quocirca
Business and IT Analysis

You sent *what*?

Linking identity and data loss prevention to avoid damage to brand, reputation and competitiveness

May 2010

Electronically stored information is a key asset for any organisation, but it is often insufficiently cared for—as the numerous high profile data breaches reported in recent years demonstrate. This failure to protect data is costly, not least because of the level of fines now being imposed by regulators. On top of this there is the reputational damage and loss of competitive advantage that usually ensue.

The technology exists today to link the use of data to people through enforceable policies. This allows a compliance-oriented architecture to be put in place based on widely accepted information security standards, such as ISO 27001. Doing so enables organisations to allow the safe sharing of information—internally and externally—ensuring both the continuity of business processes and good data governance.

This report examines the issue of data governance through the publication of new primary research that examines how well European businesses understand the risks and what steps they have taken to address them. The report should be of interest to those involved in ensuring the safety and integrity of information or those who manage business processes and operations that rely on it.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
bob.tarzey@quocirca.com

Clive Longbottom
Quocirca Ltd
Tel: + 44 771 1719 505
clive.longbottom@quocirca.com

Mariateresa Faregna
CA Inc
Tel: +39 2 90464739
mariateresa.faregna@ca.com

An independent report by Quocirca Ltd.

www.quocirca.com

Commissioned by CA

quocirca

You sent *what*?

Linking identity and data loss prevention to avoid damage to brand, reputation and competitiveness

Electronically stored information is a key asset for any organisation, but it is often insufficiently cared for—as the numerous high profile data breaches reported in recent years demonstrate. This failure to protect data is costly, not least because of the level of fines now being imposed by regulators. On top of this there is the reputational damage and loss of competitive damage that usually ensues.

- **The safe use of data is high on the list of issues that concern IT managers when it comes to IT security**
  After malware (rated at 2.9 on a scale of 1 to 5, where 1="*not a threat*" and 5="*a very serious threat*"), the issues of greatest concern with regard to IT security are internet use (2.8), managing sensitive data (2.7) and the activity of internal and external users (both 2.7). All three are linked; it is the sharing of data between users, usually over the internet, that is behind many incidents involving the loss of sensitive data.
- **Data compromise is costly and new regulations are expected to exacerbate this in coming years**
  The majority of organisations expect "*data privacy*" (ranked 3.2 on a scale of 1 to 5 where 1="*will decrease a lot*" and 5 = "*will increase a lot*") to be a major driver for regulatory change in the next five years. It is second to "*national government*" bodies (3.3), which are responsible for many such regulations anyway.
- **Cloud computing and new communication tools underline the need for a pervasive data security**
  The growing use of on-demand internet-based IT services means data is increasingly managed by third parties; consequently data security practices need greater reach. The variety of tools used to share data is also increasing, meaning that perimeter security is no longer enough and policing each communication medium separately is impractical. Only with corporate email is there a reasonable level of confidence that controls are in place.
- **IT departments struggle to deal with compliance issues and seem either unaware of how technology could help or are unable to convince the business of the inherent risks that justify required investments**
  Lack of time and resources (both ranked 2.8 on a scale of 1 to 5 where 1="*not a problem at all*" to 5="*a very great problem*") followed by a plethora of manual processes (2.8) mean IT managers find it hard to address many of the compliance issues they face. The majority do not seem to have an "*overall compliance vision*" (2.7) that could alleviate the problem.
- **Implementing a compliance-oriented architecture (COA) would help alleviate this**
  A COA is defined in this report as "*a set of policies and best practices, enforced where practicable with technology, that minimise the likelihood of data loss and that provide an audit trail to investigate the circumstances when a breach occurs*".
- **A COA requires three fundamental technologies to be in place**
  First a full identity and access management system (IAM), deployed by just 25% of the respondents; second, the ability to locate and classify data, and third, data loss prevention (DLP) tools that provide a way to enforce policies that link people's roles to the use of that data. Many DLP tools include data search and classification capabilities, with 25% of respondents already having deployed such tools.
- **Those that have deployed the elements of a COA recognise the benefits**
  Over 40% of those that have deployed full IAM say they have no concern about the safe deprovisioning of employees, compared to only 3% of those without full IAM. Approaching 90% of organisations that have deployed DLP say they are well prepared to protect intellectual property and personal data; for those without DLP the figure is under 30%.

Conclusions

The technology exists today to link the use of data to people through enforceable policies. This allows a compliance-oriented architecture to be put in place based on widely accepted information security standards, such as ISO 27001. Doing so enables organisations to allow the safe sharing of information—internally and externally—ensuring both continuity of business processes and good data governance.

quocirca

CONTENTS

quocirca

1. Introduction and target audience

Information is the life blood of any business and, just as good quality blood needs to be kept flowing in a regulated manner in a healthy creature, so too does information in a thriving business.

Businesses also need to regularly share information with each other, driving the cross-organisational business processes that keep suppliers trading and governments providing co-ordinated services to citizens.

However, whilst doing this, businesses also need to ensure they are protected from a threat that lies within the electronic storage and use of information; the possibility that it may—be it by accident or design—end up in the wrong hands. When it does, the consequences can be costly and damaging.

How confident are European businesses that they can keep information flowing, whilst ensuring they do not become the victim of a data breach and to what extent are they using technology to achieve these goals?

This report aims to answer these questions and should be of interest to those involved in ensuring the safety and integrity of information or those who manage business processes and operations that rely on it.

The report provides peer review, through the publication of new research, that shows where organisations from different industries and countries stand on these issues.

The research involved 270 interviews with senior IT managers working for businesses from 14 countries across Europe, each employing more than two thousand staff. The research covers 4 main industry sectors: financial services, manufacturing, government and telecoms & media (see Appendix 2).

