DATABARRACKS

DATA HEALTH CHECK

2015 REPORT

Databarracks

CONTENTS

EXECUTIVE SUMMARY

By Oscar Arean, Technical Operations Manager

Welcome to the 2015 Databarracks Data Health Check. This year we surveyed 404 IT decision makers, from specialists and consultants to board-level executives, on their experiences with technology in the last 12 months, and their expectations for the year ahead.

Our questions focus on the use of backup and recovery, data security, cloud computing and storage to gauge trends in attitudes and practices among UK IT professionals.

This year's respondents skew ever so slightly towards either end of the scale in terms of size, though there's still a good spread between small, medium and large organisations.

As in previous years, it has also been useful to split respondents by other factors, such as available internal IT resources, to see how usage of and sentiment towards technology varies according to different circumstances.

36%
SMALL BUSINESSES
(0-49 EMPLOYEES)

26%
MEDIUM BUSINESSES
(50-499 EMPLOYEES)

37%
LARGE BUSINESSES
(500+ EMPLOYEES)

RESPONDENTS SPLIT BY INDUSTRY

PUBLIC SERVICES: Charity, education, health, transport, utilities
18%

FINANCE: Banking and finance
8%

TECHNOLOGY: Technology, telecoms, media
27%

PROFESSIONAL SERVICES: Legal, professional services
16%

COMMERCIAL: Consumer goods, leisure, retail
10%

INDUSTRIAL: Construction, engineering, industrial, natural resources
14%

OTHER
7%

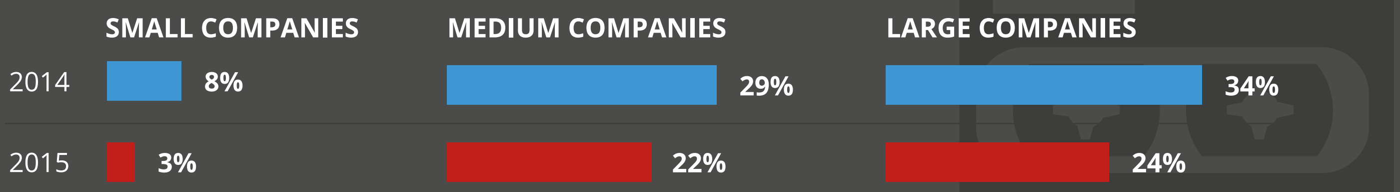
BACKUP

We'll get the obligatory statement on tape out of the way first: this year saw further decline – down from 4% to 3% this year.

It's also interesting to note that use of "Disk and Tape" – the combination often representative of a transitional period for many organisations – is also in decline.

3%
OF RESPONDENTS USE TAPE AS THEIR ONLY BACKUP METHOD - DOWN FROM 4% IN 2014

USERS OF "DISK AND TAPE"



The causes of data loss are always interesting to examine across different groups. With 2014's notable exception, human error has consistently ranked as the leading cause for years. It's back on top this year, with hardware failure following close behind.

For two years in a row now, hardware failure has caused more data loss for large organisations than human failure. If I had to guess why, I'd attribute this to two things. First, the fact that larger organisations tend to have mitigating checks and balances in place to reduce the amount of damage an individual user account can cause. Second, larger organisations often don't refresh their hardware as frequently due to the size and complexity of their infrastructure. Where IT assets are forced to sweat for longer, it's inevitable that some will just give out.

LEADING CAUSE OF DATA LOSS

16%
SMALL – HUMAN ERROR

31%
MEDIUM – HUMAN ERROR

31%
LARGE – HARDWARE FAILURE

Equally, smaller organisations both spent less time per day on backup and experienced less data loss on the whole.

