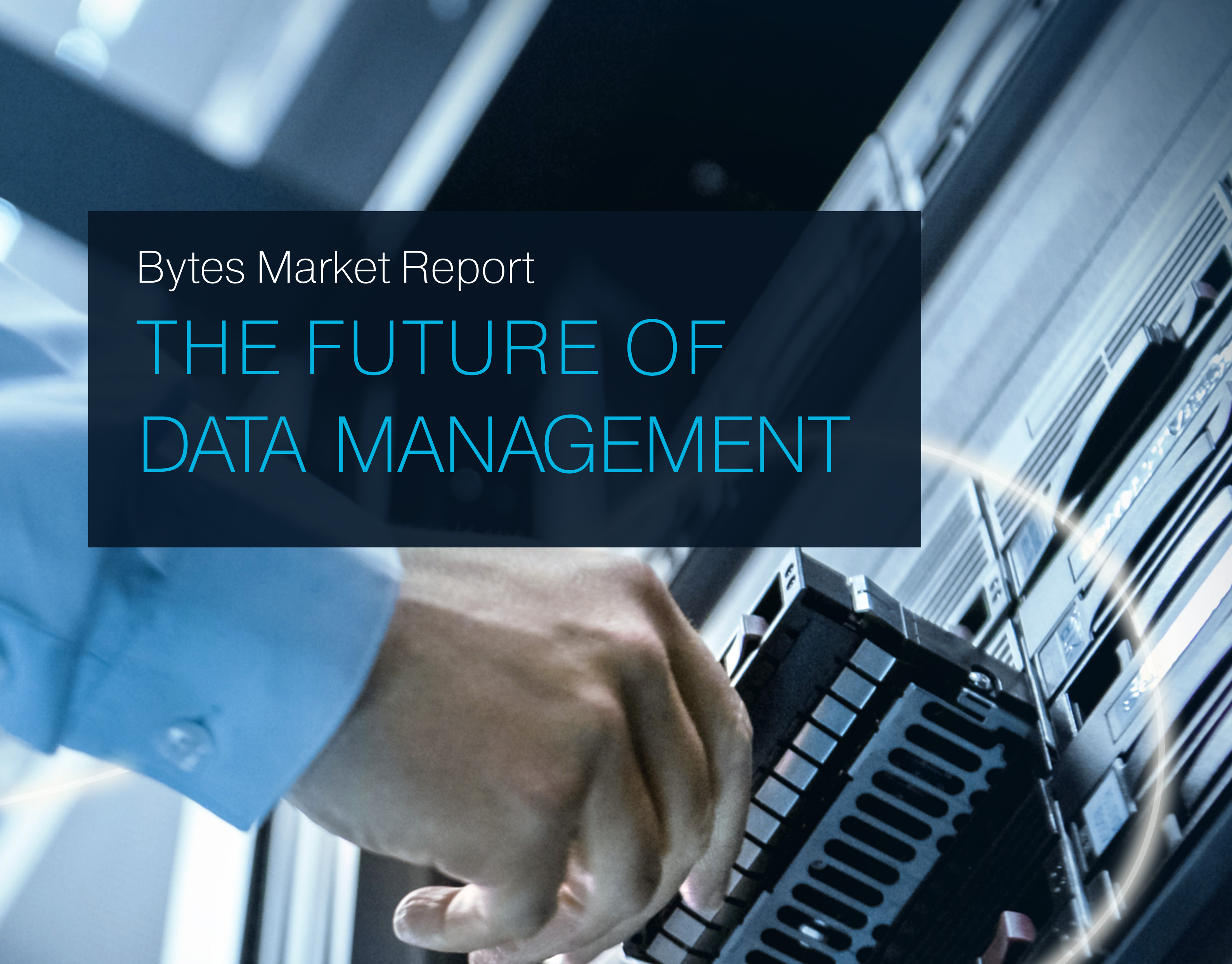
Bytes Market Report

THE FUTURE OF DATA MANAGEMENT



BYTES

Smarter together

About this Market Report

Mathematician Clive Humby is credited with first coining the phrase “Data is the new oil” but it wasn’t until the Economist published a report in 2017 titled, “The world’s most valuable resource is no longer oil, but data” that the phrase became widespread.

Today and despite the phrase being broadly agreed with by Company Directors, nearly 75% of organisations are not using their data to make informed decisions and drive their business decision-making.

In addition, over 40% of organisations that are using Office 365 are not backing up their data and as an average, organisations are only 58% confident that their data is safe and fully protected against all threats.

Given the importance of data and to help organisations understand how they can better manage theirs, we surveyed 206 UK IT Professionals, ranging from IT Managers, CISO’s and Heads of IT from a variety of companies.

This report answers the critical questions asked and includes further insights and commentary by Matt Compton, the Head of Data Management at Bytes and Robert Rhame, the Director of Market Intelligence at Rubrik.

Overview

Changing attitudes to Data Management

Since the introduction of the GDPR, data has made its way from the basement to boardroom, with Company Directors realising the potential and pitfalls that good and bad data management poses.

What is interesting from reading the survey responses is that while a lot of organisations have made positive progress improving their data management hygiene, there is still a long way to go before the majority are confident their data is fully protected and being leveraged to the max.

