Discovering trust in your data and security

Measuring the confidence of **marketing leaders** in their data and security practices

Your Tomorrow, **Today**

Methodology

The results presented in this report are based on a mobile-only, 23-question global survey. This survey targeted Manager, Director, Vice President or C-Level executives with influence in the decision-making process of cloud solutions, platforms, and infrastructure or department specific software. Respondents worked within organisations generating revenues between less than £1 million to more than £500 million, with 100 to 50,000 employees.

Contents

ORACLE®
Cloud
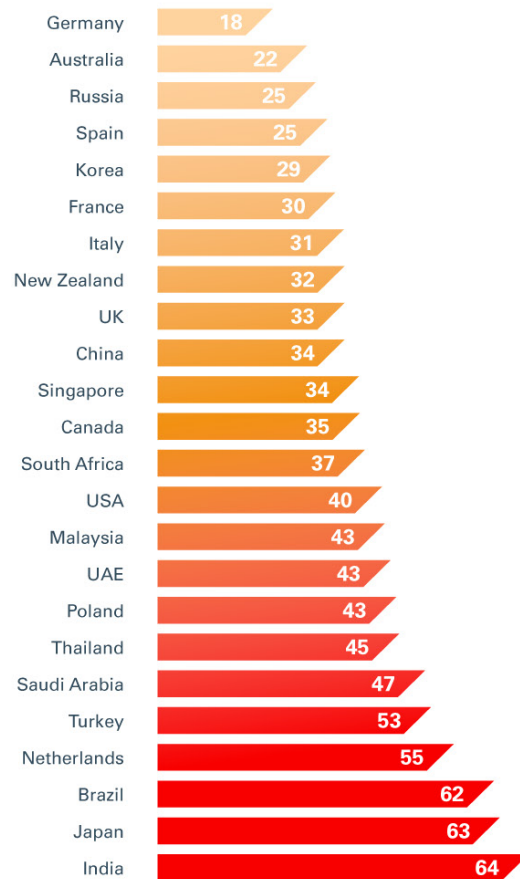
Who believes they are truly capable of managing this deluge of data? Decision makers in **Brazil, India, and Japan say they are the most capable of managing the data they generate**.

Within your organisation, how manageable is the amount of data generated? – Completely manageable – Highly confident

Base: Global population, 24 markets, nr. 5,539

% stating data as completely manageable

Country	%
Germany	18
Australia	22
Russia	25
Spain	25
Korea	29
France	30
Italy	31
New Zealand	32
UK	33
China	34
Singapore	34
Canada	35
South Africa	37
USA	40
Malaysia	43
UAE	43
Poland	43
Thailand	45
Saudi Arabia	47
Turkey	53
Netherlands	55
Brazil	62
Japan	63
India	64

