

Insights: Data Protection and the Cloud

Europe

September 2011

we can



Table of Contents

Executive Summary	Page 3
Further Information	Page 3
Key findings	Page 4
Vertical sector findings	Page 4
Investment in data protection and DR operations, as compared to last year	Page 5
Data and applications in the private and public clouds	Page 6
Use of private and public cloud as part of data protection and disaster recovery strategy over the next year	Page 7
Confidence that data and applications will be protected in the event of a disaster	Page 8
Incidents leading to the loss of data and applications	Page 9
Disaster recovery readiness	Page 10
Challenges with regard to data protection and disaster recovery operations	Page 11
Tips and Advice	Page 12
Methodology	Page 13

Copyright ©2011 CA TECHNOLOGIES. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA TECHNOLOGIES assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA TECHNOLOGIES provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA TECHNOLOGIES be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA TECHNOLOGIES is expressly advised in advance of the possibility of such damages.

Executive Summary

CA Technologies commissioned independent research in May 2011 to investigate the data protection and disaster recovery (DR) policies of organisations in Europe and Asia Pacific. This report highlights the key findings across Europe and provides insights into how these policies can be improved.

CLOUD RESOURCES BECOMING IMPORTANT PART OF DATA PROTECTION STRATEGIES

The use of cloud computing amongst businesses has been increasing rapidly in recent months. At the same time, the amount of data that companies have to manage continues to explode and companies are under renewed pressure to keep it safe. The results from this survey show that investment in business continuity continues to rise, and much of this spending is starting to be directed towards solutions that use cloud computing resources.

Of the companies that are already using cloud, a very high proportion are confident in the safety of their data, whether they are utilising public or private cloud. This highlights the positivity of the current trend towards cloud as a data protection resource.

Organisations are beginning to appreciate that cloud resources offer a solution to some of their data protection requirements. CA Technologies expects this trend to continue but highlights the need for businesses to opt for solutions that allow them to evolve their data protection strategy at their own pace – whether it be a new on-premise technology, using cloud as a backup medium or moving to a more complex hybrid cloud model.

DR INCIDENTS

Incidents leading to data loss are extremely prevalent – 94% of all organisations surveyed had experienced data or application loss over the last year. The causes of the losses were varied, but across every country, IT systems failure (such as hardware or network failure) emerged as the number one trigger. Companies need to be able to predict the likelihood of different types of incidents happening and design an infrastructure that minimizes both their frequency and their impact.

DR PLANNING

The majority of companies admit their data is inadequately protected – only 27% are confident enough to say they have a formal and comprehensive disaster recovery plan. This in part explains the consistently high levels of data loss. Poor data protection strategies are primarily attributed to a lack of both senior management support and budget.

A previous CA Technologies survey, the Avoidable Cost of Downtime*, found that companies are losing in the region of €260,000 a year through IT outages. Senior management need to consider this cost, against the much smaller investment required to keep data and applications adequately protected on an ongoing basis.

CA Technologies and its partners work with companies to help them plan and roll out the policies and IT systems they need for effective data protection – across physical, virtual and cloud environments.