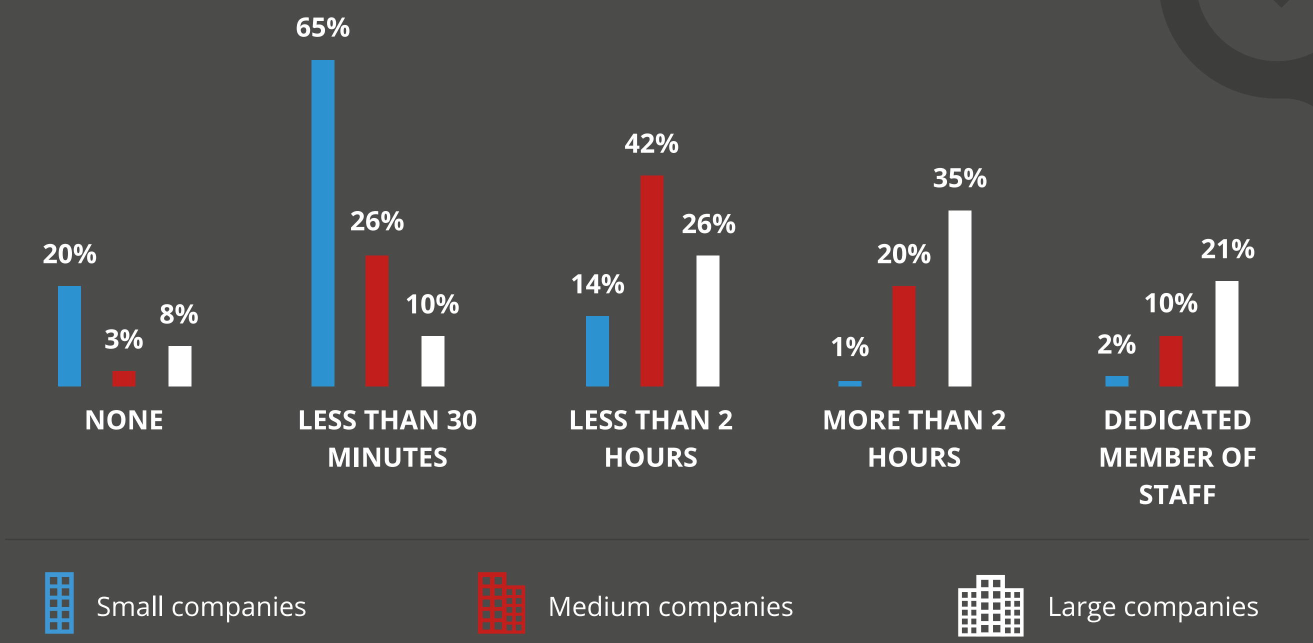
“NONE” AND “OTHER” RESPONSES TO CAUSES OF DATA LOSS

71%
SMALL – “NONE” AND “OTHER”

37%
MEDIUM – “NONE” AND “OTHER”

51%
LARGE – “NONE” AND “OTHER”

MOST COMMON ANSWER FOR TIME SPENT PER DAY ON BACKUP



DISASTER RECOVERY

Just over half of the respondents this year reported owning a business continuity plan, which is a modest increase on last year. Split the data by size however, and the results tell a different, if familiar, story.

RESPONDENTS WITH A BUSINESS CONTINUITY PLAN

SMALL	MEDIUM	LARGE
27%	68%	75%

In 2014, 42% of respondents from small organisations said they did not have a business continuity plan and they did not intend to create one in the next 12 months. A year later and it looks as though that sentiment was accurate.

Of those organisations that did own a BCP plan, there was a reassuring presence of dedicated IT disaster recovery plans included within them.

RESPONDENTS WITH A DEDICATED IT DISASTER RECOVERY PLAN

SMALL	MEDIUM	LARGE
85%	86%	90%

73% of small organisations had not tested their DR plan in the last 12 months, of which 40% said they didn't intend to in future.

However, the rate of DR testing was less consistent. Small organisations in particular would do well to take testing more seriously. As we've said before, a plan untested is just an idea.

A NOTE ON TESTING

When I talk to customers about DR testing, they often cite a lack of time as a major blocker. Last year, it was the most common reason given by small organisations when asked why they hadn't tested in 12 months.

More worryingly, the second most common answer was "I don't know". It's my opinion that organisations that genuinely don't have the time and resources to perform testing must exhaustively justify that decision; it's an essential piece of due diligence. Simply put, "I don't know" isn't good enough.

In truth, it's rarely the case that time is such an inflexible commodity. Using a lack of it as an excuse for not testing may represent more of a cultural aversion rather than a genuine lack of tangible resources.

25%

OF RESPONDENTS USE FROM SMALL COMPANIES IN 2014 WERE NOT SURE WHY THEY HADN'T TESTED THEIR DR PROCESSES

WHAT DIFFERENCE DOES TESTING MAKE?

