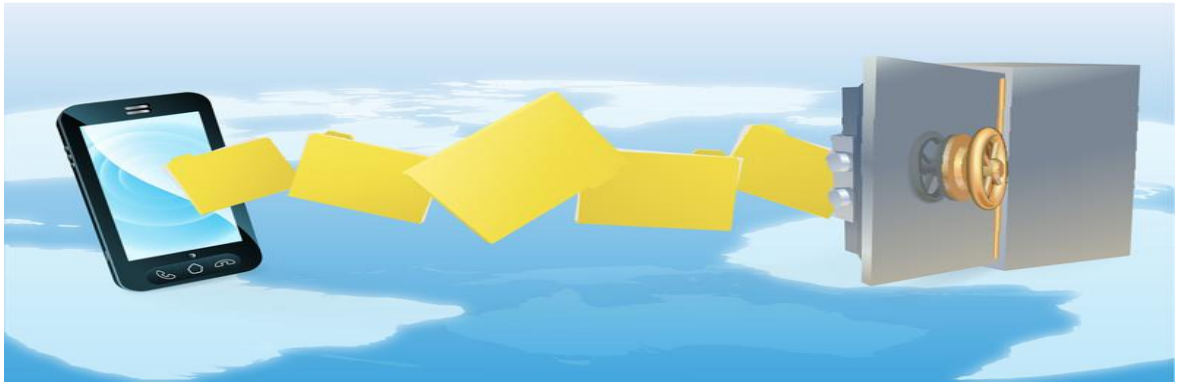
quocirca

Business and IT Analysis



Room for improvement

Building confidence in data security

March 2015

Businesses have no choice but to engage online with users from external organisations and mobile workers; that is the way the world now operates. Transacting safely and ensuring compliance rely on a high level of confidence in the data security measures that are in place. These include informed users, advanced technology and the ability to co-ordinate both security policy and incident response.

This research report demonstrates the cumulative benefits of these measures. It should be of interest to IT security professionals and others impacted by the risk of data losses; ultimately, that is the directors and board members of any organisation.

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

Clive Longbottom
Quocirca Ltd
Tel: +44 7711 719505
Email: Clive.Longbottom@Quocirca.com

DIGITAL GUARDIAN
Formerly VERDASYS

quocirca

Executive Summary

Room for improvement

Building confidence in data security

There is no silver bullet for ensuring effective data security. Organisations that want to ensure they are able to transact safely and compliantly must put in place a series of measures that collectively engender the highest levels of data security. These include educating users, deploying advanced technologies, and having the ability to co-ordinate both policy and incident response.

Faltering confidence in data security	Only 29% of organisations are very confident in the data security measures they have in place. The remainder admit there is room for improvement. The compliance-driven financial services sector is the most confident. There are a range of measures that can boost confidence in data security. These include better user awareness; advanced data, cloud and end-point security tools; and the ability to co-ordinate policy and incident response.
The power of knowledge	There is room for improvement in knowledge about data security at all levels, including in the IT security team itself. Organisations with management and employees that are considered knowledgeable about security are three or four times more likely to say they are 'very confident' about data security than their less knowledgeable counterparts.
Deploy advanced security tools	Organisations that implement advanced data protection tools, such as data loss/leak prevention (DLP), are more than three times as likely to say they are 'very confident' about data security than those without them. The same is true of cloud security measures, such as the use of secure proxies and user/device profiling. Mobile device management (MDM) and other end-point security measures double the numbers saying they are 'very confident'.
Co-ordinate security policy and incident response	Those organisations that have a strong capability to co-ordinate defences against criminal hackers are three times as likely to report that they are 'very confident' about data security than those with a more fragmented approach. Co-ordinated defence against the insider threat doubles the numbers. Co-ordination is achieved through centralised policy management and integration and rationalisation of security tools.
Cumulative benefits	Assigning a composite security score based on user knowledge levels, deployment of tools and the ability to co-ordinate shows the cumulative effect of these measures. 63% of those with a 'very high' score say they are 'very confident' about data security; none of them say they are 'not that confident'. 30% of those with a 'very low' score are 'not that confident' in their data security. None of them are 'very confident'.
Fewer vendors and policy engines	Organisations with a 'very high' composite security score tend to deal with fewer security tools suppliers and have fewer repositories for security policies. This helps ensure consistent policy is implemented throughout their organisations and that it is co-ordinated centrally. Those with a 'very low' score also have fewer suppliers and repositories, but in their case this can be put down to a lack of technology.