2. The need for data security

For those charged with managing IT security, malware remains the single greatest overall concern as it becomes more sophisticated and geared towards fast profits through stealing of data. Beyond malware, there is not much to choose between the next three issues (Figure 1). All are related to the use of data; the internet, the main way data is shared externally; internal users (what might they be doing with data?) and the compromise of sensitive data itself.

Figure 1: To what extent are the following a threat to IT security in your organisation?

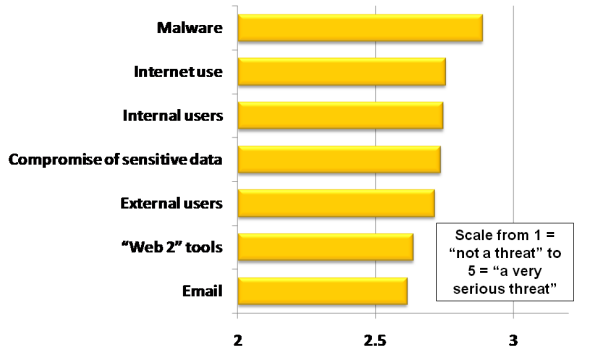
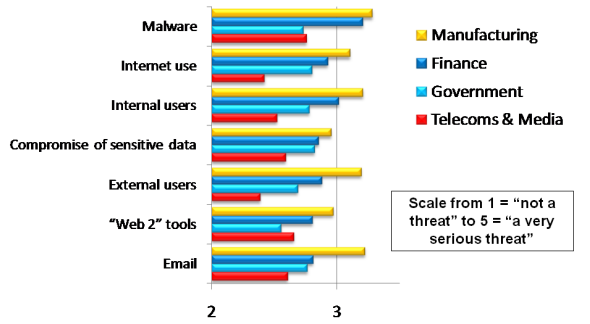


Figure 2 shows the same data broken down by industry. It is clear that issues with regard to data security are more pressing for some sectors than others.

Figure 2: To what extent are the following a threat to IT security in your organisation?



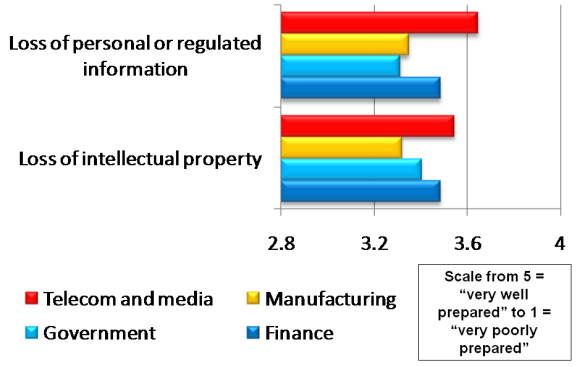
Manufacturers feel the most vulnerable, expressing the highest level of concern in all areas; this is perhaps because they worry more than their counterparts elsewhere about protecting their intellectual property (IP).

The financial sector is not far behind; just as with the overall sample, showing the greatest concern about internet use, internal users and the compromise of sensitive data. Telcos are the least concerned, perhaps because they are already highly regulated and see the safe handling of data as a core business activity.

Figure 3 shows how well different industries feel they are prepared to protect themselves against the loss of personal or regulated data and IP.

Manufacturers do indeed show the most concern about protecting IP and, given the concerns the financial sector has about users and the sharing of data, it seems poorly prepared too. Government scores lowest when it comes to personal and regulated information, which many of the citizens they serve will be aware of, given the number and scale of recent data leaks involving personal data about them.

Figure 3: How well prepared is your organisation to protect against the following risks?



One of the most high profile examples has been the loss in the post in November 2007 of a CD by the UK's HMRC (Her Majesty's Revenue and Customs) to which the private details of 25 million families had been copied.

One might not be surprised by the finding that telecoms and media companies, given the open nature of their networks and their technical expertise, are the best prepared to protect data. However, when it comes to internal use of data, a recent incident at T-Mobile (see Section 3) shows that telcos, at least, are not infallible.

Section 5 of this report will go on to show that despite the widespread availability of security tools to address all of these issues, deployment of them is at a low level by organisations in all four sectors covered in this report.

3. The consequences of data compromise

On top of the overriding concern of cost, there are three main things that worry businesses should sensitive data get in to the wrong hands;

1. Being in breach of regulations and/or a legal contract of some sort.
2. Loss of competitive advantage.
3. Reputational damage.

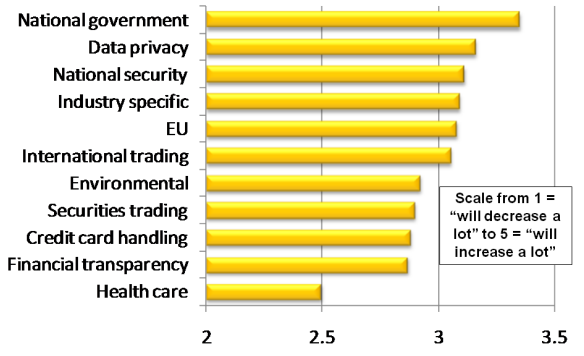
Many incidents are touched by all three of these; the T-Mobile incident is a good example.

In November 2009 it became apparent that the details of thousands of T-Mobile's UK customers had been stolen by an employee and sold to rivals—certainly not good for its reputation. The UK's Information Commissioner's Office (UK ICO) has taken an immediate interest as personal data is involved and privacy regulations have been breached (at the time of writing there has not been a ruling). Of course, for competitors to get hold of such information is clearly damaging and the subsequent bad press may deter new customers.