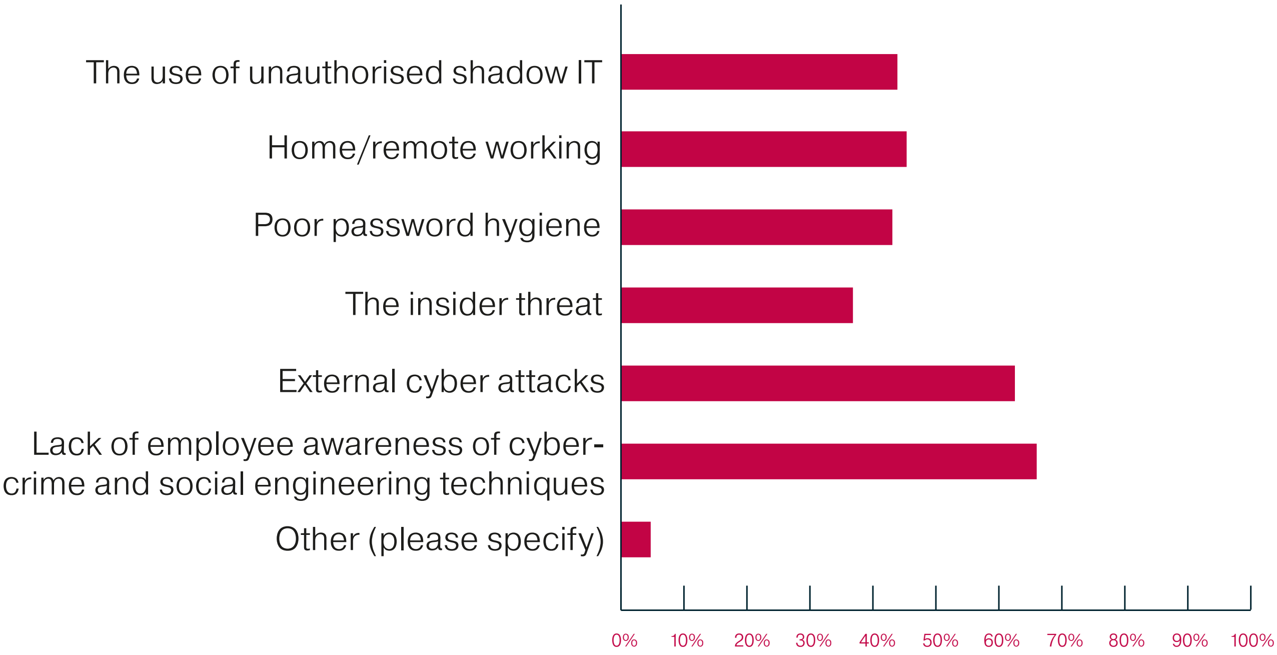
5 Key Changes to Data Management:

1. With a tectonic shift towards remote working and with greater understanding that email still remains the number one targeted vector by cyber criminals, organisations are taking greater measures to protect their endpoints and lockdown their VPNs.
2. Organisations are recognising that cloud vendors operate a shared responsibility model whereby the vendor takes responsibility for the availability of their platform and services and the customer takes responsibility for the security and backup of their SaaS data, such as the data that exists within their Office 365 environment. As such, greater focus is being placed on protecting and backing up environments using third party tools.
3. Given the growing complexity and fragmentation of data, backup teams are moving away from relying on on-premises environments and legacy management tools and seeking out new ways to backup and manage their data by leveraging cloud infrastructures and light-touch backup providers.
4. While the GDPR focused attention and effort on cleaning up data repositories, much of the good work done has now been undone as maintenance measures were not put in place to enable automated and ongoing data classification and labelling. As such organisations are recognising that Dark Data represents a growing cost and compliance risk and are looking at measures to address it.
5. Most organisations know they should be using their data more to power their decision-making but need help getting started so are taking steps to work with Partners, such as Bytes, to help them put data at the core of their business growth strategy.

In the context of good data management hygiene, James Hastings, IT Manager at Trapeze Group (UK) comments, “There are five core components of a data strategy that work together as building blocks to comprehensively support data management across an organisation: Identify, Store, Provision, Process and Govern. Have a data strategy plan that is designed to improve all of the ways you acquire, store, manage, share and use data.”

This report expands on the points above and details our predictions for the future of Data Management.

What are your main three concerns with regards to Data Loss Prevention?



Social engineering has been the number one area of concern for a while. In addition, cyber criminals are getting ever more sophisticated with their tactics. COVID-19 has compounded the problem as cyber criminals have been and continue to exploit the extraordinary circumstances by creating highly relevant and targeted messages. If they manage to get the right message through to the right person at the right time their chances of success are high and they only need to be successful once.

During the first two weeks of lockdown, Google alone reported blocking over 18 million malicious COVID-19 related emails.

Whilst organisations are right to focus on social engineering, they should also look at protecting their email platform more generally, as email is still the number one targeted vector by cyber criminals.

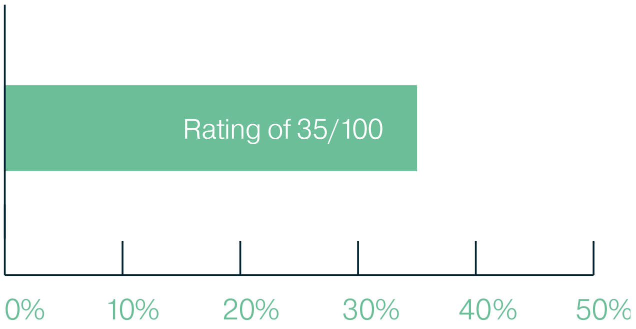
In addition to email, managing data flowing in and out of Microsoft Teams is also a potential cause of data loss as native controls within Microsoft Teams are limited. The use of tools to provide additional protection is therefore recommended.

Home working is a greater concern than before as cyber criminals are successfully exploiting more exposed endpoints to then continue their attack directly into the network via VPNs. More work needs to be done by some organisations to lock down their VPN. The lack of firewalls, web proxies, single sign-on, effective patch management and general MDM hygiene are also contributing factors to the home working conundrum.

The area that should be a higher cause of concern, particularly within larger organisations, is the Insider Threat. This is an underestimated risk that needs due focus and attention.

Ahmed Gumaa, Network and Security Analyst at Le Creuset comments, "Make sure you identify the data that you need to protect. If you don't know what you are protecting, then your outcome will be incomprehensible."

How much of an issue is Shadow IT for you?