Conclusions

Being able to safely share data online within and beyond your organisation is a necessary part of participating in modern day business processes. This requires multiple layers of data security to be in place, providing the confidence to transact and share data safely and compliantly.

Data security: a crisis of confidence?

Although recent headlines regarding incidents may suggest otherwise, UK-based businesses do not report a crisis of confidence in data security. However, they do acknowledge that there is much room for improvement. Only 29% are 'very confident' about data security, the majority of the rest being 'somewhat confident', with a minority being 'not that confident' (Figure 1).

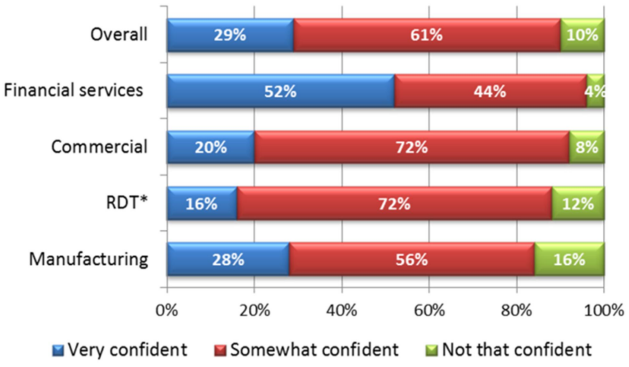
Confidence varies by industry sector; financial services being by some measure the most confident. This is probably a response to a high degree of centralised regulation of banks and insurance companies forced upon them by local, regional and global bodies, especially after the 2008 financial crash. Compliance is the biggest driver for investment in data security (Figure 2). In the retail, distribution and transport (RDT) sector, which is a prime target for cyber-crime, only 16% are 'very confident'. What can be done to increase confidence in data security?

This report looks into five areas for action, which the research indicates, if addressed together, always lead to higher confidence levels being reported. These are:

- User knowledge of security
- Technology for the security of data itself
- Technology for making the use of cloud-based services more secure
- End-point management and security technology
- Co-ordination of security policy and incident response

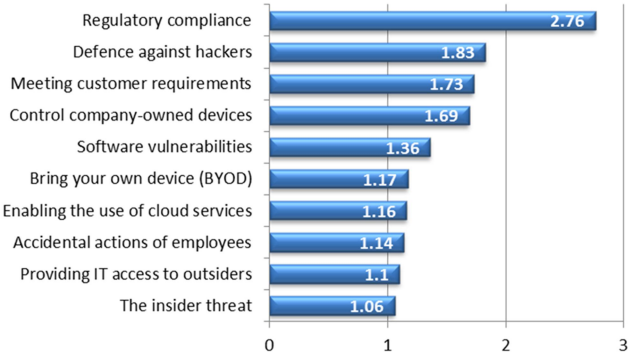
The report should be of interest to those tasked with managing data security for their organisation or those that are impacted when security measures fail. Of course this includes board members, who have the ultimate responsibility for security and compliance and therefore stand to lose the most from data losses. They also have the ultimate power to approve the investments in new data security measures that can free their businesses to transact and share data online with confidence.

Figure 1: How confident are you about the security of your organisation's data?



*RDT = Retail, distribution and transport (RDT)

Figure 2: Which of the following act as drivers for investing in data security for your organisation?



Average weighted score out of 5 (see appendix 1)

The power of knowledge

It is repeatedly said that good information security should start with making sure users understand their responsibilities; that they have the knowledge and skills to help minimise the chances and impact of security breaches. There is room for improvement at all levels, including in the general IT teams of most organisations (Figure 3).

Of course, caution is needed when considering the views held by one group of people about the capabilities of another. The respondents to this survey were mostly senior IT managers (see Appendix 2). There was no evidence that they overrated their own capabilities compared to other groups. Worryingly, 39% did not consider their own IT security teams to be highly knowledgeable. Part of that may be due to the sometimes antagonistic relationship between IT security and the rest of IT; a problem in itself.

However, there is a clear link between knowledge and confidence in data security. Knowledgeable users boost the number saying they are 'very confident' as much as four-fold (Figure 4). Knowledge is good, but to increase confidence even further, it needs to be supplemented with technology.

Figure 3: How would you rate the data protection knowledge and skills of the following groups in your organisation?