Perhaps the most important lesson about the T-Mobile incident is that the theft was perpetrated by an insider; this certainly looks like a case of complacency. The only way to defend against such actions is to better control what employees can and cannot do with data. For many organisations this requires a bottom up review of information security.

The long term overall costs for T-Mobile are not yet clear. An element of that cost is likely to be a penalty imposed by the UK ICO, which has been empowered, as of April 2010, to levy fines of up to £500K. However, such fines can be even larger; in another case of disks lost in the post, which came to light in 2009, a fine of £3 million was imposed by the UK's Financial Services Authority (FSA).

Figure 4: How do you see regulations in the following areas affecting your organisation over the next 5 years?



Few expect the regulatory climate to ease in coming years (Figure 4). Restrictions imposed by national governments are expected to increase the most. As many of these will dictate how sensitive personal data and breaches involving it

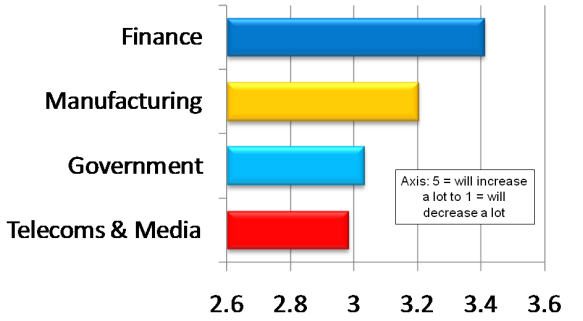
should be handled, anticipated increases in data privacy legislation also figure high on the list.

Some issues are low on the list because tough regulations have already been put in place, such as credit card handling and securities trading.

Others, such as environmental legislation, are lower because this survey was conducted during the 2009 recession when many businesses were more worried about their bottom line than their carbon footprint. Governments know they have to take action on climate change and much of this will be driven by regulating the way businesses consume resources.

Data privacy is of greatest concern to financial organisations as the consequences of losing their customer data are so serious (Figure 5). They possess large amounts of sensitive data that requires protection, including personal data, intellectual property and other non-public information. There have been a number of high profile cases of data loss from financial institutions, often leading to heavy fines.

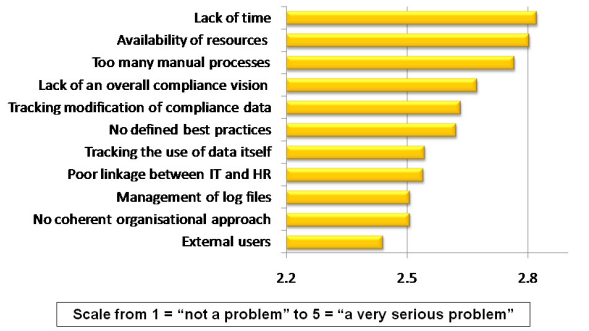
Figure 5: How do you see data privacy regulations effecting your organisation over the next 5 years?



A high profile example was the fines imposed on the US credit transaction handling company Heartland Payment Systems. It is to pay $60M to Visa and $3.6M to Amex for losses they incurred due to the breach of 130 million credit card user records in 2008. The company reported that it lost $129 million on data breach costs in its latest financial report and that it still has a reserve of $100 million for additional expenses on this case, which might bring the total cost of the breach to $229 million. In this case it was down to an external hacker (now in prison), but other, albeit so far smaller, fines have been imposed for breaches caused by internal users, as discussed earlier.

Indeed, the HMRC and T-Mobile incidents were all triggered by the actions of insiders. However, it is often necessary to grant access to internal data to outsiders, although, in this survey, controlling such external users was bottom of the list of problems organisations say they face when making sure they are compliant with the regulations that surround them (Figure 6).

Figure 6: How much of a problem are the following when your organisation tries to improve the way it manages compliance?



Topping the list are the lack of time and resources, followed by the plethora of manual processes and a lack of an overall compliance vision.

If businesses had a better understanding of how to address the issues relating to information security they might put "*lack of an overall compliance vision*" at the top of the list. Such a vision could reduce the number of manual process and, consequently, time and resources would be less of an issue.

The three issues listed at the start of this section—breach of regulations/contracts, loss of competitive advantage and reputational damage—would be mitigated if organisations could track the use of data better, which is surprisingly low down the list. All three can be addressed through deploying suitable tools as part of *compliance oriented architecture*.

4. A compliance-oriented architecture (COA)

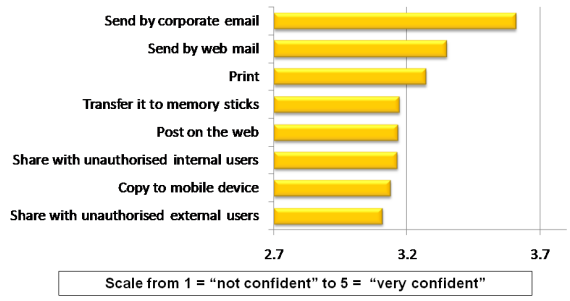
As businesses discover more and more ways to communicate, or at least try to keep up with their employees' propensity to do so, securing communication media on a case-by-case basis is no longer practical. To enable safe sharing of information, both internally and externally, whatever the medium of communication, requires a COA.

A COA can be defined as; "*a set of policies and best practices, enforced where practicable with technology, that minimise the likelihood of data loss and that provide an audit trail to investigate the circumstances when a breach occurs*".

The necessity to understand and address these requirements has become paramount in the last decade. Ten years ago, the internet was already in widespread business use, but its principal application, the web, was largely passive.

The main way information was shared was by corporate email, a single network channel (simple mail transfer protocol/SMTP) with some use of instant massaging (IM). The SMTP channel is relatively easy to monitor and filter and most businesses have invested in tools in the last decade to do this and are therefore relatively confident they have email under control (Figure 7).