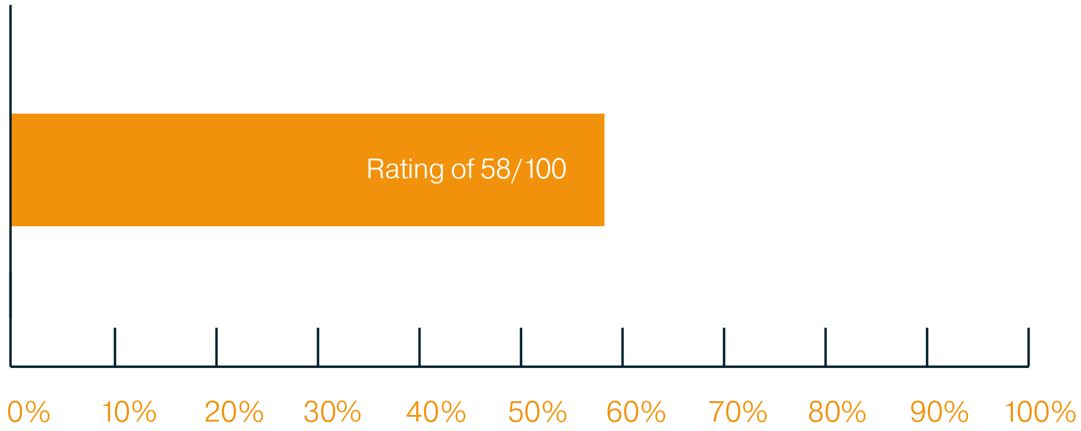
This score is the average rating across all respondents.

In many cases the use of cloud applications can help boost productivity and collaboration so IT should not be in the business of preventing universal access to them and stopping the business. They should however embrace and secure non-IT owned applications by offering ITaaS and Security-as-a-Service to the business units that wish to drive these "unauthorised" programs. IT and Security should help provide measurable metrics for proper administration (such as timely patching, responsiveness and uptime).

Organisations that are concerned about Shadow IT are advised to first size the problem by undertaking a Shadow Application and Data assessment. Bytes can help with this and can help organisations have better visibility of what Shadow Applications are being most widely used and the data flow surrounding them.

With visibility comes manageability and the ability to prevent avoidable data loss.

How confident are you that all of your data is safe and fully protected against all threats?



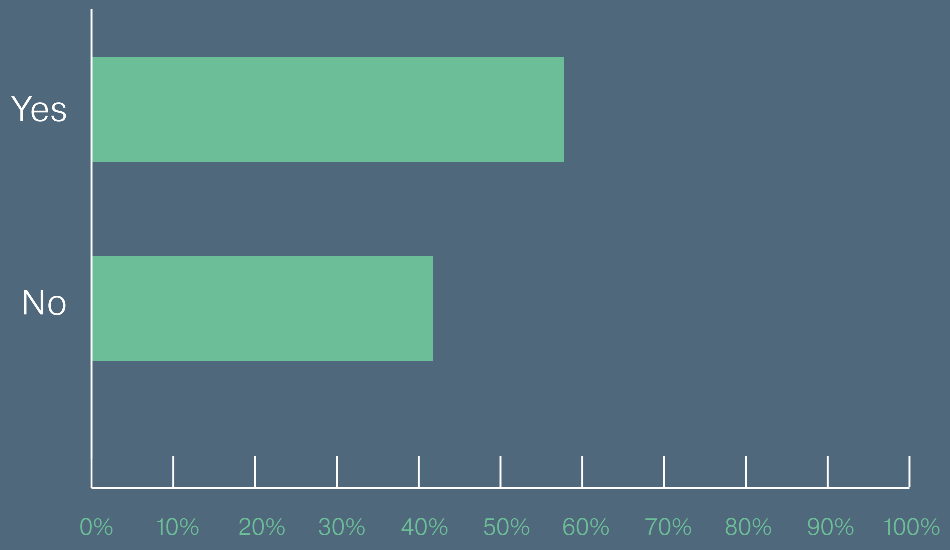
This score is the average rating across all respondents.

Whilst no organisation is going to be 100% confident that all of their data is safe and fully protected against all threats, a confidence score of 58% is very low. Confidence levels are directly correlated to an organisation's tolerance to risk and resilience.

Low risk and highly resilient organisations, for example, will have multiple layers of measures in place to protect their data. For example, in addition to protecting their endpoints, datacentres and internal systems, they will also be protecting their perimeter and beyond their perimeter - extending their cover to the web and to the cloud.

Aftaab Allyman, Technical Architect at Cantium Business Solutions, comments, "Run a playbook of all the data disasters that can happen on your real data to surface all weaknesses. Categorise them in risk weight and prioritise the remediation activities that arise."

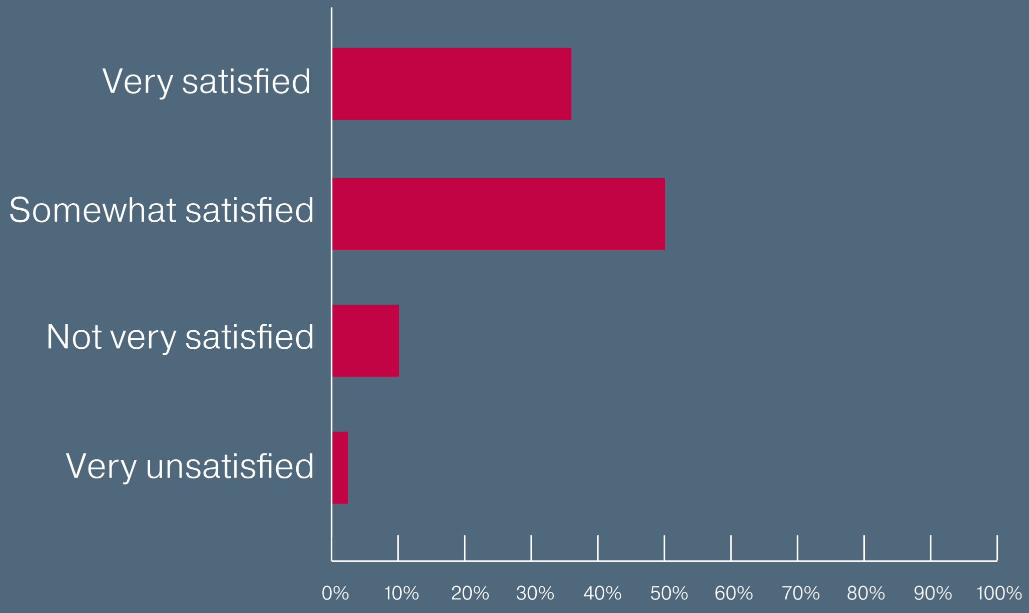
Are you currently backing up your Office 365 environment?