FURTHER INFORMATION

For further information please visit: www.arcserve.com/gb/idp

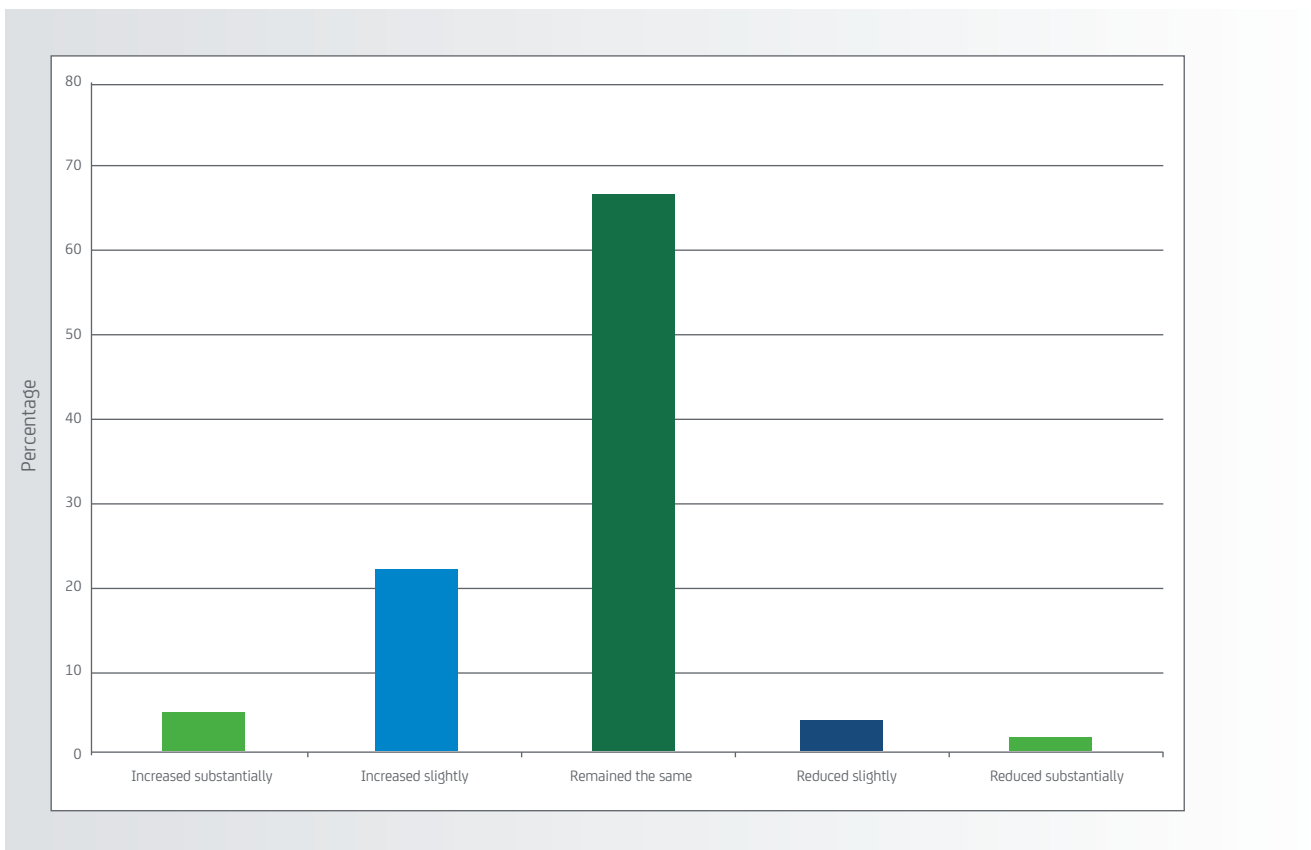
KEY FINDINGS

- Organisations throughout Europe are starting to use cloud computing as a key component of their data protection plans. 34% of organisations expect their use of cloud to increase as part of these plans over the next year.
- Investment in data protection and DR continues to rise. 94% of organisations have at least sustained their investment budgets throughout the period 2010 to 2011 whilst 27% have increased investment.
- Currently 31% of organisations in Europe have data residing in a private cloud, and 17% in a public cloud. 75% of those that use private cloud and 81% that use public cloud are confident that their data would be safe in the event of a disaster.
- 94% of organisations surveyed have experienced application and data loss incidents over the last year. 70% of data loss is a result of IT systems failure e.g. hardware or network failure.
- Just 26% of organisations in Europe have a comprehensive DR plan.
- Inadequate buy-in from senior management (48%) and lack of budget (39%) were cited as the main barriers to improvement of data protection and DR operations.

VERTICAL SECTOR FINDINGS

- Of the vertical sectors surveyed, there is very little difference in the investment in data protection and DR. The manufacturing sector revealed it had invested slightly more than the other sectors (30% compared with an industry average of 27%).
- Organisations in the finance sector are more likely to have data residing in both the private and public cloud than those in the other sectors (36% and 22% respectively). The retail sector has least data in the private (29%) and public (14%) cloud.
- Similarly to the statement above, financial organisations are most likely to expect an increase in cloud usage in the next year (41%). Just 27% of organisations in the retail sector expect an increase.
- There are no significant differences in confidence in private cloud data in the event of a DR incident. The retail sector is most confident in the SLAs provided by public cloud service providers (87%) whereas the finance sector is the least confident (76%). Interestingly, confidence in service providers appeared to be opposite of the degree of cloud usage, implying this has not been a barrier to adoption.
- IT systems failures is the number one cause of data loss for all sectors. There are no significant differences for the frequency of data loss overall.
- The public sector is the most likely to have a full DR plan in place (29%) and the retail sector the least (24%) although differences are small.
- Inadequate support and buy-in from senior management is the main concern with regard to DR operations for all sectors. The manufacturing sector cited this as the biggest barrier (52% compared to 46% of retail organisations).