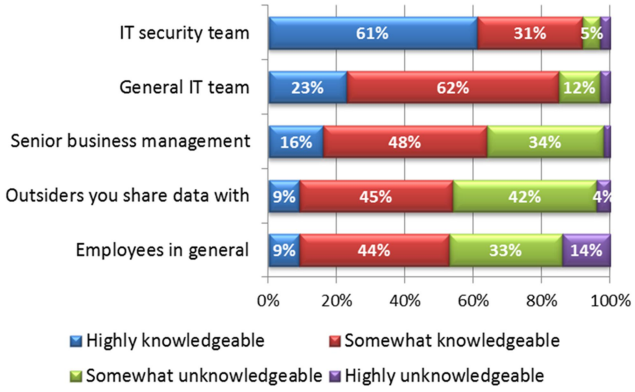
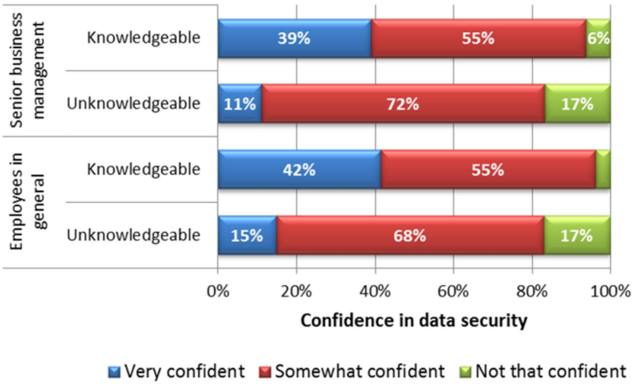


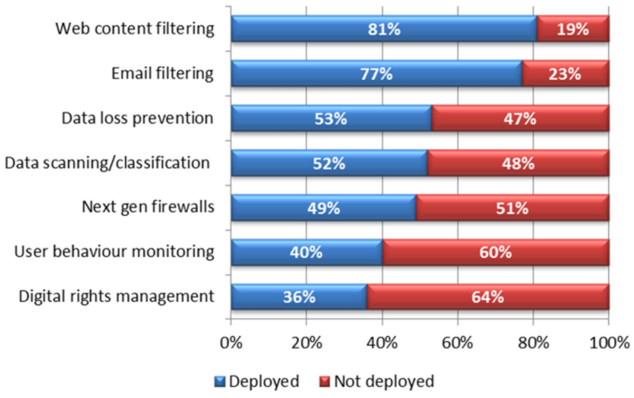
Figure 4: Knowledge of "*Employees in general*" and "*Senior business management*" versus confidence in data security



Advanced security tools

Information needs protecting wherever it is used, so many consider that protection measures should start with the data itself. Some technologies that enable this, such as web and email filtering, have been around for a long time, are widely deployed (Figure 5) and are best considered as hygiene factors. Other more advanced technologies such as data loss/leak prevention (DLP) are less widely used. However, it is these that do the most to increase confidence in information security. DLP can boost the number saying they are 'very confident' three-fold compared to email filtering, which does so by about 50% (Figure 6).

Figure 5: Which of the following data and/or user protection measures do you have in place?



Specific measures to protect the use of data in the cloud also boost confidence. The majority of organisations say they have capabilities to control the use of cloud data sharing services (DLP is one of these) and other measures such as secure links, cloud proxies and user/device profiling (Figure 7). Having any one of these in place can boost the number saying they are 'very confident' in data security four fold (Figure 8).

Finally, there are measures that can be taken to manage and secure the utilisation of user end-points. Technology for doing so is widely deployed (Figure 9) and having any one in place can double the number that say they are 'very confident' (Figure 10). Technology clearly has a major role to play, but there can be a down side; too many tools can lead to lack of co-ordination.

Figure 6: Deployment of *Email filtering* and *DLP* versus confidence in data security

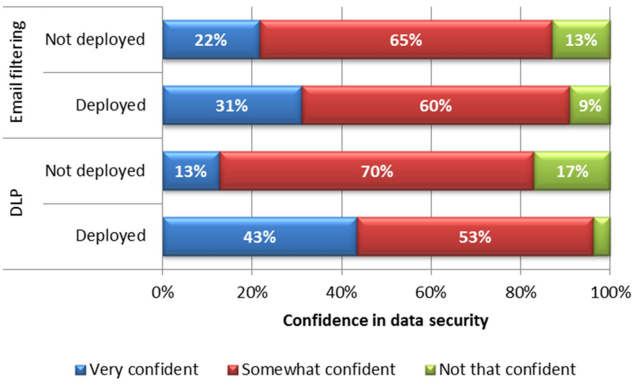


Figure 7: Which of the following measures do you have in place to make sharing data in the cloud more secure?