Figure 7: When users have legitimate access to data how confident are you that you can control their ability to do the following?

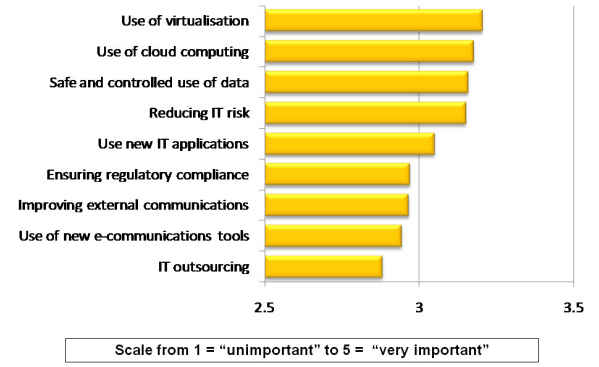


Today the use of the web is dynamic; blogs, webmail, social networking, web conferencing (so called Web 2.0 technologies)—countless ways to transmit data. There has been much less investment in technology to control web traffic, which is transmitted via a different protocol (hyper-text transfer protocol/HTTP). This has led to a reduced overall confidence in the safe sharing of information.

Furthermore, the very nature of the way IT is managed and delivered is changing rapidly. Many computing services are now being delivered on-demand over the internet.

These range from business applications (software as a service/SaaS), software platforms (platform as a service/PaaS) to basic infrastructure (infrastructure as a service/IaaS). These different models are often collectively referred to as cloud computing and are enabled by virtualisation. IT security is considered a key enabler of both (Figure 8).

Figure 8: How important do you think IT security is in enabling the following?



Cloud computing means not just that there will be even more data transmitted across networks, but that more and more of it will be stored on infrastructure managed and owned by third parties. Some fret about the security issues with the use of such services, perhaps unnecessarily, as the service providers will often have better practices in place than their customers, however it does underline the need to apply security policies at the data level.

This is not only necessary to protect data from falling into the wrong hands but also to ensure that some types of data remain within certain geographic boundaries. Some regulations require that certain types of personal data are not physically stored outside of a given legislative area.

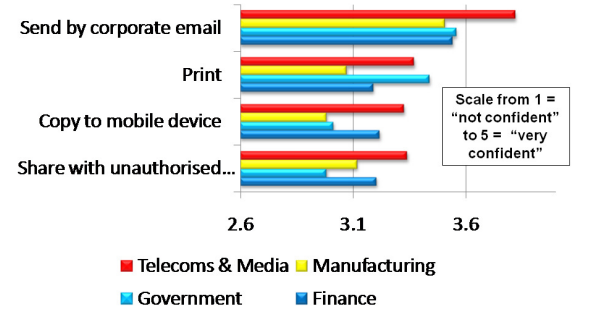
To achieve this it helps to define information storage and usage zones with understood risk. For example, highly sensitive data might be restricted to infrastructure that is managed behind the corporate firewall and only data of low sensitivity being suitable for processing and

storage on shared infrastructure from a cloud service provider. The categorisation will depend on the risks inherent in a given cloud service.

Understanding the type of data, and its classification, enables real time decisions to be made about what is and is not allowed to be handled in each zone. Employees cannot be expected to understand such issues; indeed they may be completely unaware that copying a sensitive document from one location to another is moving it from internally managed to third party infrastructure, where it might be in contravention of corporate policy.

In all the areas listed in Figure 7, telco and media companies were the most confident that they could control how their users shared data, again reflecting that the transmission and sharing of data is their core business (Figure 9). Finance, public sector and manufacturing were all less confident, except in one odd area; public sector organisations were more confident than others about their ability to manage the use of printed materials.

Figure 9: When users have legitimate access to data how confident are you that you can control their ability to do the following?

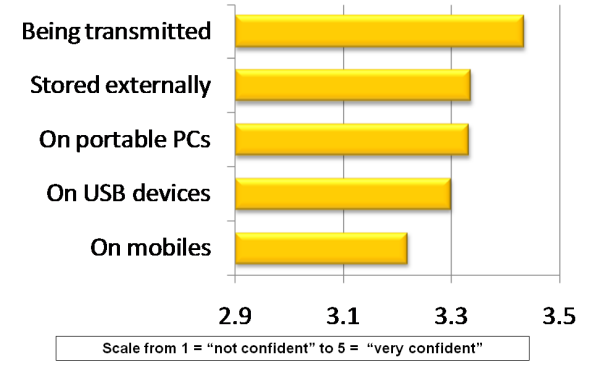


Such confidence may be misplaced; network printers, through information stored on their internal disks and memory or the output they produce, are a security risk. Unclaimed output has certainly been a source of data leaks in the past. The higher confidence amongst government organisations may be because of their growing use of secure print services.

Employee productivity is an issue often raised when it comes to the use of internet-based communications tools, but is not the subject of this report. Whatever tools businesses believe are useful, for good reasons or bad, their employees will seek to use others too. So, rather than trying to police the internet and the ways users are communicating, it simply underlines the need to apply security to the data itself. This can only be done in the context of knowing who the appropriate users of information are, as policies regarding its use will vary by job role and individual.

Many businesses have a reasonable understanding of their users through the use of some sort of identity and access management (IAM) system. They tend to have a poorer view of their data, not knowing what is stored where and what is of true value (and therefore risk, if compromised). There is most concern about the security of data stored on mobile devices with their rapidly increasing disk capacity (Figure 10).

Figure 10: How confident are you that access to data is controlled at the following levels?