INVESTMENT IN DATA PROTECTION AND DR OPERATIONS, AS COMPARED TO LAST YEAR

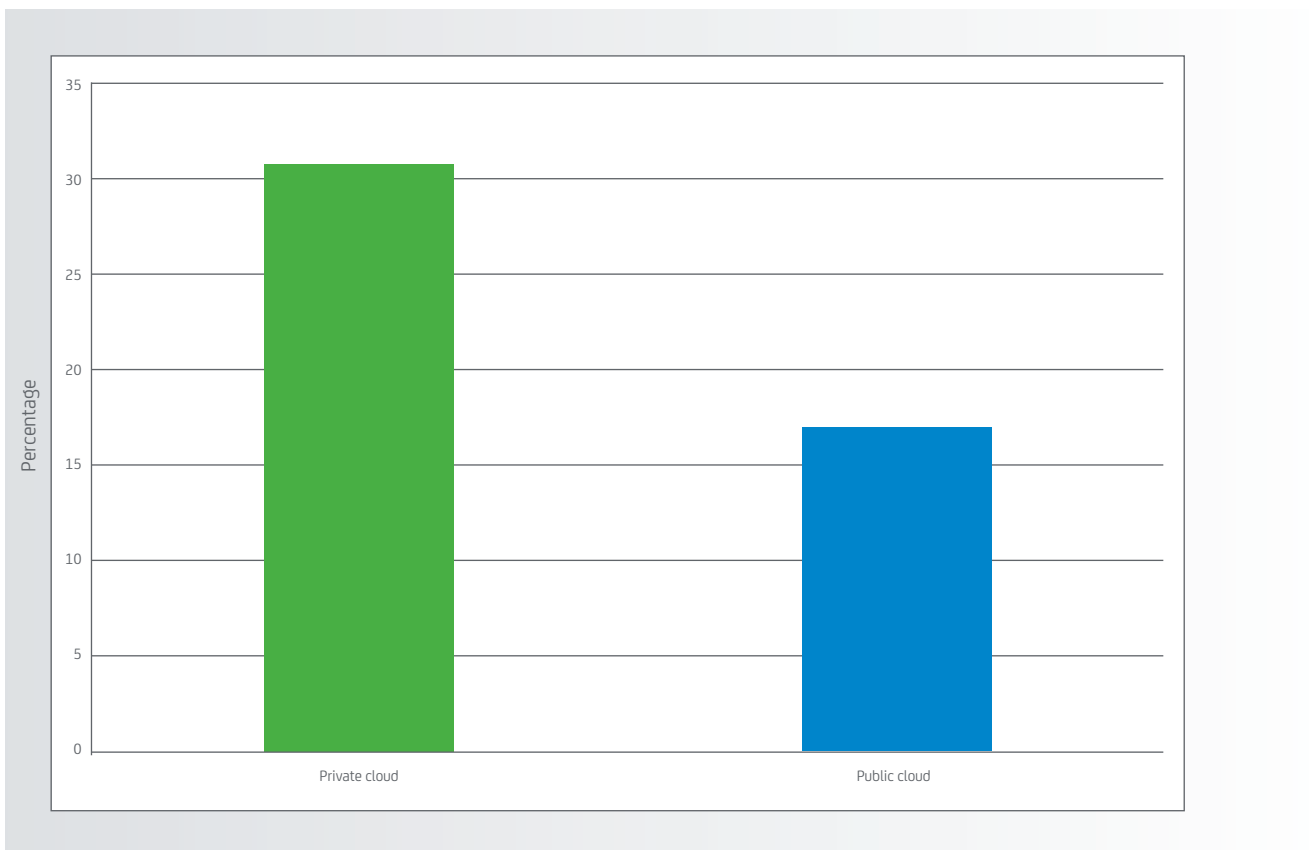


The report highlights a positive trend of investment in data protection and DR throughout Europe. Over two thirds of organisations (67%) surveyed have maintained the same level of investment as last year. In addition, a further 27% have increased investment in data protection and DR options compared to just 6% who have decreased spending. The highest increase in investment comes from companies in Norway (39%) and the lowest is from companies in the Netherlands and Denmark (16% each).

Negligible differences occurred across companies of different size. There is, however, a slight variation between the vertical sectors - 30% of manufacturing organisations have increased spending in data protection and DR compared with 24% in the retail sector.

“Six months ago network failures led to an IT outage affecting the whole workforce. Revenue wasn’t affected but we couldn’t deal with customer queries satisfactorily.”