Respondents that tested their DR plans in the last 12 months tended to have a firmer grasp of their overall DR capabilities and ambitions as a whole.

TESTERS

Of the 169 respondents who have had tested their DR plan in the last 12 months:

- 58% felt "very confident" about their plan
- 40% felt "fairly confident"
- 3% "had concerns"

There was also an even split in the frequency of restores with:

- 24% Daily
- 23% Weekly
- 25% Monthly

42% said these restores never failed.

25% could recover within 4 hours, and 54% could recover with 8 hours.

The largest ideal RTO was less than 1 hour (29%) closely followed by less than 4 hours (22%).

NON-TESTERS

Of the 186 respondents who had not tested in the last 12 months, 30% restored less than once a year, and 23% restored monthly. 53% said their restores never failed, but this may be the result of fewer restores overall.

- 28% felt "very confident" about their plan
- 55% felt "fairly confident"
- 16% "had concerns"

Organisations that test their DR plans restore more often, more successfully and with more confidence than those that don't test at least annually.

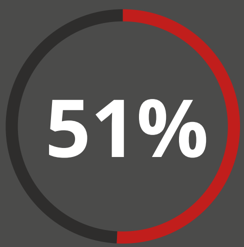
The largest group didn't know how long it would take them to recover from a disaster (23%), closely followed by "less than 4 hours" (18%).

The most common ideal RTO was less than 1 hour (25%) closely followed by less than 4 hours (22%). However, 18% also said "I don't know".

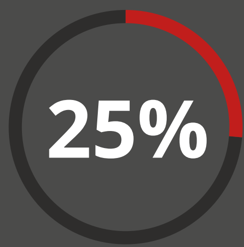
CYBER SECURITY

Unsurprisingly, respondents who were affected by cyber-attacks had (for the most part) reviewed their security policies in response. I'm not particularly concerned about the 25% of respondents who reviewed their security policies and made no changes – human error is often better addressed through education rather than Draconian usage policies.

OF RESPONDENTS WHO HAD EXPERIENCED A CYBER-ATTACK:



had reviewed their security policies and made changes



had reviewed their security policies and made no changes

I'm particularly encouraged by the 47% of respondents that had reviewed their security policies in the last 12 months despite not experiencing a cyber-attack. This is very good general hygiene, and it's heartening to see so many organisations getting security right. I'd encourage the rest to regard the threat of constantly evolving cyber-attacks (rather than the experience of one) as justification enough to review security policies regularly.

Backup and disaster recovery can be an excellent tool in mitigating the damage of cyber-attacks. We've helped many customers avoid downtime and the damaging effects of malware by safely restoring their unaffected backups. In the case of attacks such as CryptoLocker, this not only avoided downtime, but also negated both the ransom costs and the irretrievable loss of data itself.

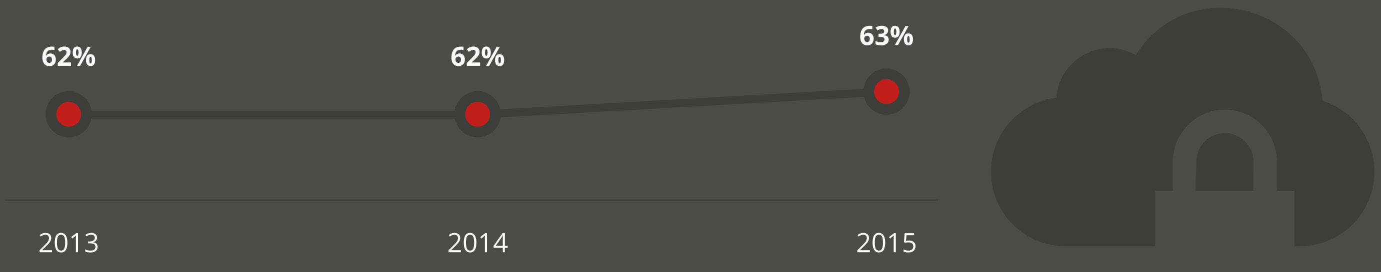
47%
OF ORGANISATIONS WHO HAD NOT EXPERIENCED A CYBER-ATTACK IN THE LAST 12 MONTHS STILL REVIEWED THEIR SECURITY POLICIES

55%
OF RESPONDENTS STATED THEIR DR SOLUTION PROTECTED THEM FROM CYBER-ATTACKS

CLOUD COMPUTING

Attitudes to cloud computing evolve slowly and over time. As such, it's not difficult to account for the appearance of "security" as the top priority when selecting a cloud service provider for the fourth year in a row.