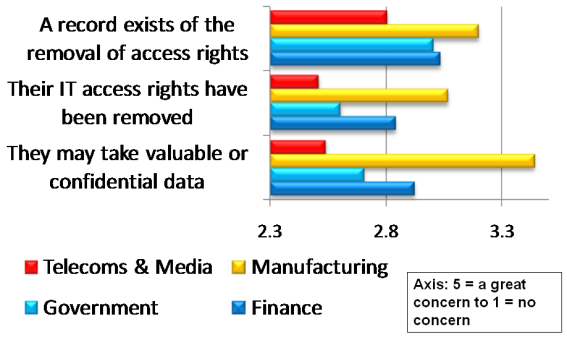


Many businesses have no linkage between their identity and access management tools and the way data use is governed, often treating the two as silos. This makes it hard to create and enforce centralised policies as to how people can use data and to track them as they do.

This last point is important; tracking the legitimate activities of those in given roles, and understanding how they are using information, enables fine tuning and improvement of a COA through continual feedback.

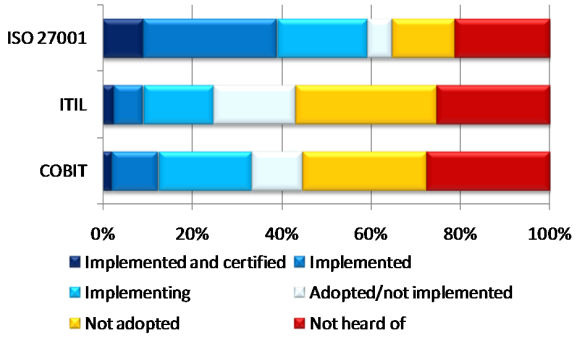
Having such systems in place also leads to improved confidence at a key stage in any business's relationship with an individual employee—their departure (Figure 11). Here, manufacturers show the most concern, presumably because of their worry about IP, followed by financial organisations with the large amounts of sensitive information they handle.

Figure 11: When your employees leave your organisation, how much do the following concern you?



Such concerns are well placed. In Nov 2008 a former Intel worker was indicted for stealing IP with an estimated value of $1B when he left to join rival chip manufacturer AMD. Another case of attempted IP theft emerged in July 2009, when a Goldman Sachs employee was charged with stealing computer code that automated the firm's high-volume trading on stock and commodities markets. The employee intended to make use of the software when he joined a rival employer.

Figure 12: Deployment of security standards and methodologies



Defining a COA is not something that needs to be done from scratch; there are frameworks for information management and IT governance that lay down good practice. One of the most widely adopted is ISO 27001, but there are others such as ITIL and COBIT (Figure 12).

These standards and guiding principles also help on the road to regulatory compliance. For example, many of the requirements laid down in the Payment Card Industries Data Security Standard (PCI DSS) overlap with controls specified in the ISO 27001 information security standard.

5. Use of technology

The examples laid out in the last section underline the three main threats that are inherent with data breaches discussed in Section 3; being in breach of regulations/contract, loss of competitive advantage and reputational damage. Technology can be used to underpin a COA and mitigate these, but few organisations are actually doing so.

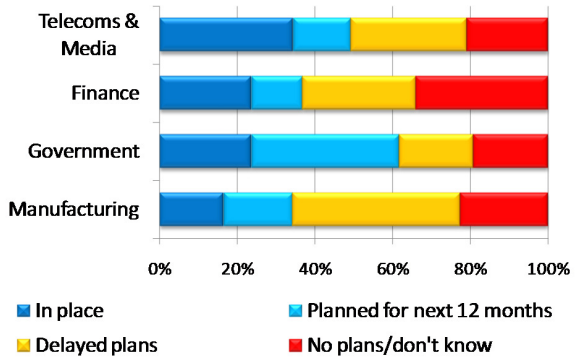
A COA requires three technology elements to be in place; identity and access management (IAM), data search/classification and the ability to enforce policies that link the two.

IAM provides the ability to understand people, their roles and responsibilities and to be able to define their privileges and access rights. This is more than simply a directory of individuals and needs to embrace both internal and external users.

IAM also enables the enforcement of access rights at runtime, applied to assets such as IT resources and applications. However, most IAM systems do not provide the ability to secure access to unstructured content. To achieve this, a strong link needs to be created between IAM and DLP technologies to provide identity-centric data protection.

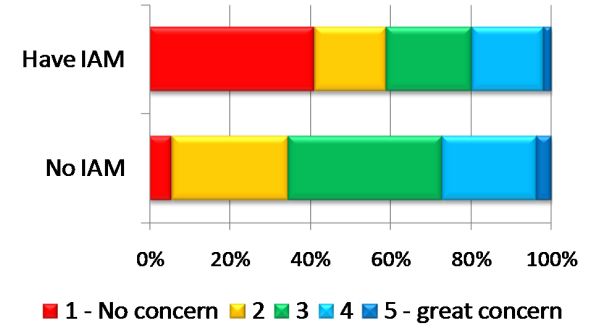
The majority of organisations do not have a full identity management suite in place (Figure 13).

Figure 13: Has your organisation deployed a full identity management suite?



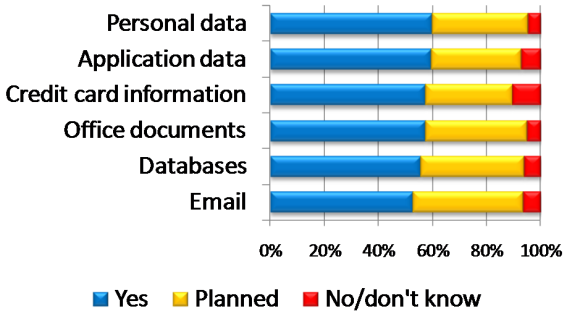
For those that do, not only do they have the first key part of a COA, they also overcome a common problem that often results in data loss; the safe deprovisioning of employees (Figure 14).