DATA AND APPLICATIONS IN THE PRIVATE AND PUBLIC CLOUDS

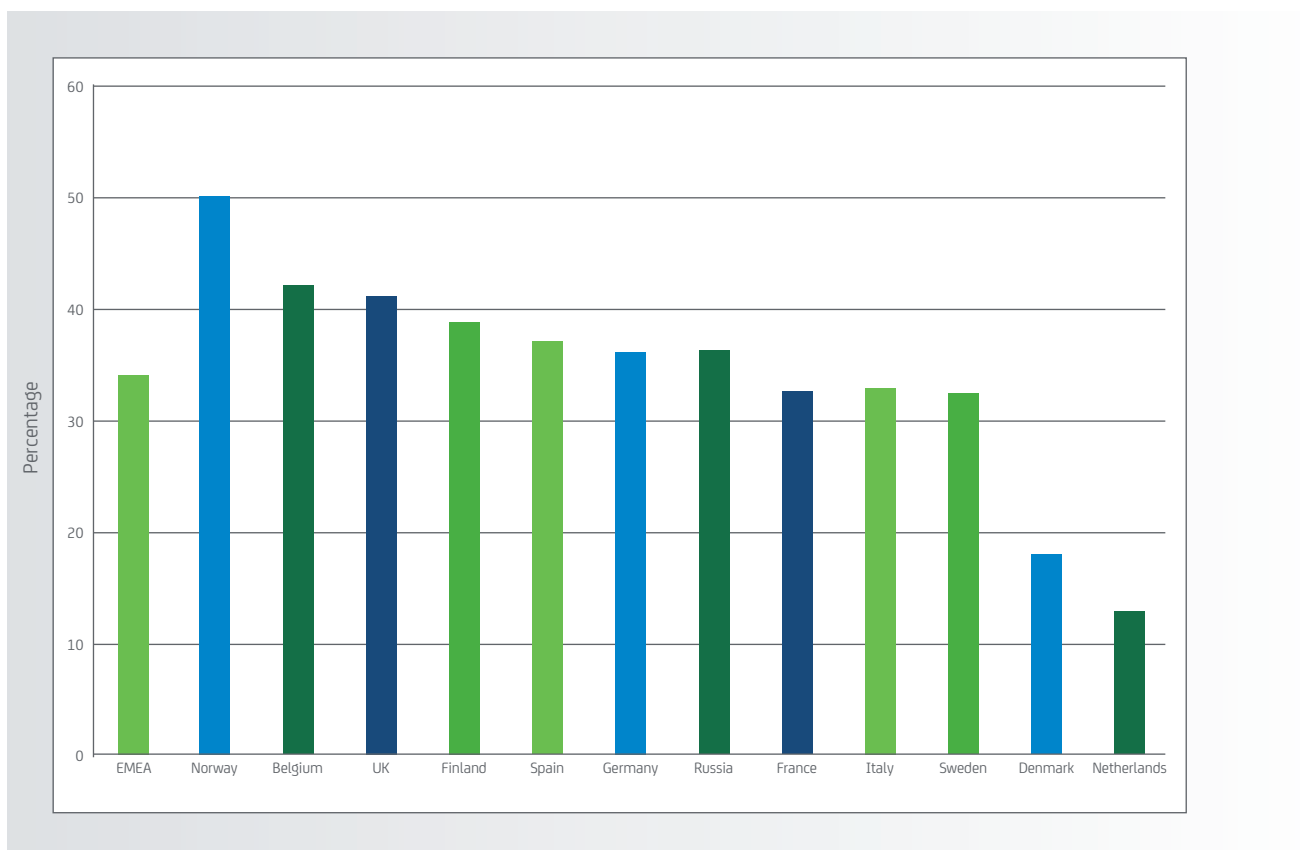


A significant proportion of companies in Europe have data and applications stored in either private (31%) or public (17%) clouds. Use of private clouds is highest in the UK (39%), whilst companies in Belgium and Finland have the highest levels of data and applications in public clouds (24%).

Very little variation was shown between the different sizes of organisations in Europe. Across the vertical sectors, organisations in the finance sector use the cloud the most: 36% for private cloud and 22% for public cloud. The retail sector is making use of these services the least (29% for private and 14% for public).

“Hardware failure resulted in the loss of a large amount of data. The impact on the company was huge as the data was never recovered.”