Over 58% of respondents stated that they are backing up their Office 365 environment - this is higher than a few years ago and shows more organisations are understanding the shared responsibility model adopted by most cloud vendors. In this model, the cloud vendor, in this case Microsoft, accepts responsibility for the availability of their platform and applications, while organisations using their services accepts responsibility for the data that resides within them.

SaaS backup discipline should be the same as datacentre discipline. This is a view shared by Leo Cunningham, Head of InfoSec at Zonal Retail Data Systems who comments, “Backups are a must, as with data classification and protection.”

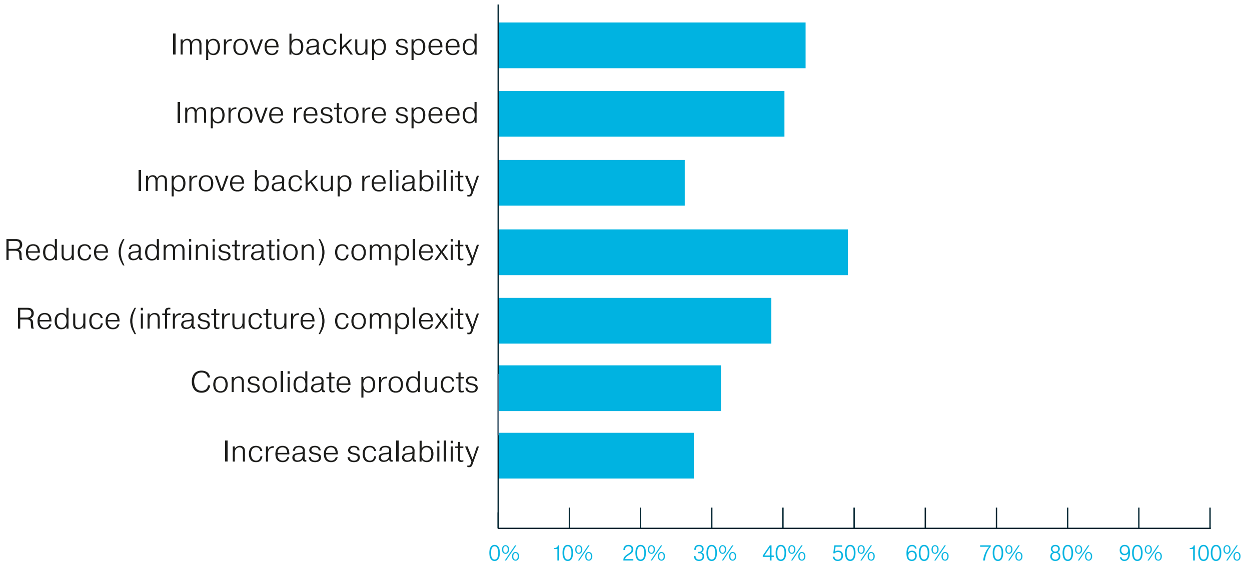
Taking into consideration the amount of data you have and the frequency it needs to be backed up, how satisfied are you with your current back up solution?



The findings from this question are in line with the broader market analysis and with over 60% of respondents not stating that they are 'very satisfied' with their current backup solution highlights there is room for improvement around RTOs and RPOs, particularly when it comes to having to manage multiple tools.

With data now residing in physical, virtual and cloud repositories and with each requiring different management tools with different SLAs, backup management is a growing headache.

What three improvements would you make to your organisations backup solution?



As mentioned in the commentary above, with data now residing in multiple repositories, backup solutions are becoming ever more complex. Add to the mix M&A activity, poor documentation and resource-heavy legacy backup management systems that often require specialist and dedicated resources, it is easy to see how environments can quickly become highly inefficient to manage.

It is no surprise therefore that "Reduce (administration) complexity" is coming out top here. The good news is there is light at the end of tunnel, as there are newer tools on the market, such as those provided by Rubrik, that are much simpler, lighter touch and that have been designed from the ground up to address this very specific and vey common problem.

Regarding the desire to improve backup and restore speeds, the key here is to have a clear tiered storage strategy that incorporates on-site appliances, cloud (or an S3 on-premise solution) and a deep archive.

