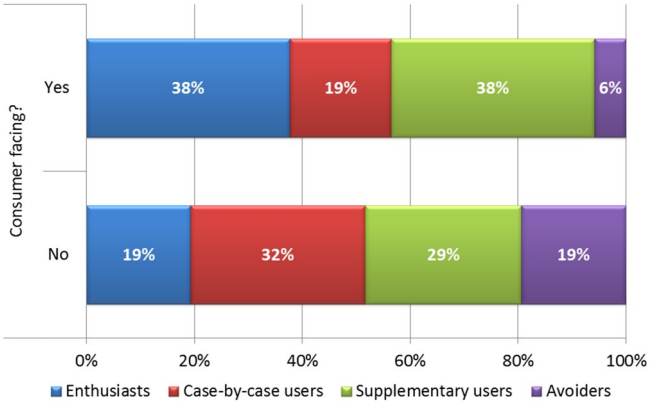
Avoiding over investment in infrastructure

The cost of data centre space, server and storage hardware and infrastructure software is easier to justify if it is to be fully utilised for running key business applications. Justifying investments is harder when such resources are likely to sit idle. Examples where the use of on-demand cloud service can avoid such a scenario include:

- Using cloud as an application test bed – when developing applications, scalability and performance can be tested
- Instead of investing in redundant hardware for failover and disaster recovery, a selected cloud infrastructure provider can be put on standby instead
- Cloud bursting to handle peak loads is becoming more common, for example to handle seasonal demand
- New business plans can be test run using applications running on cloud infrastructure avoiding under or over investment should the new initiative surpass or fail to meet expectations

The new research underlines the last two points above. Transaction volumes are especially hard to predict when dealing with consumers; consumer-facing organisations are twice as likely to be enthusiasts and one third as likely to be avoiders of cloud services (Figure 2). As well as the scalability, whether it is dealing direct with consumers or other businesses, the users are in the cloud so the applications may as well be to.

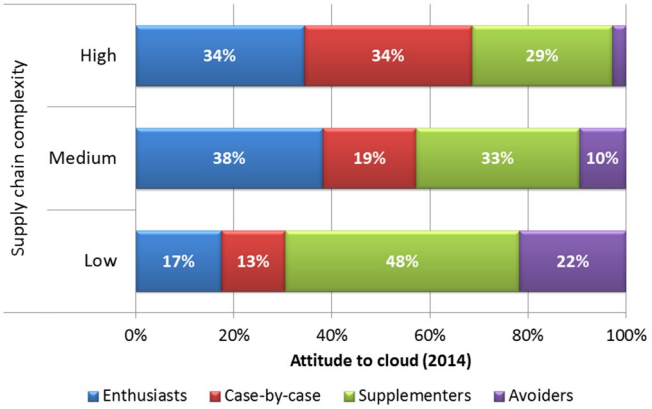
Figure 2: Cloud use and dealing with consumers



Business processes that live in the cloud

Some business processes fall in to this 'live-in-the-cloud' category really well. For example the management of information supply chains which was the topic of the second of the three briefs in this series[2]. Information supply chains may overlay physical supply chains in some sectors such as manufacturing and retail, but in other areas such as financial services and the public sector, information supply chains are often purely about the electronic exchange of data. The more complex the information supply chain, the more benefit is seen from using cloud-based services (Figure 3).

Figure 3: Cloud supports info supply chain complexity



Those with the least complexity are the least likely to turn to cloud. Those with the highest complexity are the most likely to be case-by-case users; specific apps for supporting specific users and processes, rather than wide reaching cloud access.

Utility computing and applications

Previous Quocirca research[1] has shown that many organisations see the benefit of using cloud services for utility requirements. This may be compute power and storage for the reasons just described, but also applications through the use of software-as-a-service (SaaS). Why should an organisation maintain skills for deploying and managing email, CRM, communications or collaboration applications in-house when there are many expert providers with proven platforms?

Furthermore, with the ever increasing need to support mobile users and interaction with outsiders via public internet access points, the applications have to be internet enabled with appropriate access controls. Cloud services are an easy way to achieve this and, with the maintenance of the platform or application effectively outsourced, in-house IT teams are left free to focus on core applications that truly differentiate a given business. In the long term this will shift IT workers with a technical bent to positions with service providers, whilst those working in end-user organisations will be more focussed on business process enablement through the use of whatever on-demand or in-house IT resources are best suited for the job.