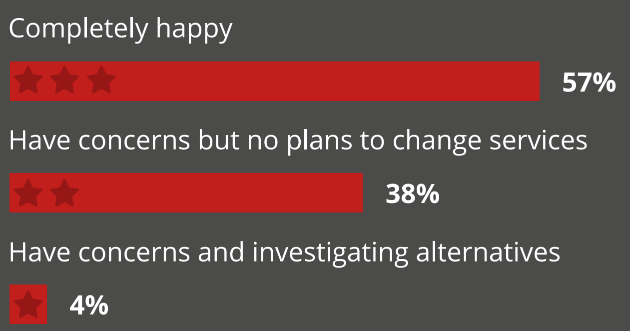
PERCENTAGE OF RESPONDENTS THAT SELECTED "SECURITY" AS THE MOST IMPORTANT WHEN SELECTING A CLOUD SERVICE PROVIDER



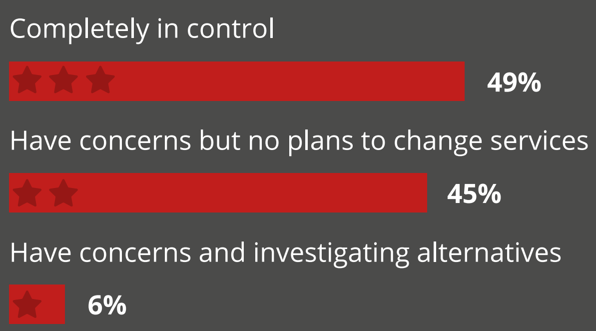
Last year we found that experience positively impacts attitude towards cloud services. The same was true this year: respondents who actively use cloud services not only tend to view them more favourably, they use different metrics to determine their value.

Given this trend, we've adapted our line of questioning to delve into the reasoning behind the preoccupation with security.

HOW MUCH CONFIDENCE DO YOU HAVE IN THE CLOUD SERVICES YOU USE TO KEEP YOUR DATA SECURE AND AVAILABLE?



DO YOU FEEL A LOSS OF CONTROL OVER YOUR DATA WHEN USING CLOUD SERVICES?



How are we to reconcile the continued prevalence of security anxieties with the news that the majority of respondents who use cloud services are “completely happy” that their data will remain secure and available? Are we to accept security concerns as a permanent fixture in the minds of cloud users? Is this attitude simply the cost of doing business?

Well, just over half of respondents also admitted to feeling a loss of control when using cloud services. Speaking optimistically, I think this is a good representation of market attitudes as they stand. Users of cloud services are generally pleased with the services they consume, but remain reflexively cautious when their data leaves the corporate firewall.

It’s up to cloud providers to continue building confidence in the security and availability of data held in the public cloud, as well working to help customers understand the controls around access to their data.

DATA STORAGE AND ANALYTICS

Throughout our annual Data Health Check reports, file data and emails have consistently ranked as the leading causes of storage growth, and this year is no different.

FASTEST AREA OF STORAGE GROWTH

SMALL COMPANIES

Email **28%**

MEDIUM COMPANIES

File Data **27%**

LARGE COMPANIES

Email **19%**

I had imagined that organisations with larger IT departments would have a stronger grasp of ongoing operational factors, such as storage growth. However, this wasn't the case. When asked where their fastest area of storage growth was, the top answer among respondents with small and mid-sized IT departments was either email or file data. The top answer among respondents with large IT departments was "I don't know".

FASTEST AREA OF STORAGE GROWTH SPLIT BY SIZE OF IT DEPARTMENT

27%
1-10 IT STAFF
EMAIL

22%
11-30 IT STAFF
FILE DATA

27%
30+ IT STAFF
I DON'T KNOW

Rates of adoption for file analysis tools are still relatively low across the board, which is possibly why so few respondents actively distinguish between recently accessed and unused files. Organisations with larger IT departments tended to make the distinction more often, though again, mid-sized teams out-performed larger ones.