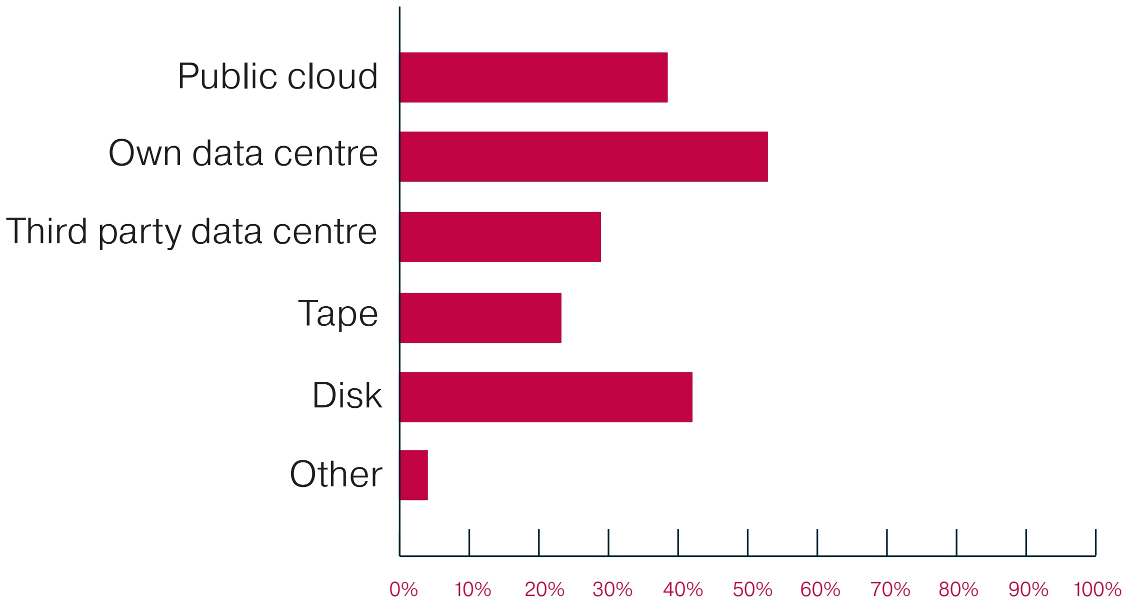
On-site appliances provide the fastest recovery times for the most recent data since they do not rely on transferring large amounts of data across the internet.

Backing up to tape on the other hand is very cost effective however restoring individual files and physically transporting and re-ingesting recalled tapes from off-site storage can be time consuming.

Selecting the correct architecture is a balance. There are also issues with using Cloud as a destination and these physical and network considerations must be examined especially where long retention is required.

Again, due to its architecture and when implemented as part of an effective tiered storage strategy, Rubrik can help materially improve RTOs and RPOs.

What do you back your data up to?



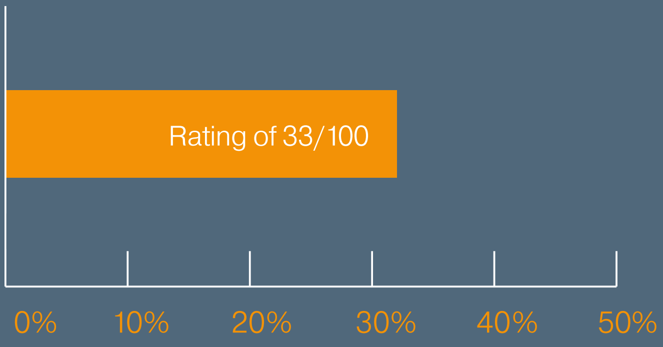
The trend to backup to public cloud has been on the increase for a while, mainly fuelled by increasing confidence levels around cloud security, but these figures show the trend is happening much faster than forecasters predicted, largely at the cannibalisation of tape as the decline in tape is virtually equal to the increase in cloud.

Tape is not disappearing anytime soon however, particularly as it is widely used by the major cloud vendors for the cold tier, but its need for physical management is not conducive to the rise of home working. With more IT teams working from home, managing tape is increasingly more challenging.

In addition, many tape libraries are aging and in need of refresh. This is where tape's "image problem" comes in with CIOs reluctant to request budget for a new tape library at the same time there is a big push to the cloud.

Richard Murdoch, IT Technical Team Leader at Galway Clinic comments, "Ensure that you have multiple copies of data stored in a safe and efficient manner. In other words, De-duplicate your data and tier it so that the data that is most accessed can be done so quickly."

How much of an issue is Dark Data for you?



This score is the average rating across all respondents.

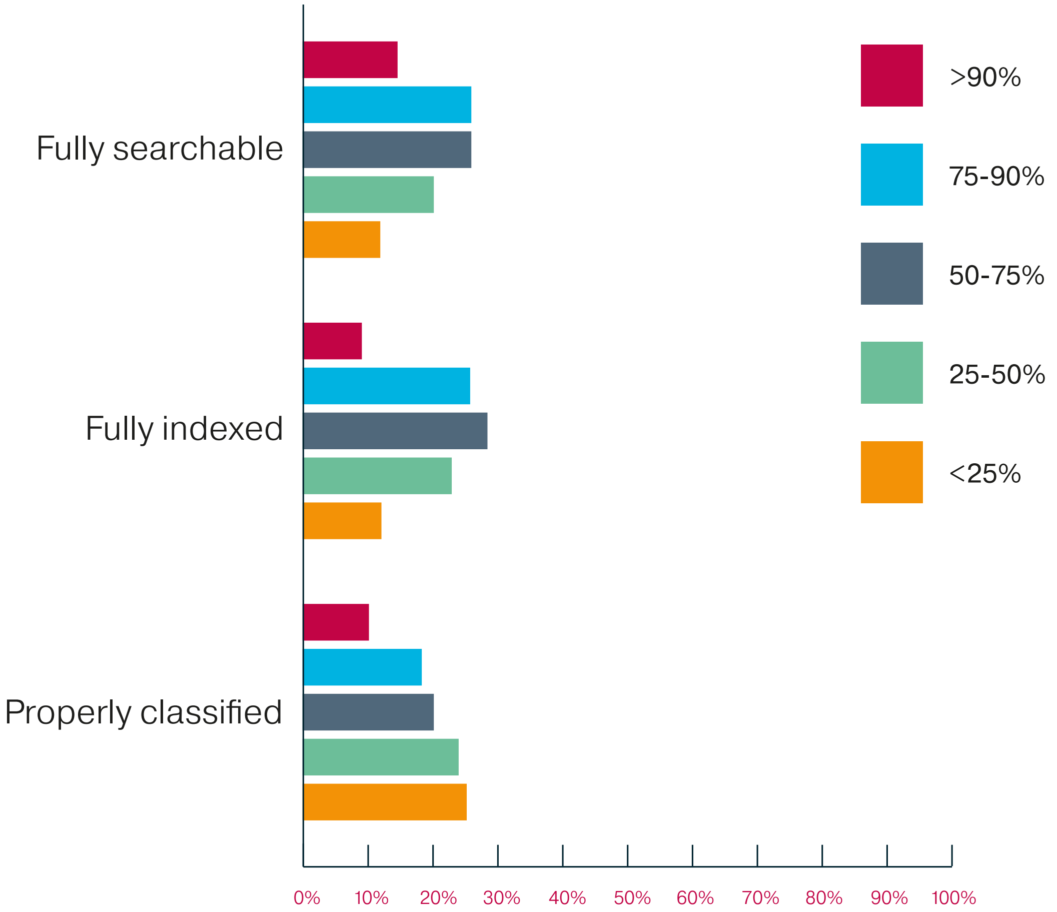
While the introduction of the GDPR drove a lot of activity around dark data analysis, much of the effort was centred around a specific point-in-time. Since then the problem has continued to fester. Research shows that after one week of data creation it goes dark, so unless there is a strategy in place to address this, the problem is going to get quickly out of hand again.