Shadow IT

If IT management does not recognise the value of these use cases, the users and lines-of-business they are there to serve will. The phenomenon of users invoking their own cloud applications and service is widespread and IT needs to facilitate this so called *shadow IT* not block it. IT departments that are still trying to say NO, need to put in place the measures to KNOW who it is doing what with their organisation's data.

Preparing for secure use of cloud

In the first of the three research briefs[1] in this series, Quocirca looked at the confidence organisations had in data security and the measures taken to increase confidence, in particular:

- User knowledge about information security
- The deployment of advanced technologies
- The ability to co-ordinate security policy and the response to incidents

The correlation of confidence with views on cloud use (figure 4) may at first seem surprising. The most confident are the *avoiders*! However, remember, these organisations have taken an active decision to deter the use of cloud services and negative approach is easier to have confidence in; punitive IT usage policies, closed firewall ports, filtered web traffic, excluded user end-points and so on. Their confidence levels may be high today, but their stance is unsustainable in the long term.

Enthusiasts are also confident as they have put in place security measures to support their pro-cloud stance. They also have the most informed users (Figure 5). Both the extreme groups are also most confident about their ability to co-ordinate policy and incident response (Figure 6).

Confidence, knowledge and co-ordination in the middle ground all need boosting. With *case-by-case users* it might be expected to be higher, but they are likely to have focussed on their own specific use cases, but still be concerned that informal cloud use (shadow IT) is not well covered. Supplementary users are simply behind the curve and not investing in security.

Figure 4: Confidence in data security

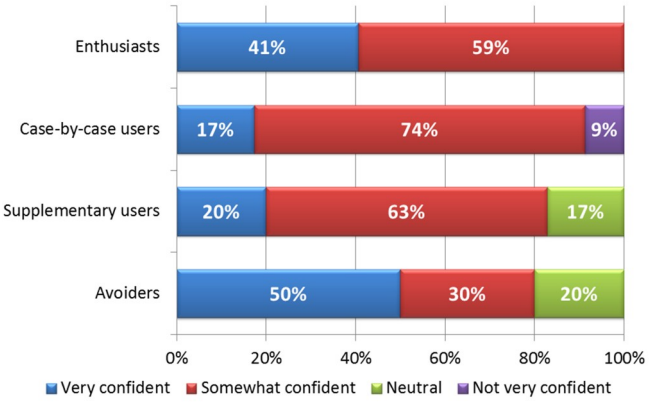


Figure 5: Knowledge of employees in general with regard to data protection

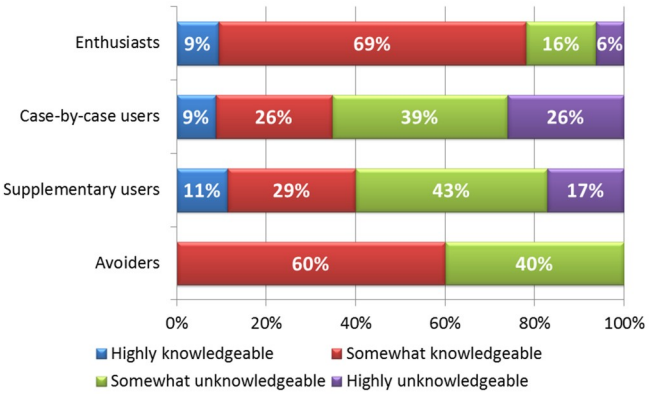
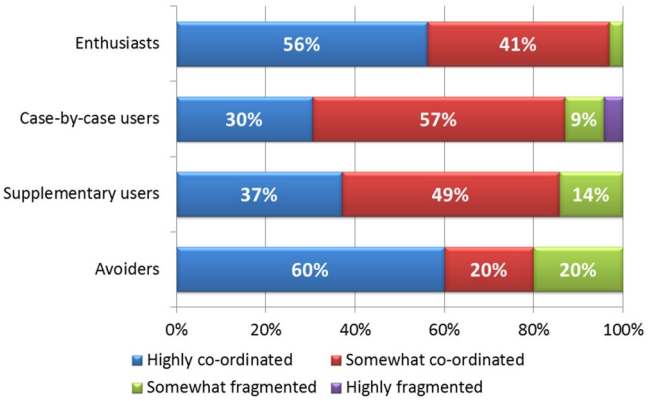


Figure 6: How co-ordinated is your organisation's activity against criminal hackers



The research looked at the likelihood of organisations having deployed a range of security capabilities. These were asked about and can be considered as three groups:

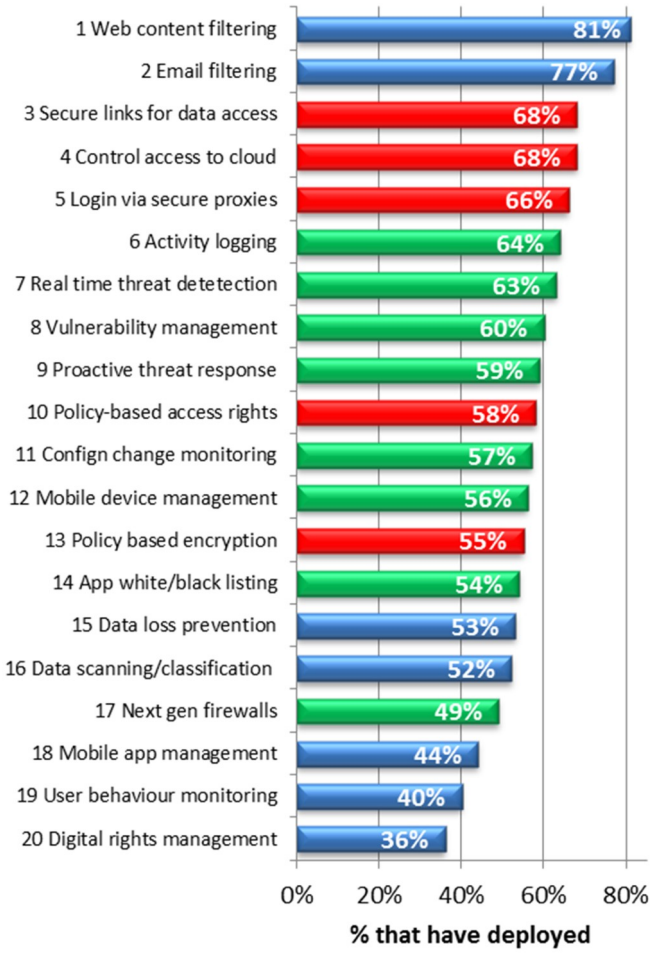
General data security measures: *which of the following data and/or user protection measures do you have in place?*
*7 options given – **blue in Figures 7, 9, 10, 11 and 12***

Specific measures for securing data use in the cloud: *which of the following measures do you have in place to make sharing data in the cloud more secure?*
*5 options given – **red in Figures 7, 9, 10, 11 and 12***

End-point security measures: *which of the following user end-point security and/or management capabilities do you have in place?*
*8 options given – **green in Figures 7, 9, 10, 11 and 12***

The overall deployment of these is shown in Figure 7. The first brief[1] in this series concluded that whilst email and web filtering were the most widely deployed, such measures are today's hygiene factors; they make the least difference when it comes to increasing confidence in data security. Other technologies, that were less widely deployed, such as data loss prevention (DLP) and specific capabilities to secure cloud use make much more of a difference to confidence. The first brief[1] also looked at the motivators for security investment (Figure 8). Regulatory compliance is the top overall motivator, however, as with all the motivators the degree to which this was so varies with attitude to cloud.

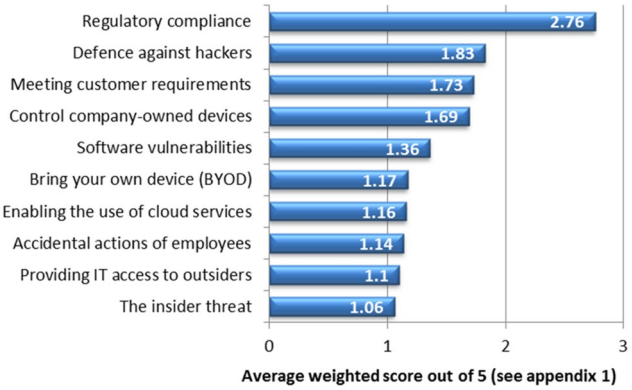
Figure 7: Use of data protection technologies (see reference



Enthusiasts (Figure 9)

Of the 20 security capabilities looked at *enthusiasts* were more likely than average to have every one of them in place (Figure 9). 3 of their top 5 were cloud sharing security capabilities; their bottom 5 included none of these. *Enthusiasts* go for cloud because it suits their business but they make sure it is safe. Compared to other groups, *enthusiasts* were more motivated to invest in security, to open access to outsiders and to prevent hacking. This makes sense; there is a strong positive correlation between cloud use and the use of open cross-organisational business processes: however, this also expands a given organisation's attack surface, hence more concern about being attacked.

Figure 8: Which of the following act as drivers for investing in data security for your organisation?