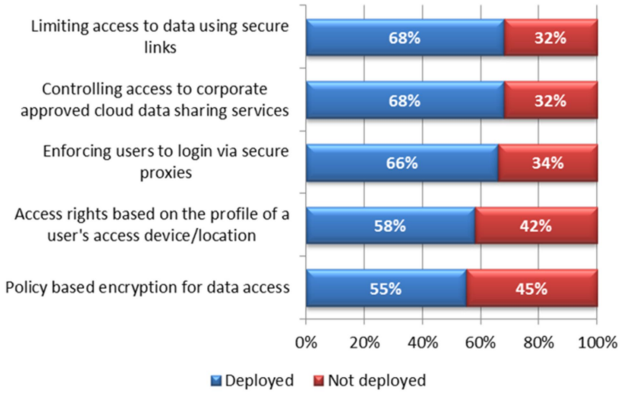


Figure 8: Deployment of *user/device profiles, secure proxies* and *secure links* versus confidence in data security

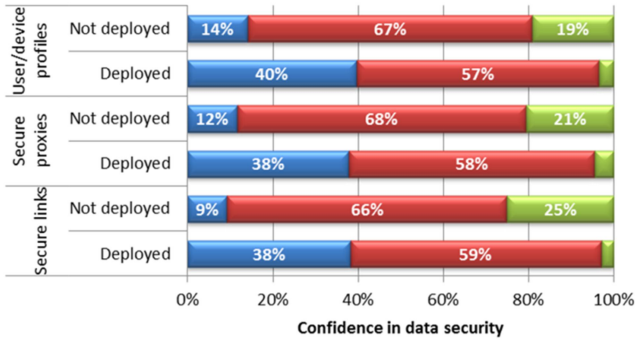


Figure 9: Which of the following user end-point security and/or management capabilities do you have in place?

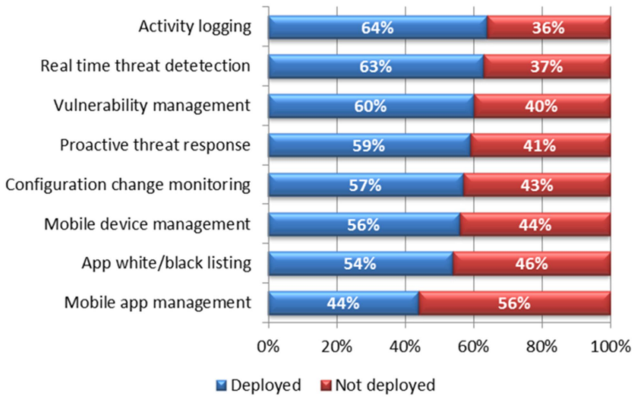
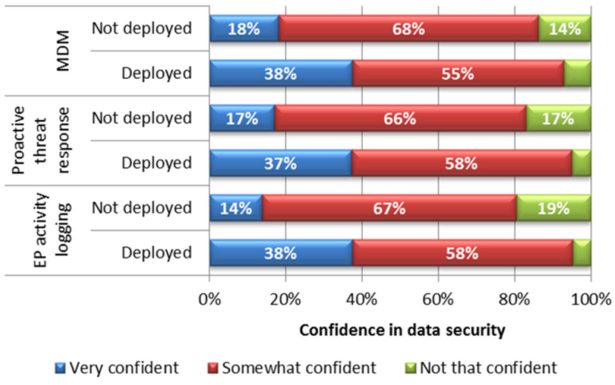


Figure 10: Deployment of *MDM, proactive threat response* and *end-point activity logging* versus confidence



A co-ordinated response

Knowledgeable users supported by advanced technology is all to the good, but not enough to achieve the highest levels of confidence. That requires a co-ordinated security policy and response to the varied threats extant in cyber-space. For example, ensuring sensitive data is not leaked must start with users understanding their responsibilities, but many will still carelessly fall short of expectations. DLP tools can detect and prevent some misuse of data and provide feedback into the education process, reminding users of the rules.