USE OF PRIVATE AND PUBLIC CLOUD AS PART OF DATA PROTECTION AND DISASTER RECOVERY STRATEGY OVER THE NEXT YEAR

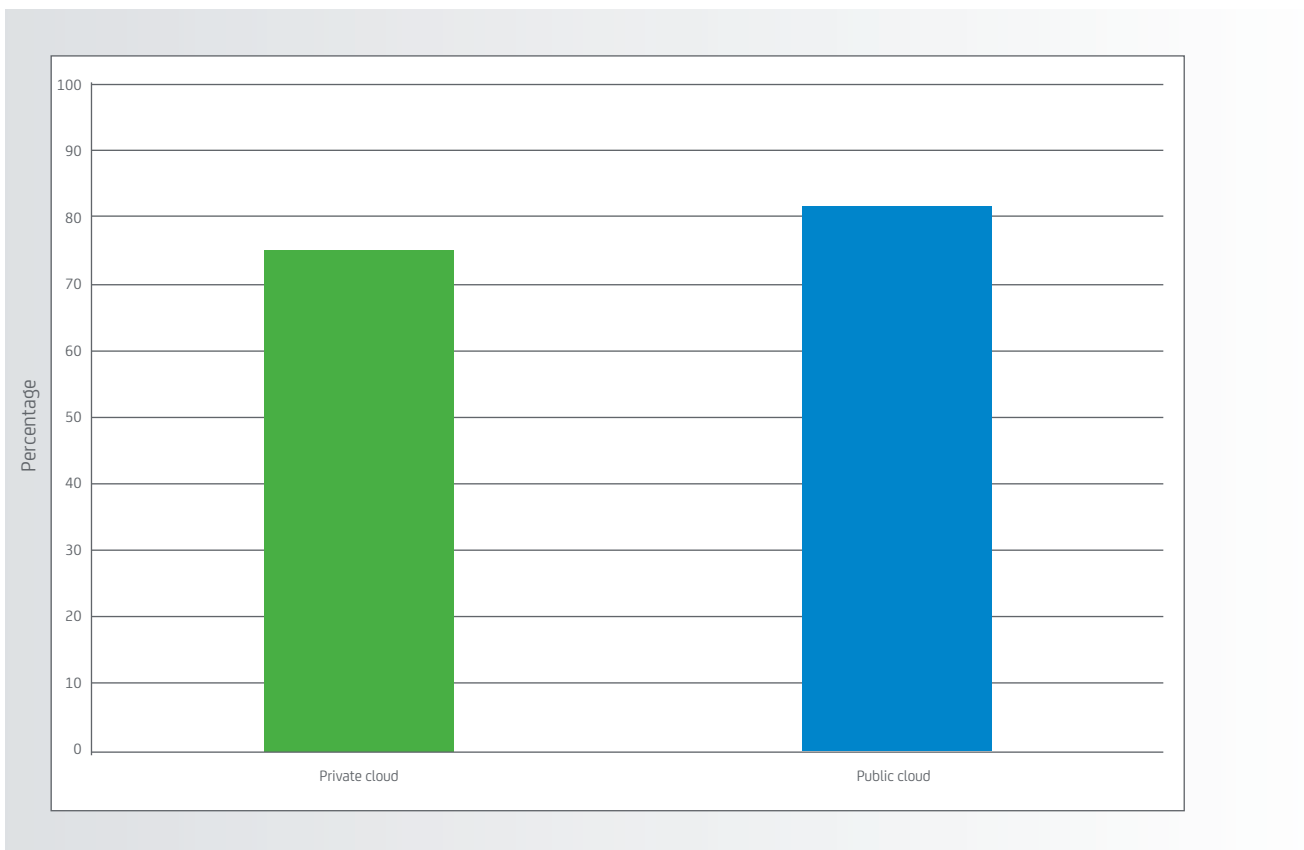


The survey indicates that over one third (34%) of businesses across Europe intend to increase their use of cloud computing as part of their data protection and DR strategy over the next year. Companies in Norway showed the highest levels of expectancy (50%) whereas just 13% of organisations in the Netherlands expect to see a rise in the next year.

Large companies are 5% more likely to use a cloud as part of their business continuity plan over the next year than small businesses (36% compared with 31%). However the difference in these figures is not large enough to suggest that cloud computing as a data protection and data recovery is exclusive to large companies. Organisations of all sizes are realising the important of this move.

Organisations in the financial sector (41%) are the most likely to implement this strategy over the next 12 months. Companies in the retail sector showed the lowest level of expectation at 27%. This result is in line with the current levels of cloud use for these vertical sectors.

CONFIDENCE THAT DATA AND APPLICATIONS WILL BE PROTECTED IN THE EVENT OF A DISASTER

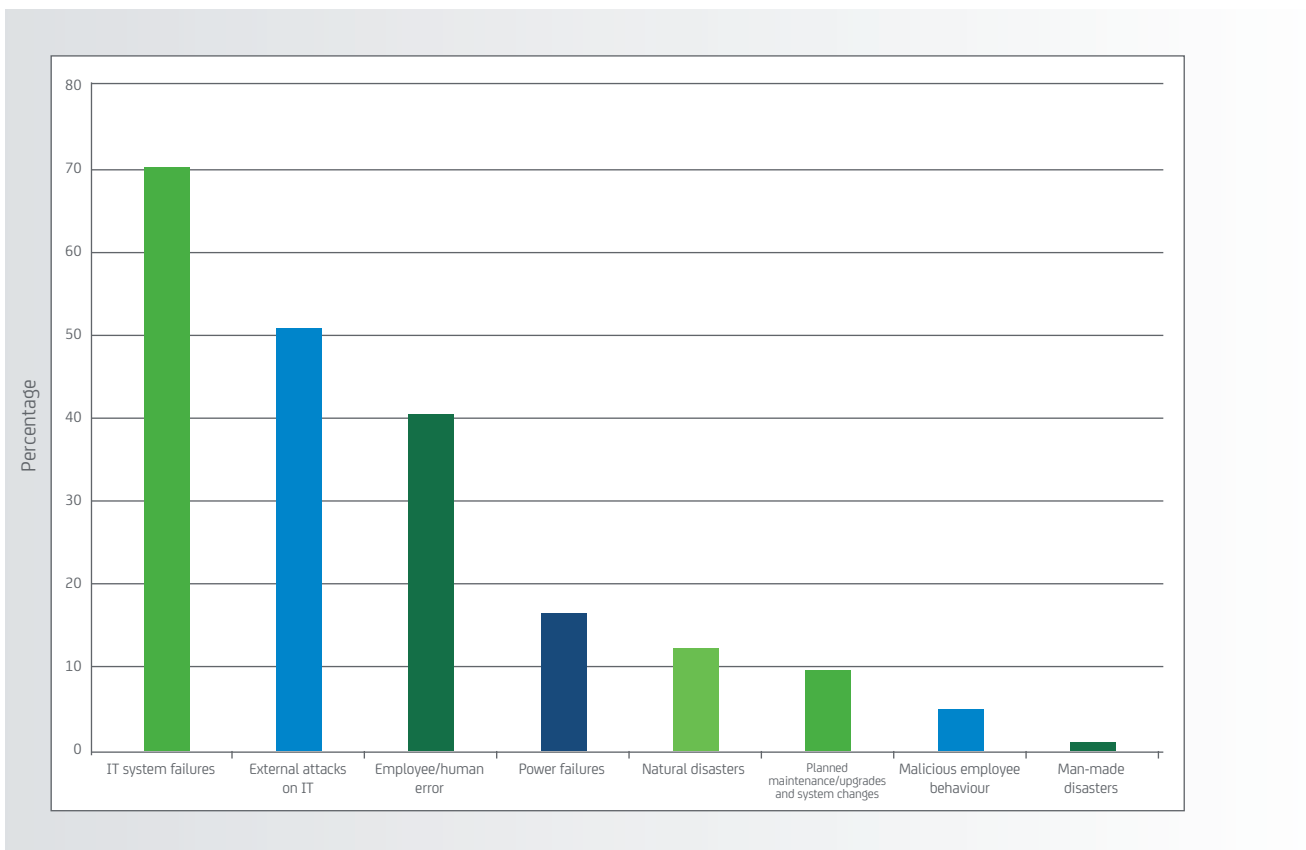


Encouragingly, the survey indicated high levels of confidence in the safety of data in the cloud. Three quarters (75%) of organisations in Europe claim that they are confident that their private cloud data and applications would be protected in the event of a disaster. The highest level of confidence was displayed by the Netherlands (87%) and the lowest by Finland (68%) and the UK (68%). There is little difference in the results between the sizes of the companies. The public sector is the most confident amongst the vertical sectors (77%) whilst the manufacturing industry is the lowest at 73%.