Case-by-case users (Figure 10)

Case-by-case users are more selective. They turn to technology that restricts what users can do, especially on end-points. They are less likely than average to restrict general access to cloud as controls are embedded in the applications deployed for each uses case, for example they are more than twice as likely as other groups to be motivated to invest in security for customer compliance requirements. Their focus is on enabling specific processes, such as integrating the information supply chain, and less on enabling generic requirements such as the user desire to invoke shadow IT.

Supplementary users (Figure 11)

Just how laissez faire about security *supplementary users* of cloud services are can be seen in Figure 11. They are taking a dangerously casual approach. Of the 20 security capabilities looked at, they were less likely than average to have deployed all but two. That said, perhaps surprisingly, they were the most likely to rank cloud use as a top-5 motivator for investing in security. Perhaps this is something they know they really should be doing, but just have not got around to yet! They were also, by some measure, more likely to see supporting bring-your-own-device (BYOD) as a motivator for investing in security; another area where a casual approach to security is not sustainable, again perhaps recognition of something that needs to be done – soon.

Avoiders (Figure 12)

Avoiders turn to DLP to control data movement as part of their efforts to minimise their perceived dangers from cloud use. As might be expected they see less need for cloud access controls, with 3 of the five 5 capabilities investigated fall in their bottom 5. They are the most likely to see regulatory compliance as a motivator for security investment, suggesting a rules driven overall approach. There are also by far the most likely to list the insider threat (through accidental and malicious actions) as a motivator for security investment, pointing to a general suspicion that IT management know best what users should be doing with IT. Perhaps it is time *avoiders* saw value in security as an enabler for the users.

Figure 9: Enthusiasts top 5 and bottom 5 *Showing the % above or below average they are likely to have invested in given security technology*

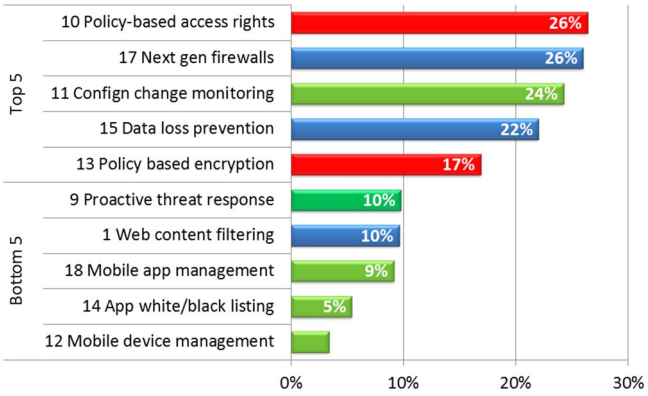


Figure 10: Case-by-case users top 5 and bottom 5
Showing the % above or below average they are likely to have invested in given security technology

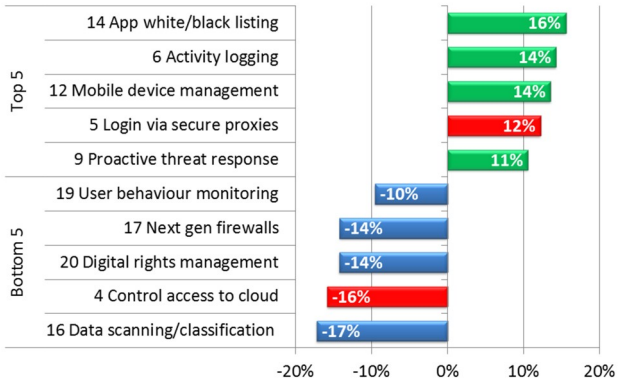


Figure 11: Supplementary users top 5 and bottom 5
Showing the % above or below average they are likely to have invested in given security technology

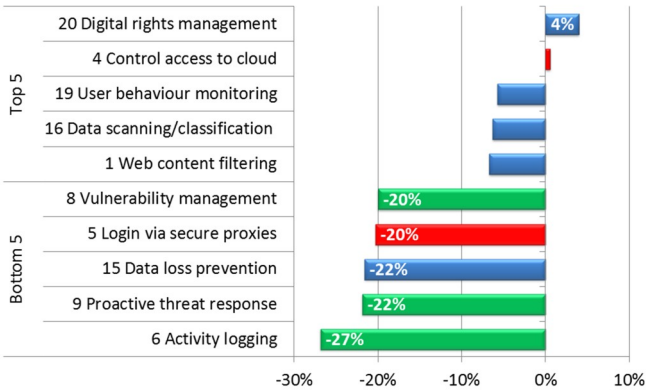
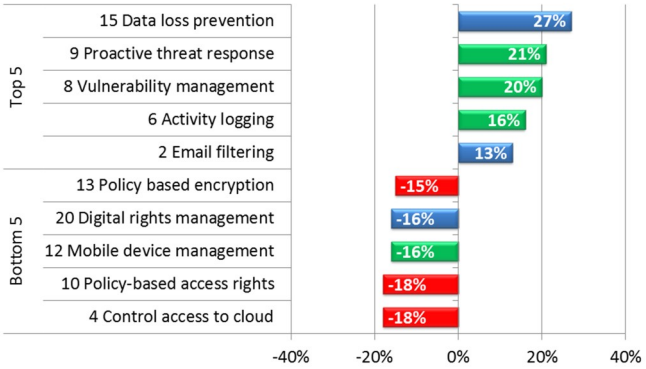