IT DEPARTMENTS THAT ACTIVELY DISTINGUISH BETWEEN FILES THAT HAVE BEEN RECENTLY ACCESSED AND FILES THAT HAVE NOT BEEN ACCESSED IN OVER A YEAR?

17%
1-10 IT STAFF

47%
11-30 IT STAFF

39%
30+ IT STAFF

The data analytics market is simultaneously maturing and diversifying. Where previously data analytics services relied on expensive consultancy and impenetrably complex tools to be effective, the last few years have seen a shift towards usability. There are several low-cost tools available today that are built to engage a much broader range of users – IT staff and non-technical alike – in data lifecycle management.

USE OF FILE ANALYSIS TOOLS SPLIT BY SIZE OF IT DEPARTMENT (TOP ANSWER)

FIND OUT MORE

Take a look at the Data Health Check interactive infographic, or to read previous reports visit datahealthcheck.databarracks.com.

APPENDIX

1. What best describes your business sector?

Banking & Finance	8%
Charity/NGO	2%
Construction & Property	5%
Consumer Goods	2%
Education	8%
Engineering	5%
Health	5%
Industrial	4%
Legal	2%
Leisure	2%
Media	2%
Natural Resources	1%
Professional Services	14%
Retail	6%
Technology	23%
Telecommunications	3%
Transport	3%
Utilities	1%
Other (please specify)	7%

2. What is your position within the business?

Corporate / Board-level responsible for IT	22%
Director-level responsible for IT/IS	19%
IT Manager	25%
IT Technical Specialist	28%
IT Admin	0%
IT Consultant	7%
General Management - Non-IT (inc. Product/Project Managers, Sales and Marketing)	0%
Other - Non-IT (please specify)	0%

3. How many employees does your company have?

< 15	31%
25-49	5%
50-99	5%
100-249	9%
250-499	13%
500-999	9%
1000-4999	11%
5000+	18%

4. How many employees in your IT department?

< 5	39%
5-10	12%
11-15	11%
16-30	13%
31-100	12%
100+	14%

5. Where is your UK head office located?

North East	4%
North West	12%
Yorkshire and The Humber	5%
East Midlands	5%
West Midlands	8%
East of England	4%
London	23%
South East	20%
South West	9%
Scotland	6%
Wales	2%
Northern Ireland	1%
We do not have a UK head office	0%

6. What is your annual turnover?

< £5m	39%
£5 - 9.9m	5%
£10 - 24.9m	7%
£25 – 49.9m	6%
£50 – 99.9m	10%
£100 – 249.9m	8%
£250 – 499.9m	7%
£500 – 999.9m	4%
> £1000m	15%

7. What is your current backup method?

None	5%
Tape only	3%
Disk and tape	16%
Disk only	16%
Online backup (internally between sites)	18%
Cloud backup (to a third party backup company)	30%
Backup appliance	8%
Other (please specify)	4%

8. What were the causes of any data loss over the last 12 months? (tick all that apply)

Hardware failure	21%
Software failure	16%
Data corruption	19%
Human error/accident	24%
Internal security breach (member of staff)	6%
Cyber-attack (hacker/virus)	8%
Natural disaster	2%
None	54%
Other (please specify)	1%

9. On average, how much time does your organisation spend on backup each day?

Less than 30 minutes	34%
Less than 2 hours	26%
More than 2 hours	19%
Dedicated member of staff	11%
None	11%

10. Do you have a Business Continuity Plan?

Yes	56%
No but we will within the next 12 months	16%
No and we don't intend to implement one within the next 12 months	18%
I don't know	11%

11. Who is involved in the writing of your business continuity plan? (tick all that apply)

IT Manager	47%
IT Director	35%
CIO	17%
CFO	8%
CEO	20%
Finance Director	16%
Individual department heads (HR Manager, Marketing Manager, etc.)	22%
Business Continuity Manager	24%
Operations Manager	21%
Board	12%
I don't know	8%
Other (please specify)	0%

12. In your organisation, who is ultimately in charge of the business continuity plan?

IT Manager	22%
IT Director	27%
Business Continuity Manager	12%
Operations Manager	5%
Financial Director/CFO	4%
MD/CEO	17%
I don't know	11%
Other (please specify)	2%