Similarly, companies across Europe with data and applications in a public cloud are happy with the security SLAs from suppliers, with a very positive response of 81%. Companies in the financial sector are the least satisfied by the SLAs from their suppliers at 76%, this is 11% lower than organisations in the retail sector who are the most content (87%). There is very little difference between small, medium and large companies.

“Earlier this year heavy snowfall brought down power lines nearby. The whole site went down and the company was affected for three whole days. Over 75 users were affected and the company lost a significant amount of revenue as a result.”

INCIDENTS LEADING TO THE LOSS OF DATA AND APPLICATIONS



94% of companies across Europe have experienced data and application loss resulting from a DR incident in the last year. All companies surveyed (100%) in the Netherlands lost data in the last 12 months. The lowest incidence of data loss occurred in the UK (88%) and France (88%).

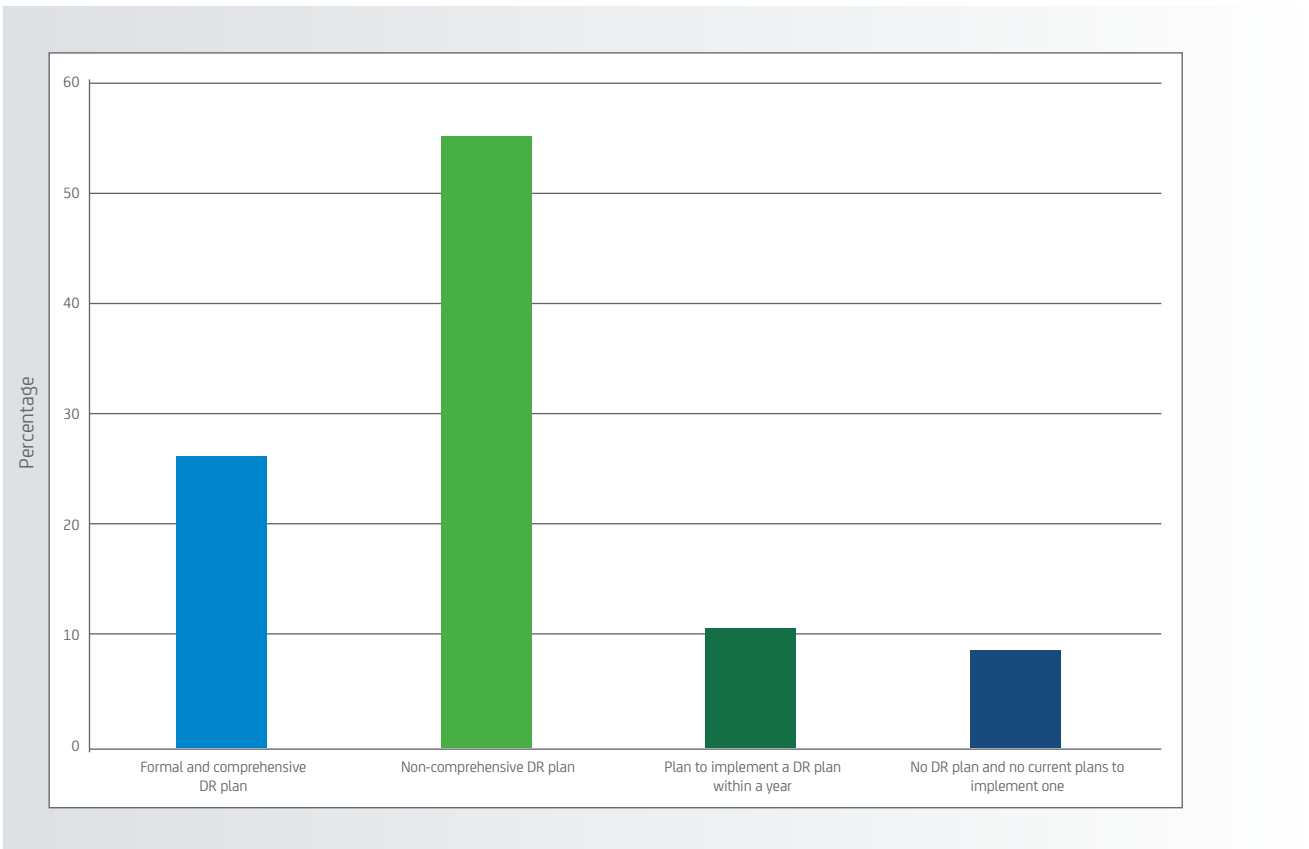
The largest contributing factor to instances of data loss is IT systems failure (such as network, storage, hardware or software failures). This accounted for 70% of data and application loss incidents across Europe over the last 12 months. IT systems failure was the number one cause of loss in all of the countries considered in the survey. In Sweden a high 84% had been affected by this type of incident.

External attacks on IT account for the second highest cause of incident, an average of 50% of companies across Europe have experienced this type problem. Human error accounts for more than a third (41%) of data loss incidents.