Figure 12: Avoiders top 5 and bottom 5
Showing the % above or below average they are likely to have invested in given security technology



Conclusions

Enthusiasts like the idea of using as much cloud as possible and see security as key to enabling this. *Avoiders* are wary of the cloud and see certain security technologies as effective for controlling use. *Case-by-case users* focus in on particular use cases, for example customer facing applications, and they make sure they are deployed effectively and securely. Those that see cloud as supplementary to in-house use are the least likely to have thought through cloud security taking a perhaps too casual approach, but are perhaps aware of the short-coming of their current approach.

However, the truth is that for most organisations a conservative stance is not a long term plan. If they do not recognise the value of and support the uptake of cloud-base services their users and lines of business will. They need to start preparing for this and putting in place the security measures that will allow them to move from NO to KNOW. In the not too distant future, all organisations will be making widespread use of cloud-based services and the distinction between *enthusiasts* and *avoiders* will be unnecessary.

References

1 – Room for improvement – link to be provided
2 – Strengthening the information supply chain

Appendix 2 – Calculations

Weighted averages used in Figure 8
Respondents were asked to select the five most important issues from a list of ten, ranking them from 5, the most important, to 1, the least important. For each respondent, the five unselected issues were scored 0. Across the 100 responses a weighted average was then calculated. If all respondents had ranked the same issue as most important it would have scored 5, if none had ranked any one given issue it would have scored 0.

Appendix 1 – Demographics

All respondents were from UK-based businesses. The industry sectors, business sizes and job roles are shown below.

Figure 13: Industry sectors by size

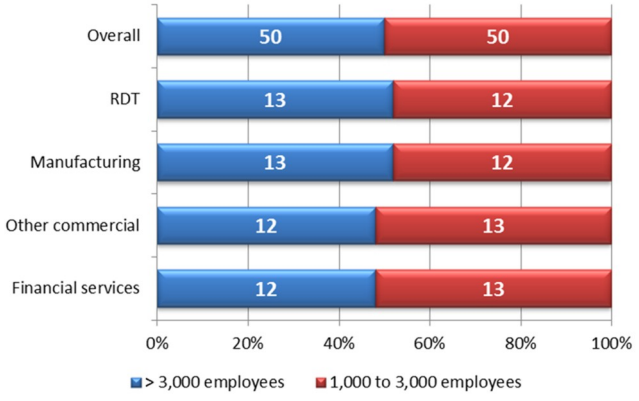
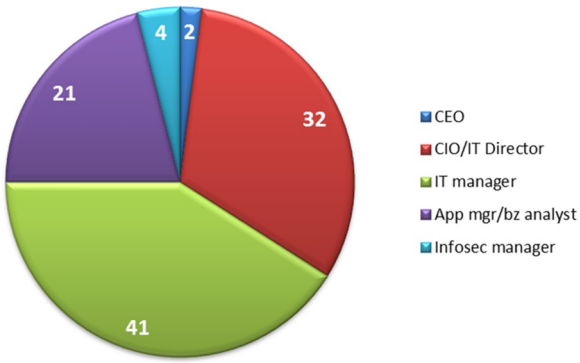


Figure 14: Job roles (actual sample numbers)



About Digital Guardian

Digital Guardian offers security's most technologically advanced endpoint agent. Only Digital Guardian ends data theft by protecting sensitive data from skilled insiders and persistent outside attackers. For over 10 years we've enabled data-rich organizations to protect their most valuable assets at the endpoint. Our unique contextual awareness, transformative endpoint visibility, and flexible controls let you minimize the risk of data loss without slowing the pace of business.

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations with regard to information security.

The report draws on Quocirca's research and knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create more secure information supply chains.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

quocirca