13. Within your Business Continuity Plan, do you have a specific IT Disaster Recovery plan?

Yes	88%
No, but we're planning to write one in the next 12 months	7%
No, and we have no intention of writing one	1%
I don't know	4%

14. Have you tested any elements of your disaster recovery process in the last 12 months?

Yes	42%
No, but we're planning to within the next 12 months	23%
No, and we're not planning to	24%
I don't know	12%

15. What is most important to you in a disaster recovery situation?

Business intelligence systems	7%
Call centre management	4%
CRM/customer service	8%
Data warehouse management	6%
Desktops	5%
Email	9%
Employee intranet	1%
ERP	2%
File Data	13%
Financial systems (such as SAP, Oracle Financials)	8%
Human resources systems	0%
Inventory management	1%
Online trading systems	2%
Point of sale	2%
Supply chain management	1%
Telephone system	2%
Test and development environment	1%
Website	3%
All equally important	25%
Other (please specify)	4

16. On average, how often do you perform restores of data?

Every day	15%
Weekly	19%
Monthly	22%
Yearly	8%
Less than once per year	18%
I don't know	18%

17. On average, what percentage of these restores failed within the last 12 months?

None	47%
Less than 10%	31%
More than 10% but less than half	13%
More than half	3%
I don't know	6%

18. How confident are you in your current disaster recovery plan?

Very confident	41%
Fairly confident	49%
I have concerns	10%
Not confident at all	1%

19. How long would it currently take for you to recover from a disaster?

Less than 5 minutes	3%
Less than 1 hour	12%
Less than 4 hours	19%
Less than 8 hours	11%
Less than 12 hours	8%
Less than 24 hours	12%
Less than 48 hours	7%
More than 48 hours	4%
I don't know	24%

20. What would be your ideal RTO (Recovery Time Objective)?

Less than 5 minutes	9%
Less than 1 hour	25%
Less than 4 hours	20%
Less than 8 hours	10%
Less than 12 hours	7%
Less than 24 hours	7%
Less than 48 hours	3%
More than 48 hours	0%
I don't know	19%

21. How long do you think your organisation could survive without its crucial IT systems (i.e. what is your maximum tolerable outage)?

Less than 30 minutes	4%
Less than 1 hour	5%
Less than 4 hours	11%
Less than 8 hours	10%
Less than 12 hours	8%
Less than 1 day	12%
Less than 2 days	12%
Less than 3 days	6%
Less than 1 week	9%
Less than 2 weeks	3%
Less than 1 month	4%
I don't know	18%

22. If you were to ask your senior management team how long they thought your organisation could cope without its crucial IT (your maximum tolerable outage) - what would they say?

Less than 30 minutes	7%
Less than 1 hour	9%
Less than 4 hours	12%
Less than 8 hours	7%
Less than 12 hours	6%
Less than 1 day	10%
Less than 2 days	8%
Less than 3 days	5%
Less than 1 week	7%
Less than 2 weeks	3%
Less than 1 month	3%
I don't know	23%

23. What is your biggest worry in a disaster?

Reputational damage	16%
Loss of revenue	22%
Loss of sales opportunities	7%
Customer dissatisfaction	16%
Regulatory penalties	5%
Employee dissatisfaction	3%
Lost productivity	13%
I don't know	10%
None	7%
Other (please specify)	2%

24. Have you been affected by any cyber-attacks in the last 12 months (malware/ spyware/ransomware/etc)?

Yes, on one occasion	15%
Yes, on multiple occasions	10%
No	74%

25. Which of the following cyber threats have you been affected by in the last year? (tick all that apply)

Carberp	11%
CryptoLocker	24%
CosmicDuke	13%
GOZeus	12%
Heartbleed bug	11%
KeyLogger	25%
Perkle	8%
Podec	5%
Reveton Ransomware	6%
Shylock	7%
SpyEye	13%
Volatile Cedar	6%
ZeroAccess Rootkit	7%
ZitMo	6%
None	0%
I don't know	26%
Other (please specify)	4%

26. Have you reviewed you security policies in the last 12 months in response to recent cyber threats?

Yes, we have reviewed our security policies and have made changes	30%
Yes, we have reviewed our security policies and made no changes	24%
No, we have not reviewed our security policies	30%
I don't know	16%

27. Have you reviewed your backup schedule and RPOs (Recovery Point Objectives) in the last 12 months in response to recent cyber threats?