As was the case before the frenzy of GDPR-related activity, organisations today don't confidently know what data they are storing which has implications on cost and compliance.

While storage costs continue to decrease many organisations find it easier to simply keep saving data rather than clean it. This has been the case for twenty years and after multiple migrations most organisations today have many, many terabytes of data they do not need. Aside from the cost of actual storage, the cost of managing and protecting it do not disappear. This means that excess backup licensing and capacity is needed. Furthermore eDiscovery tools charge by the terabyte, so the more the data, the higher the discovery costs.

Peter Wilson, Systems Administrator at M&C Saatchi comments, "Find out what data the users really need to keep and focus on that. Everything else isn't important and is just costing you money."

What percentage of your unstructured data is:



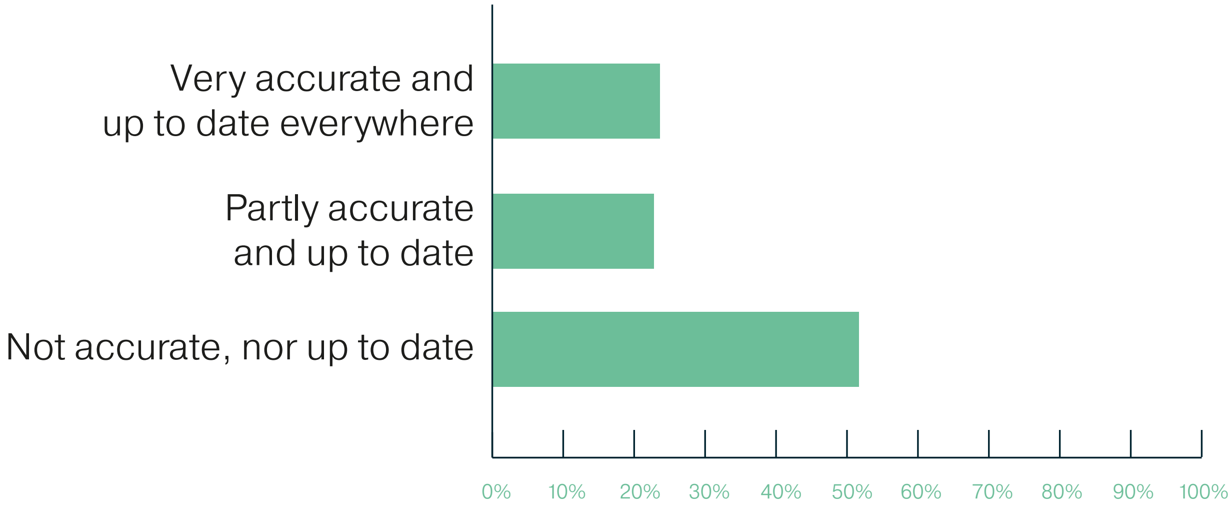
At face value some of these findings seem okay, however, it is important to look at the detail, specifically around data residing in the cloud – such as OneDrive. In most cases organisations have good hygiene relating to their on-premise file stores, however this is often not the case with SaaS applications.

While the likes of Office 365 does have its own automated classification tooling built in, human input is still needed to ensure full classification compliance, which is why larger organisations are now heavily investing in teams to support their DPO.

Without a clear data management strategy in place and as more cloud applications and services are used, the problem is likely to increase.

Jim Kingston, Service Management Manager at Ervia, comments, “Bring the end users along with you or it will not work. Ultimately they own the data and need to understand how valuable it is and how it needs to be protected and destroyed properly when no longer valid.”

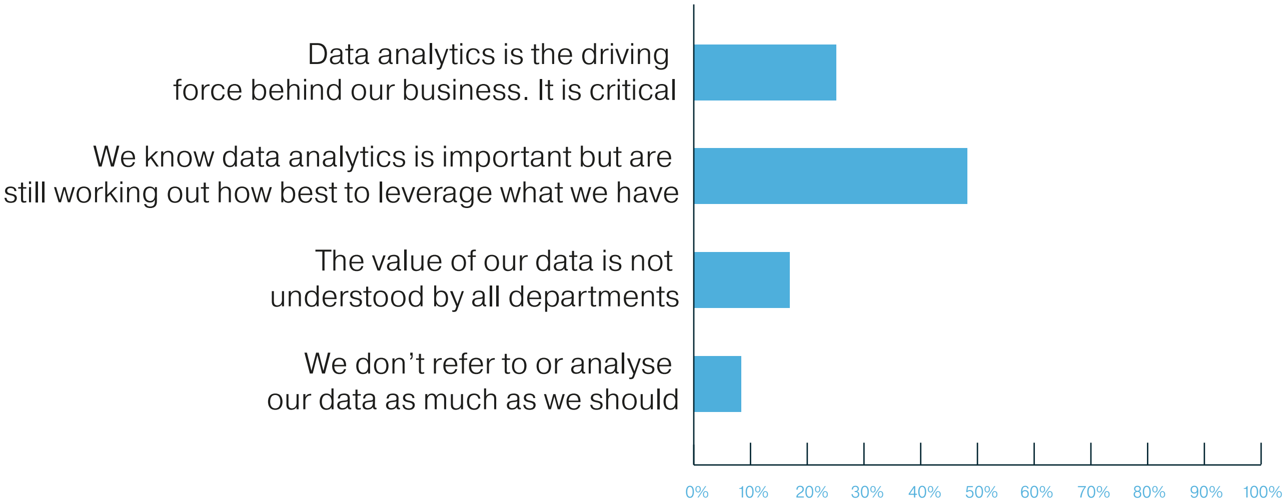
How accurate and up to date is your data classification and labelling across all your company data?