Ultimately, even sensitive data must be shared, often with users from external organisations and employees working offline and/or remotely. This often means using tools from multiple vendors, for example one to secure data use in the cloud and another for securing data on user end-points. One danger with multiple toolsets is that policy implementation becomes fragmented and inconsistent. Avoiding that requires co-ordination of policy across multiple repositories or, better still, to have a single shared repository.

This is especially true when the rule breaking is malicious. Insiders that want to steal data will seek ways around security and ignore warnings if they think they can get away with it. This requires co-ordinated monitoring and auditing of the use of data in all places. This is not only to be able to record that data has been compromised, but also to show that a user has abused their privileges and there is hard evidence to take appropriate action against them. Of course, most businesses would like to feel that they can trust their employees, so defences are mostly co-ordinated against external threats (Figure 11). Doing so has a big impact; boosting the numbers saying they are 'very confident' about data security three-fold (Figure 12).

Figure 11: How co-ordinated is your organisation's activity in defending against the following threats?

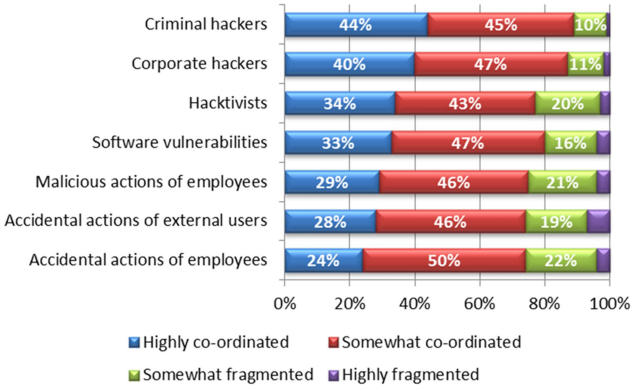


Figure 12: Co-ordination of responses to *criminal hackers* and *accidental action of employees* versus confidence

Putting it all together

Having the combination of higher knowledge levels, advanced data security technology and the capability to co-ordinate all this with the responses to cyber-threats should lead to the highest levels of confidence. This is exactly what is observed if confidence is measured against a composite security score (see Appendix 1). Each respondent organisation was given a score ranging from 'very low' to 'very high' (Figure 13).

No organisation with a 'very low' score felt 'very confident' and none with a 'very high' score reported being 'not that confident' (Figure 14). In line with other findings, financial services organisations had the highest composite security score (Figure 15). Those with a 'very high' composite index also deal with fewer vendors and have fewer repositories for security policies (Figure 16). This makes it easier to co-ordinate (and to change) policy. Those with a 'very low' composite security index, also have fewer vendors and repositories, however, in their case it is because they have not invested in many tools in the first place.

Figure 13: Composite score ranges based on five criteria (see Appendix 1)

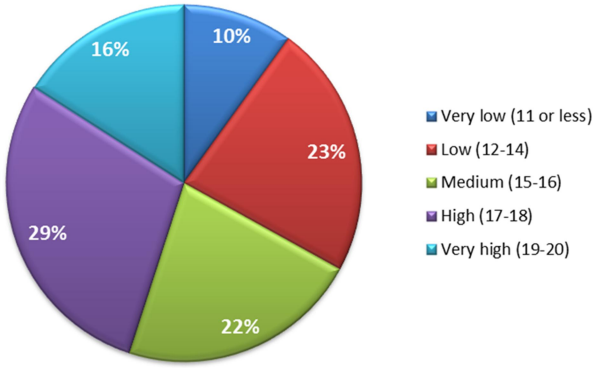


Figure 14: Composite security score and cumulative increase in data security confidence