Figure 14: Levels of concern that access rights of departing employees have been removed relative to deployment of IAM tools



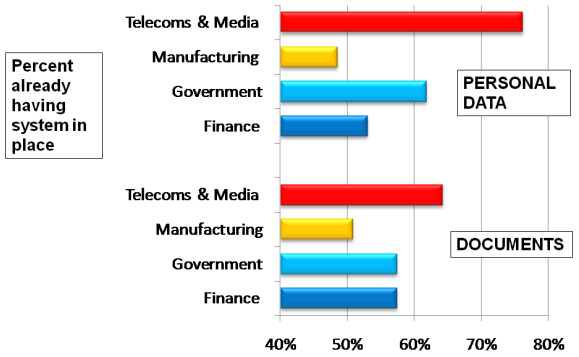
The second element of a COA is the need to be able to understand and classify data in the many places it may reside. Only 50% of organisations say they have such a capability in place (Figure 15), although the current research did not delve into the type of tools being used for this. If a business cannot identify its critical data, how can it protect it? This is exacerbated by the growing use of cloud computing, whereby some data assets will be stored on infrastructure provided by external providers, perhaps distributed across a number of locations.

Figure 15: Do you have a system for indentifying and classifying the following types of data?



Telecoms and media companies are the most likely to have data identification and classification in place for personal data and documents (Figure 16). The low level amongst manufacturers may reflect more exacting standards; given their concerns about IP, they seem to lack confidence in whatever technology they have had to rely on to date to protect this.

Figure 16: Do you have a system for indentifying and classifying the following types of data?



Understanding people and data is not enough. They need to be linked through enforced policies that control how data is used depending on a given user's role, privileges and access rights. This requires an ability to monitor data, recognise the sensitivity of various data elements—from whole files down to sentences, phrases and specific data types—and apply policies on a per-user basis. The technology that enables this has become known as data loss prevention (DLP).

As well as providing the capability to search for and classify data, DLP tools also police its use. The tools enable the inspection of content and enforcement of pre-defined policies depending on the rights of the individual concerned.

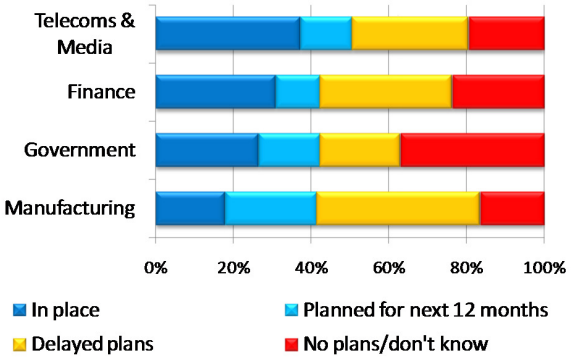
For example, documents containing the term "company confidential" can be blocked from being sent to external email recipients or being printed, except perhaps for managers above a certain level. Encryption can be enforced for the transmission of any data that contains credit card numbers.

DLP tools are also increasingly being used for information control purposes. Some organisations use the technology to identify and prevent price fixing, bid rigging and collusion. There are other, more positive, uses, such as making sure only the most recent version of public reports and brochures are distributed.

DLP tools were deployed by around 25% of the organisations interviewed for this survey, leaving the remaining 75% with no sure way of protecting from the threats posed by data breaches. DLP is most widely deployed by telecoms and media companies and least by manufacturers (Figure 17).

Given the responsibility that government organisations have for their citizens' data and the sensitive data held by financial services organisations, such low levels of deployment should be a concern for regulators.

Figure 17: Has your organisation deployed data loss prevention technology?



Manufacturers should also take an urgent look at DLP; the leading products in this area not only prevent unwanted copying, printing and transmission of certain data, but they also include the identification and classification capabilities required for a complete COA and the protection of IP.

The fact is that two of the areas where many organisations are weak in data governance—understanding data and enforcing policies regarding its use—can be addressed through a single technology investment: DLP.

DLP also enables the continuous tracking of how data is being used. This provides feedback to those managing the COA, ensuring critical data is available to those with legitimate need for access, understanding new usage patterns and redefining policy.

For example, a new partnership might mean that certain confidential documents can now be shared on a regular basis with employees of another organisation. This may lead to sudden rise in the blocking of the documents being sent by email, flagging the need for a change in policy.

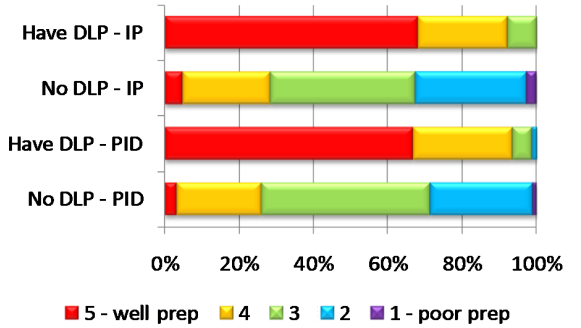
Making sure policy keeps pace with acceptable practice also makes it easier to spot anomalous behaviour and maintain adaptive access control mechanisms.

As IAM and DLP solutions get more tightly integrated, there will be significant advances in how information is secured. For example, at present, many web access management (WAM) tools use static access control mechanisms (users being explicitly assigned access to certain resources). Linking WAM with DLP technologies can enable dynamic, on-the-fly security decisions.

WAM will then have an adaptive, content-aware access control layer. This will simplify the securing of resources such as portals (e.g. Microsoft SharePoint). When a user tries to access a document, the WAM tools can make a call to a runtime DLP component to dynamically check if the content within the document is suitable for the requested use and appropriate action gets taken.