As mentioned above, many organisations took steps around the launch of the GDPR to get their house in order, however few have since managed to maintain the level of effort needed to ensure ongoing data classification and labelling compliance. The challenge in most cases is finding the data owner, a problem exacerbated by repeated data migrations, attrition and business unit disinterest in undergoing a protracted classification and culling exercise. When they have been identified, it is suggested to:

"Make the users the owners." Adam Sheppard, Senior Design Officer at Surrey County Council.

How central is data to your business decision making process?



There is nothing unpredictable in these findings. In most cases organisations know they should be leveraging their data more, but few know where to start.

What is clear is that those organisations who have figured out how to harvest their data effectively are outperforming their competitors. One example of this is a large fast food chain that has been able to identify which menu items are selling best at a micro level across its extensive network of outlets. Not only has this helped them optimise their stock control but has also helped them better target their local advertising - improving their returns. There are many similar examples.

Often the problem is not to do with a lack of data scientists or data analytics software however, but is not knowing what questions to ask.

> James Davenport, Professor of IT at the University of Bath comments, “Start from the business, not the data.”

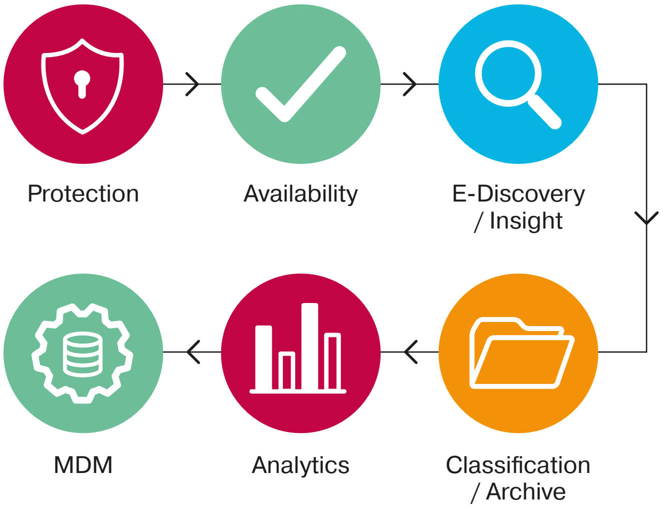
Organisations that want to understand how to best use their data should invest in a start-up assessment. Bytes have a team of data scientists who are expertly trained to help with this. The assessments help organisations understand what they are hoping to achieve from their data and help them prioritise their action list.

Survey Analysis

The findings of this survey highlight that data management is a complex issue.

- Employees need access to data wherever they are, creating access control and security challenges;
- Data is highly fragmented and residing in multiple data repositories, creating classification, eDiscovery and backup challenges;
- Data science and analytics is a specialist area which many organisations struggle with, creating data intelligence challenges.

One way of helping to overcome the data management problem is to break the problem into 6 core areas:



By taking this approach organisations can more easily define a "success scale" for each area, then assess how well they are doing against each. Plans can then be put into place to help move the organisation up the various scales.

During the planning phase organisations will be able to quickly determine where third party help is needed and precisely what help is required. In some cases it may be to simply get started, such as in the specialist field of data analytics and in others it may be help simplify the current state, such as with data backup.

What is important is that data management remains a Boardroom focus as lack of control and visibility can quickly have material cost and compliance consequences.

Wherever data is residing, it is the responsibility of every organisation to know where it is, how it is being protected and backed up, how it is being used, how it is being classified, how easy it is to find and how it is being used to power business decision making.

Bytes have expertise in each of the 6 areas opposite and can help organisations define their success-scales and implement measures to help transform them from their current "as is" state to the desired "to be" state.

Key Takeaways

Email

Email still remains the number one targeted vector by cyber criminals so due to the increase in home working it is more important than ever that organisations are properly protecting their endpoints and more effectively locking down their VPNs.

Office 365

More organisations are taking measures to properly backup and protect their Office 365 data to prevent loss or exposure to theft than in previous years. This demonstrates awareness of the shared responsibility model adopted by all the major cloud vendors.

Administration Complexity

With data now residing in physical, virtual and cloud environments, organisations are looking at measures to reduce the administration complexity of their backup solutions. Rubrik has published numerous customer success stories where organiations save between 60-90% of the time previously spent on backup.

Dark Data

While not reflected in the findings, Dark Data continues to pose a big problem for organisations as if not properly managed it will continue to cost organisations unnecessary money, consume resources and open them up to compliance related risk.

Business Intelligence

Most organisations know they should be using their data more to power their decision-making but over 70% are not doing it effectively. Bytes has a team of data scientists that can help organisations get started with their data driven programme and begin using their data effectively.

The Future of Data Management

Robert Rhame, Director of Market Intelligence at Rubrik

It’s the End of the Office as we Know it (and the CFO feels fine)

The pandemic has demonstrated that employees can work remotely and many organisations are rethinking their mix of on-premises seating requirements. This trend will outlast the end of the current turmoil and the implications for the on-premises datacentre are enormous. There will be offices, but they will have to be reconfigured in many cases to comply with distancing requirements. This could lead many organisations to just decide it is not worth it. Especially given that COVID-19 might mutate into COVID-20 or 21. CIOs and IT Leaders should expect a permanent 30-50% reduction in office space in those organisations that leverage knowledge workers. This reality will drive many other decisions.