Figure 15: Composite security score by industry sector

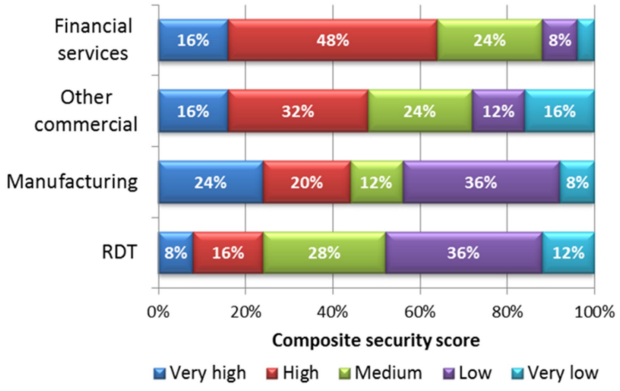
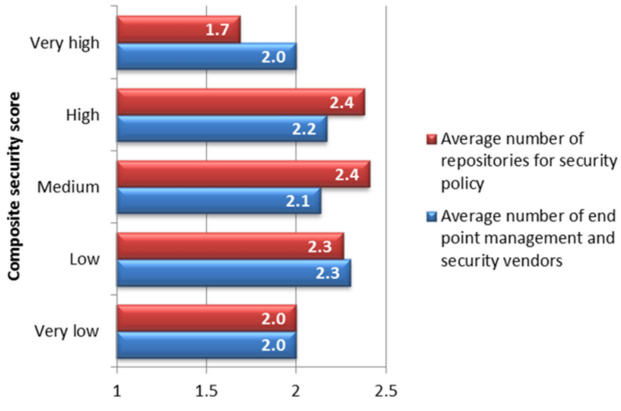


Figure 16: Composite security score and number of end-point tools/security policy repositories



Conclusions

Ensuring that a given organisation's use of IT is completely secure is not possible. There has to be a level of trust in employees and the external users that they are engaged with. IT systems have to have a level of openness and data must be shareable to be of value. However, multiple layers can be put in place to improve security.

This must start with the users themselves. Those that remain honest, can, if aware of their responsibilities, make a major contribution to data security. However, not all users can be trusted and there is a constant barrage of hackers trying to penetrate IT systems and steal data. Mitigating this threat requires a range of technologies, some of the most important of which, security of data itself, the safe use of cloud services, and end-point management have been covered in this report.

Finally, however much knowledge users have and whatever technology is in place, there is a danger that the responses to cyber-security incidents will be haphazard and policy implementation will be fragmented if the way security is deployed and managed is poorly coordinated. Get all three right – educated users, advanced technologies and coordination – and confidence levels in data security can soar.

Appendix 1 – Calculations

Weighted averages used in Figure 2

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.

Composite security score

The composite security score has five elements.

1. Knowledge of employees in general: highly knowledgeable = 4, knowledgeable = 3, unknowledgeable = 2, highly unknowledgeable = 1
2. Deployment of DLP: deployed = 4, planned next 12 months = 3, planned beyond next 12 months = 2, no plans = 1
3. User device and location profiling: deployed = 4, planned next 12 months = 3, planned beyond next 12 months = 2, no plans = 1
4. Deployment of MDM: deployed = 4, planned next 12 months = 3, planned beyond next 12 months = 2, no plans = 1
5. Co-ordination against criminal hackers: highly co-ordinated = 4, co-ordinated = 3, fragmented = 2, highly fragmented = 1

The maximum score is 20, the minimum is 4.

Appendix 2 – Demographics

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

Figure 17: Industry sectors by size

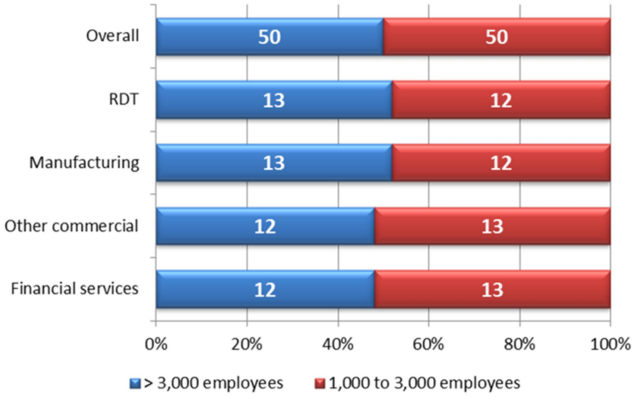
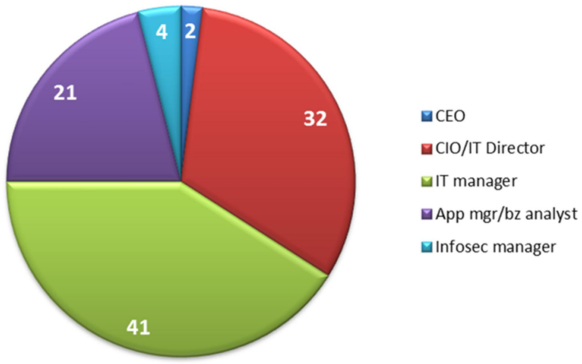


Figure 18: Job roles (actual sample numbers)



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 extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

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