Yes, we have reviewed our backup windows and have reduced them	17%
Yes, we have reviewed our backup windows and made no changes	29%
No, we have not reviewed our backup windows	36%
I don't know	18%

28. Does your DR solution protect you from cyber threats (ransomware, spyware, DDos, etc.)?

Yes	55%
No	16%
I don't know	29%

29. Which of the following cloud services do you use? (select all that apply)

Xero	1%
Zendesk	3%
Huddle	5%
Akamai	3%
Workday	3%
Freshbooks	3%
Freshdesk	3%
Salesforce	7%
SAP	10%
Google Apps	18%
Office 365	21%
NetSuite	2%
Amazon Web Services	10%
Google Cloud Platform	16%
Microsoft Azure	14%
vCloud Air	3%
None	32%
Other (please specify)	7%

30. Which of the services do you backup? (select all that apply)

Xero	3%
Zendesk	3%
Huddle	3%
Akamai	3%
Workday	4%
Freshbooks	4%
Freshdesk	4%
Salesforce	12%
SAP	15%
Google Apps	15%
Office 365	19%
NetSuite	3%
Amazon Web Services	11%
Google Cloud Platform	16%
Microsoft Azure	16%
vCloud Hybrid Service	6%
None	12%
I don't know	12%
Other (please specify)	4%

31. How do you backup your cloud services?

Within the same cloud	33%
Back to on-premises	32%
To another cloud provider	20%
I don't know	13%
Other (please specify)	1%

32. Have you suffered an outage in the last 12 months for any of these services? (select all that apply)

Xero	1%
Zendesk	3%
Huddle	4%
Akamai	2%
Workday	4%
Freshbooks	2%
Freshdesk	6%
Salesforce	4%
SAP	4%
Google Apps	4%
Office 365	5%
NetSuite	2%
Amazon Web Services	3%
Google Cloud Platform	4%
Microsoft Azure	3%
vCloud Hybrid Service	1%
None	62%
I don't know	10%
Other (please specify)	0%

33. How much confidence do you have in these services to keep your data secure and available?

I feel completely happy with the security and availability of my data	57%
I have concerns about the security and availability of my data but have no plans to stop using the services	38%
I have concerns about the security and availability of my data and am investigating alternative solutions	4%

34. Do you feel a loss of control over your data when using any of these cloud services?

I feel completely in control of my data	49%
I have concerns about loss of control of my data but have no plans to stop using the services	45%
I have concerns about loss of control of my data and am investigating alternative solutions	6%

35. Which of the following services are you planning to invest in over the next 12 months?

Software as a Service (SaaS)	21%
Infrastructure as a Service (IaaS)	13%
Platform as a Service (PaaS)	13%
Disaster Recovery as a Service (DRaaS)	15%
Backup as a Service (BaaS)	13%
Desktop as a Service (DaaS)	5%
Business Process as a Service (BPaaS)	4%
None	53%
Other (please specify)	1%

36. Which factors do you consider to be most important when choosing a cloud service provider? (Tick all that apply)

Security	63%
Data sovereignty	23%
Reputation	32%
Size of company	11%
Functionality of service	39%
Location of hosting	14%
The hypervisor	7%
The hardware	13%
The data centres	16%
The location of the cloud service provider HQ	10%
The standard of SLA (service level agreement)	29%
Other (please specify)	5%

37. Do you use any tools for analysis of file data?

I don't know	29%
No	68%
Yes (please specify)	4%

38. Do you actively distinguish between files that have been recently accessed and files that have not been accessed in over a year?

Yes	30%
No	54%
I don't know	16%

39. What is your fastest area of storage growth?

Email	23%
File Data	21%
CRM	8%
Test and development environment	5%
ERP	4%
Accounts	6%
HR	1%
Log data	2%
Archive	8%
I don't know	20%
Other (please specify)	2%

40. What is your biggest cost associated with storage growth?

Backup	12%
Hardware	25%
Maintenance	17%
Physical real estate	8%
Support contracts	6%
Cost of high performance disk	4%
I don't know	28%
Other (please specify)	1%