New Paradigm in Collaboration

We've seen that people can work effectively from home, but nothing really beats face to face when it comes to collaboration and sales. The emergence of video conferencing fatigue is evidence for that. Web collaboration sessions with overly large teams are time consuming. Mixed, enhanced and virtual reality meetings don't really exist today in any widespread fashion but they will.

The Acceleration of Cloud Adoption

Remember those cloud projects that were on the back burner six months ago? We have come a long way, essentially delivering 2 years of transformation in 2 months. This fluid future of the hybrid datacentre gets a boost because many employees may never go back to regularly being in the office. This makes major purchases for datacentre equipment look a bit out of balance with the emerging reality. Up until 2020 CIOs looked at their most important applications and those that had the highest performance requirements and held those close in their own datacentre. Years of discipline surrounded that walled-in and air-conditioned area of intellectual property and competitive differentiation. For the rest of 2020 and if a large portion of the employees remain permanently remote, organisations will have to deal with the VPN.

Satisfying Regulatory Requirements

Some organisations, especially government and financial organisations have to adhere to regulatory requirements that force them to hold certain data on-premises. The tectonic shift to remote workers and a dwindling focus on the datacentre that comes from accelerated cloud adoption will carry much with it. Securing that data enough to satisfy regulators and modelling the new risk becomes paramount. Visibility across the data estate suddenly gets a little more urgent.

The Death of Tape (Long Live Tape!)

Tape will outlive us all, but its role is changing and its place in the datacentre alongside backup is dwindling by the year. It is not the reliability or the cost that is driving this trend. Tape is simply not really as appropriate for backup as it once was. Despite being offline from attackers, the requirement to live mount and instantly restore workloads is not possible with tape, which limits its usefulness in a ransomware situation. In addition, the forward looking CIO who is tasked with executing a cloud strategy usually feels that refreshing the tape library might not be the best career decision with the CFO. We will continue to see tape used as an archive tier, especially in the cloud.

Decentralised IT and Security

The trend of empowering the business through digital transformation initiatives started several years ago, but the organisational impact of "digital" is more than an increasingly overused phrase. Transformation delivery is a move from a services delivery model to a model where IT is more embedded in levelling-up the business activities, but less responsible for them. In this way IT collaborates and conspires with the business to find new ways of enabling them. The ultimate goal is to support non-IT led projects with the discipline, data integrity, security and reliability they need. Aside from the official collaboration between IT and business units on things like AI/ML, IoT, BI/Analytics, expect that business leaders will be increasingly ready to engage ITaaS and Security-aaS to help with their self-funded SaaS projects and developer initiatives. This requires a fundamental cultural shift from the "no" mentality to one of enablement in some organisations, in others where the Chief Digital Officer role has been around for a while this will be an easier and more natural transition.

Need advice with your Data Management Strategy?

To help you identify the areas of your Data Management strategy that need attention and help guide you through the process of documenting a plan to resolve them, you should book a **Data Management Workshop** with Bytes.

The workshop: **3 steps to getting answers**

Our data management and cloud consultants will consult with your company and spend time with your team, sharing knowledge, exploring ideas and identifying possible solutions.

Step 1: **Assess**	Step 2: **Discover**	Step 3: **Recommend**
We'll discuss your current data management landscape, applications and locations. We'll baseline your current backup and DR - and look at a data management roadmap.	Having understood your needs, we'll look for gaps and potential improvements that could pay off for your business. We'll consider various vendors and their offerings.	We'll align appropriate technologies and services to create a solution. We'll also produce a bespoke report that could support a business case and help with planning.

Alternatively if you have a plan in place and need instead to pinpoint where your biggest data security threats are, you should book a **Data Risk Assessment.**

The assessment will help you:

Identify and prioritise at-risk areas like global access, stale data and inconsistent permissions.

Discover overexposed and at-risk sensitive & classified data, including PII, HIPAA, PCI and more.

Review access controls and authorisation processes and find out where you can improve.

Analyse folder and file access to determine where you're most at-risk and easily reduce your risk profile.

Expose data vulnerabilities so that you can be confident in your data security.

About Bytes

Bytes provides leading insights, expertise and practical help to over 3,600 organisations nationwide. We enable effective and cost-efficient technology sourcing, adoption, security and management of software, hardware and cloud services.

Our UK business began in 1982 and has grown profitably each year to reach a turnover in excess of £500m, making us one of the largest software services and solutions businesses in the country.

The most important aspect of our business is our people. We value initiative, teamwork and achievement. Together, we focus on providing the highest levels of service so we can deliver our ultimate goal – customer satisfaction and success.

Our customers include leading brands across retail, media, finance, manufacturing, legal, healthcare and the public sector.

We work closely with the majority of IT vendors and are delighted to regularly receive honours from them in addition to being named a Sunday Times Best Company to Work For 2020.

About Rubrik

Rubrik helps enterprises achieve data control to drive business resiliency, cloud mobility and regulatory compliance. Reasons for partnering with them, through Bytes, include:

- Cloud Data Management – achieve near zero RTO's, instant search results and immediate hard savings of 30-50% from software convergence.
- Ransomware recovery – instantly access your applications and data in an immutable format, allowing you to resume business within minutes of an attack.
- Simplification – with just a few clicks free your apps and data from infrastructure and benefit from policy, security, compliance and access controls.
- Automation - integrate Rubrik into your ideal stack to deliver application and data services. Create what you want, when you want it via a single portal.
- Modernisation - Rubrik eliminates legacy point solutions with a converged software platform that's simple to use.

To understand how Bytes can help you develop and enhance your Data Management Strategy, get in touch and start a conversation today.

BYTES | Smarter together

UK Head Office

Bytes House
Randalls Way
Leatherhead
Surrey
KT22 7TW

T 01372 418 500
E tellmemore@bytes.co.uk
W www.bytes.co.uk