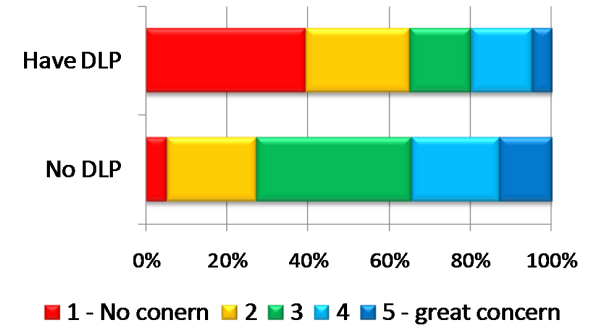
Adaptive access control approaches will also prove critical to securing cloud computing resources. Current static models will be too complex and expensive to maintain.

Figure 18: Confidence to protect intellectual property (IP) and personally identifiable data (PID) relative to use of data loss prevention (DLP) technology



The increased confidence that DLP can give an organisation should not be underestimated. Those that have it in place have far more confidence in their abilities to protect IP and personally identifiable information (PID) (Figure 18) and to prevent departing employees taking valuable data with them (Figure 19).

Figure 19: Concern about departing employees taking valuable or confidential or data with them relative to DLP deployment



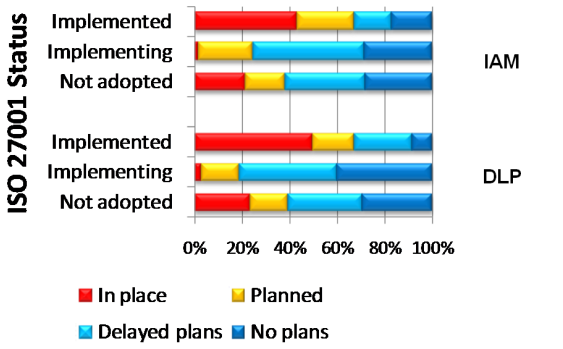
A COA cannot be implemented successfully without fostering a compliance-aware culture across a business. This underlines another valuable benefit of DLP tools; they can be educational—for instance alerting users that certain actions are in violation of corporate security policies. Ultimately, they will raise awareness and drive behaviour.

6. Conclusion—attaining the highest standards

This report has used the term COA to define a set of practices and tools that can be put in place to protect data. These involve linking people to data through a set of well defined and enforced policies.

The aim is to avoid the costly data breaches that can cause reputational damage, loss of competitive advantage and the ire and fines of the regulators. To achieve this, the deployment of a comprehensive set of IAM and DLP tools is recommended and this report shows that those that have done so reap the benefits of increased confidence in how they use and share data.

Figure 20: Adoption of ISO 27001 and deployment of DLP and IAM



A COA need not be invented from scratch but can be based on widely adopted information security standards such as ISO 27001. In fact there is a strong link between the two, as Figure 20 shows.

Organisations that have adopted ISO 27001 are more likely to have deployed full IAM and DLP tools; these help them put in place the controls specified by the standard.

It is interesting to note that those that have adopted ISO 27001 but have not completed its implementation are the least likely to have adopted IAM and DLP—clearly they are yet to discover how much these technologies can help. The fact that quite a few that have not adopted ISO 27001 have also put these two technologies in place merely suggests they are using different standards to help achieve a COA.

Either way, it requires an evolutionary approach to constantly improve the way data is managed to give an organisation the confidence to keep data flowing safely. Deploying the technologies that underpin a compliance-oriented architecture can help any organisation take a quantum leap along the road to better regulatory compliance.

Appendix 1: demographics

This Appendix shows how the 270 interviews were distributed across the country, industry, company size and job roles categories covered by the survey.

Figure 21: Countries covered in survey

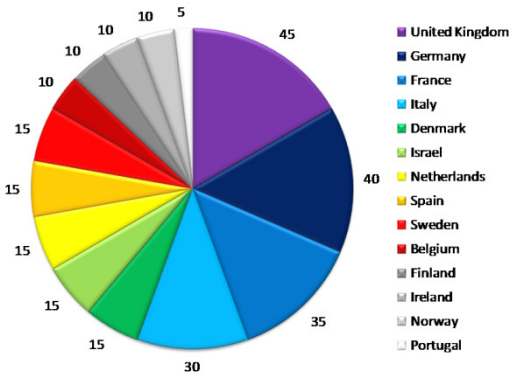


Figure 22: Company sizes covered in survey

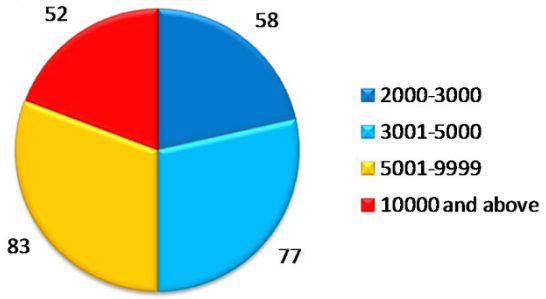


Figure 23: Business sectors covered in survey

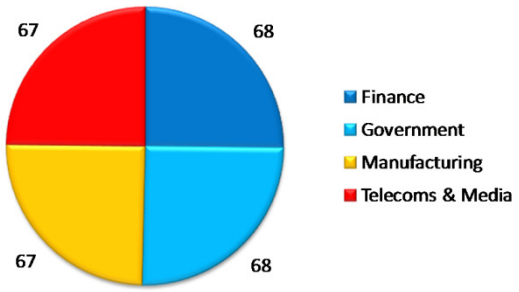
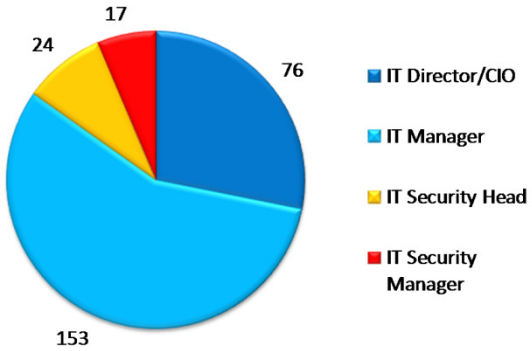


Figure 24: Job roles of respondents covered in survey



Appendix 2: IT spending trends by industry

This Appendix shows some more detail, by industry, of total IT spending and factors that limit security spending.