Company size appears to have very little bearing on the most likely cause of data loss incidents. This trend is also reflected across the vertical sectors, where on average the type of contributing factor affected the different sectors fairly equally.

Companies need to be able to predict the likelihood of different types of incidents happening and design an infrastructure that minimizes both their frequency and their impact.

DISASTER RECOVERY READINESS



Of the organisations surveyed across Europe just 26% have a formal and comprehensive disaster recovery plan in place. An additional 55% of companies indicated that they have a DR plan in place but that it is not comprehensive.

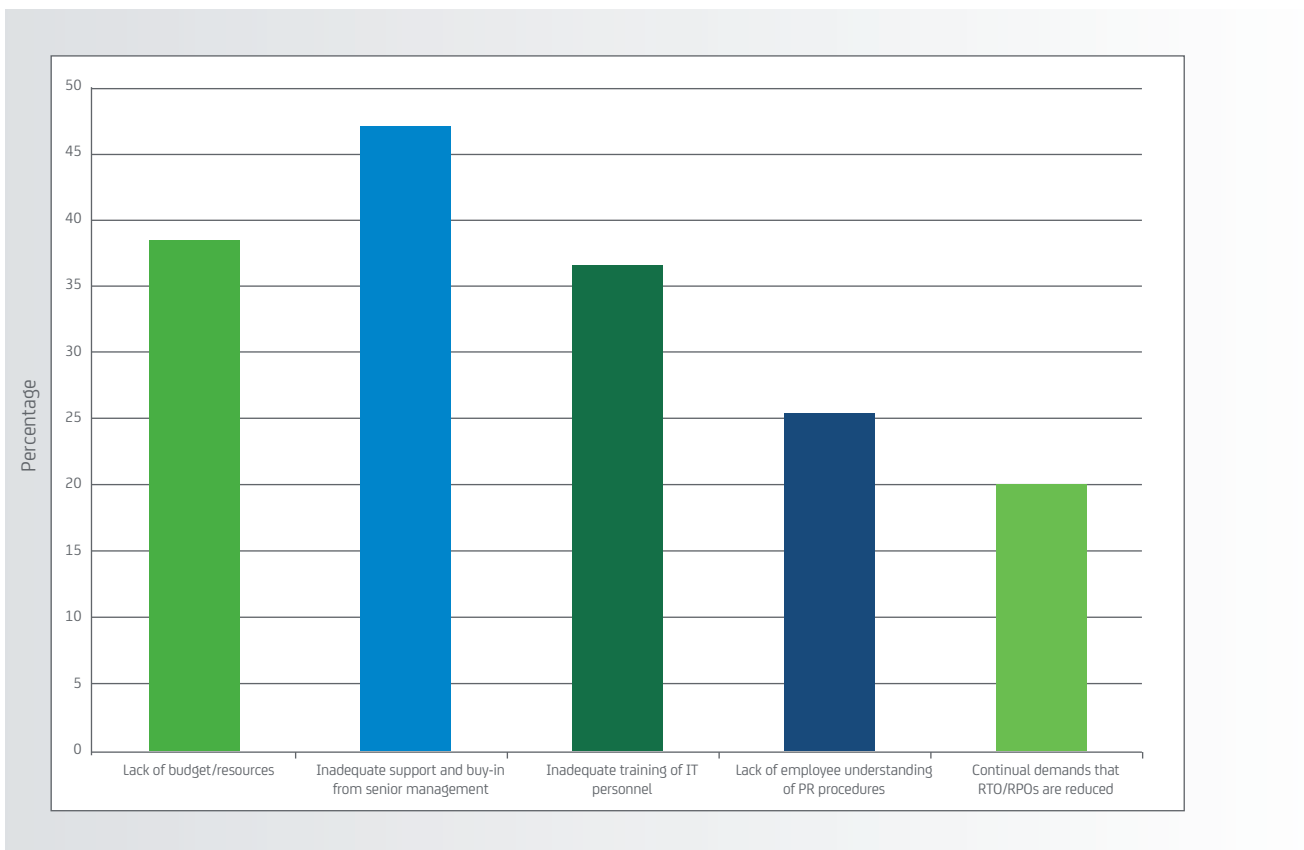
Organisations in France are the most prepared for a disaster, with 41% stating that they have a formal and comprehensive DR plan, followed by Germany with 35%. The least well-prepared businesses are in the Netherlands (13%) and Finland (18%).

There was little variation between the different sizes of the companies. In terms of the vertical sectors, the public sector is the most prepared, as 29% have a formal and comprehensive DR plan. The least well-prepared sector is manufacturing as 19% of companies in this sector currently do not have a DR plan in place.

There is a distinct correlation between the lack of DR readiness and the high instances of data and/ or application loss through Europe.

“An employee plugged in a wrong cable resulting in a short circuit and power failure. This led to downtime lasting two days. We couldn’t work properly for all that time and it cost us a lot of money.”

CHALLENGES WITH REGARD TO DATA PROTECTION AND DISASTER RECOVERY OPERATIONS



The main challenge faced by companies across Europe in regard to data protection and DR comes from inadequate support and buy-in from senior management. Almost half of companies (48%) see this as a contributing factor. This trend was consistent across most companies throughout Europe, although lack of budget is the most important factor for France and Spain, and inadequate training was cited for the UK and Belgium.