Figure 25: What proportion of your organisation's total IT budget is spent on IT security (excluding salaries)?

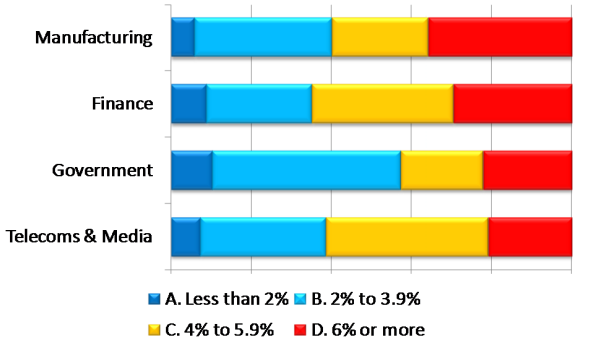


Figure 26: Is the proportion of your organisation's total IT budget spent on IT security increasing or decreasing?

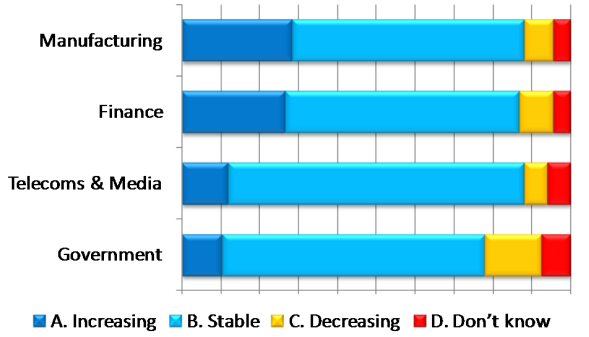


Figure 27: Approximately how much does your organisation spend each year on IT?

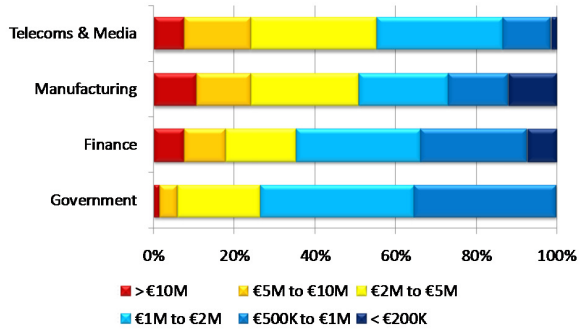
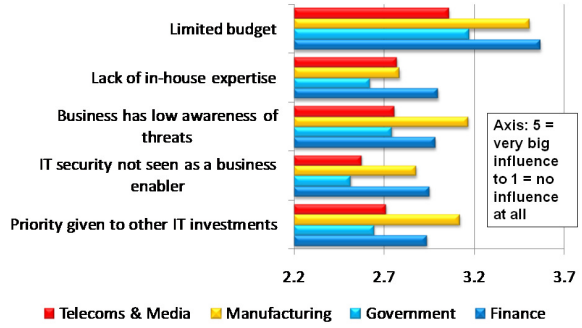


Figure 28: How influential are the following factors in limiting investment in security?



About CA

CA Inc. (NASDAQ: CA) is a global information technology (IT) management software company. We enable organisations to secure and manage IT in all environments—mainframe, distributed, virtualised and cloud—to help control risk and compliance, drive operational excellence, and facilitate business growth and innovation.

CA Security products and solutions help customers secure and control identities, their access and how they use information. They give customers the control to help them confidently move their business forward. By implementing robust, comprehensive and integrated solutions that help optimise all user identities and their access to critical IT resources, organisations can operate in a more adaptable and efficient manner. With more than 3,000 security customers and over 25 years experience in security management, CA offers pragmatic solutions that help reduce security risks, enable greater efficiencies and cost savings, and support delivering quick business value.

CA DLP (Data Loss Prevention) discovers, classifies and sets control policies for information across physical, virtual and cloud environments. The solution empowers organisations to reduce risk, comply with regulations and support business agility. It controls sensitive data at rest or in transit and prevents its inadvertent or malicious movement within or outside organisational boundaries. By rapidly reducing risks, organisations are able to better address compliance and privacy requirements while protecting corporate brand and competitive advantage.

While the proper use of information is essential to the operations of a business, it also needs to be protected from various forms of misuse and loss. CA DLP helps organisations understand where critical information is located throughout their environment, who is using it, and in what context. By combining deep content analysis and control with an identity-centric approach, CA DLP provides more accurate and business-relevant results to help organisations achieve the appropriate mix of business continuity and risk remediation.

Founded in 1976, CA is a global company with headquarters in Islandia, NY and offices in more than 40 countries. CA had fiscal year 2009 revenues of $4.3 billion. For more information, visit www.ca.com.

For additional background information on the report please visit
www.ca.com/gb/mediaresourcecentre.

REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations with regard to compliance and data loss prevention.

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.

Quocirca would like to thank CA for its sponsorship of this report.

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 firsthand 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 advise 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, Microsoft, IBM, O_2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, 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