Lack of budget and resources is the second highest contributing factor across Europe, with 39% of businesses citing this as a challenge. This is followed closely by inadequate training of IT personnel in risk planning and disaster recovery planning (37%).

A previous CA Technologies study (the Avoidable Cost of Downtime*) has shown the cost of outages to a company over a year in the region is of \$350,000. Senior management need to consider this cost, against the much smaller investment required to keep data and applications adequately protected on an ongoing basis.

There is not a significant amount of variation between the company sizes and vertical sectors. All sizes and sectors of company cited inadequate management support as the biggest challenge to operations. The manufacturing sector consider this the biggest challenge (52%).

Tips and Advice

CLOUD FOR DATA PROTECTION

- For businesses that do not have a remote site for data protection purposes, cloud computing is a great way to bolster business continuity and disaster recovery operations. For those that do have a remote site, using cloud for data protection can help organisations convert CAPEX to OPEX, and enable better budget management as companies typically pay only for what they use.
- Many companies today are already using cloud for offsite back-up, archiving and disaster recovery purposes. However, the cloud can also be used for real-time replication and high availability solutions, helping to minimise IT outages and data loss.
- Companies preparing to use the cloud for disaster recovery initiatives need to ensure they understand how their products, processes and providers will deal with various issues. For example, what impact will the cloud have on application performance? Or, what SLAs do providers offer? CA Technologies and or partners can help you navigate through this, ensuring you get the best solution.

PREVENTING DATA LOSS

- Although companies today understand there are threats and consequences associated with a lack of disaster recovery planning, they still frequently experience IT outages and data loss. IT managers point to lack of budget and lack of senior management buy-in as the reasons behind this. There are two ways of tackling this – the first is to do ‘more with less’ and the second is to secure additional funding from the senior management team.
- There are many ‘best practices’ that can help organisations achieve more with less - here we talk very briefly about just three.
 - o In today’s world of mushrooming data volumes, management of the data is becoming increasingly management-intensive. In order to free up valuable man hours, companies need to choose solutions which feature advanced levels of central management and automation.
 - o Data deduplication is another proven method of reducing the cost of storage through improved storage utilisation.
 - o When selecting data protection solutions, companies should be wary of opting for the cheapest products as they often have hidden costs. For example, many don’t include a centralised management function, or may even require companies to simply use lots of storage. Over the medium- to long-term, the drain on personnel to compensate for the product’s shortcomings, and the cost of buying the add-ons, can quickly become expensive.
- It’s a common complaint of the IT department that, through lack of investment in business continuity initiatives, senior management run the risk of incurring the costs of a potential data breach as opposed to implementing what they view as costly data protection solutions. So how can IT set about convincing the CTO that this is a false economy and that investing strategically in data protection can be the better long-term option? The best way is to show them the potential cost of not doing anything. For example, a previous CA Technologies study* has shown the cost of outages to a company over a year in the region is of \$350,000. Tangible figures can really help persuade senior management about the cost of not investing.

Methodology

- The survey was conducted by an independent research firm, Coleman Parkes. All interviews were undertaken during May 2011. The survey was based on a total of 1,987 online interviews amongst CIOs/IT Directors/IT Managers across Europe and an even split of small (50-499 employees), medium (500-999 employees) and large (1000+ employees) companies. 1,086 interviews were also carried out in Asia Pacific.
- The frequency of interviews across Europe was: Belgium 191, Denmark 100, Finland 101, France 200, Germany 200, Italy 202, Netherlands 189, Norway 100, Russia 202, Spain 200, Sweden 102, UK 200. Total sample: 1,987. Fieldwork was controlled to ensure even coverage across the following vertical sectors within each country: Finance 25%, Retail 25%, Public Sector 25%, Manufacturing 25%. All interviews were conducted in strict accordance with the rules and guidelines laid down by ESOMAR and the Market Research Society.
- Follow-up telephone interviews were conducted with a pre-selected sample of respondents, to gather additional information about incidents that had occurred.

* <http://www.arcserve.com/gb/lpg/cost-of-downtime.aspx>

Further Information

For further information please visit: www.arcserve.com/gb/idp

Social Media Links – have your say too



[Twitter/arcserve_europe](https://twitter.com/arcserve_europe)



[Linkedin/arcserve](https://www.linkedin.com/company/arcserve)



[Facebook/arcserve](https://www.facebook.com/arcserve)



[Youtube/arcserve](https://www.youtube.com/arcserve)

About CA www.ca.com

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and physical to virtual and cloud. CA Technologies manages and secures IT environments, enabling our customers to deliver more flexible IT services.

Our solutions help our customers gain a level of deep insight into and exceptional control over complex, mixed IT environments. It's that level of insight and control that enables IT organizations to power business agility.

About Coleman Parkes www.colemanparkes.com

Coleman Parkes Research was set up over 8 years ago to deliver premium quality, action focused research, specialising in the business-to-business space. The Company undertakes research for service and product suppliers to all parts of the business community including Finance, Retail, Government, Services and Manufacturing. The last of these is a specialist area and with both Directors of the Company having devoted most of their working lives to this sector, the Company is able to offer informed, incisive manufacturing based research that is without peer.