Europe

Africa

North, Central and South America

Asia, Japan and Pacific

ORACLE
Cloud

Try Oracle Cloud today

3

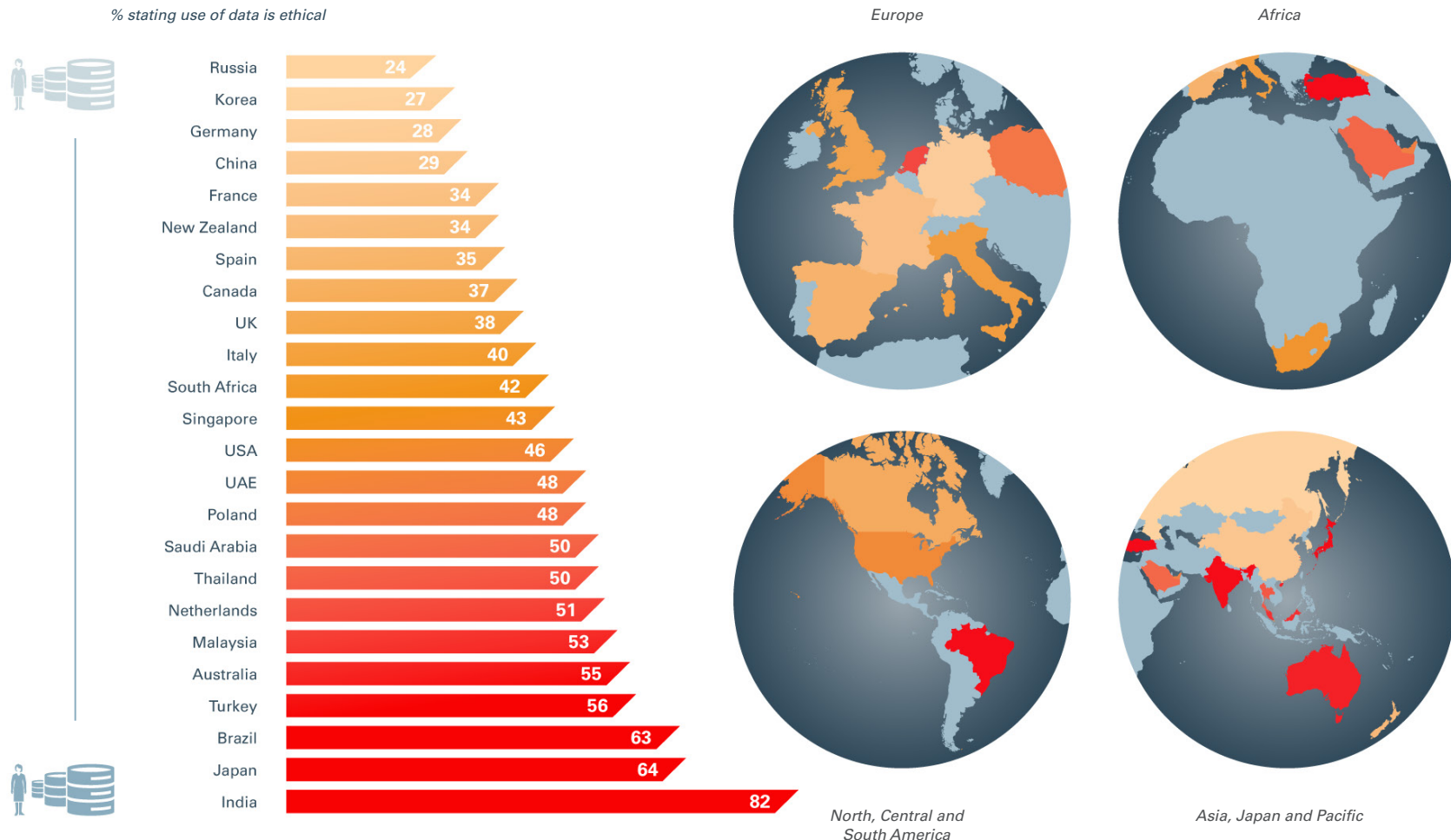## Ethical use heat map

Perhaps of greater sensitivity – who tells us they are most confident that their use of data is ethical? Decision makers in **Russia score themselves the lowest alongside Korea, Germany and China** – whilst again India, Japan and Brazil hold themselves in high regard. Coincidence, or is there a cause and effect between these two maps? Let's find out...

Based on the last six months, how confident are you that your organisation's use of data is ethical? – Highly confident

Base: Global population, 24 markets, nr. 5,539

% stating use of data is ethical

Country	%
Russia	24
Korea	27
Germany	28
China	29
France	34
New Zealand	34
Spain	35
Canada	37
UK	38
Italy	40
South Africa	42
Singapore	43
USA	46
UAE	48
Poland	48
Saudi Arabia	50
Thailand	50
Netherlands	51
Malaysia	53
Australia	55
Turkey	56
Brazil	63
Japan	64
India	82

Europe

Africa

North, Central and South America

Asia, Japan and Pacific

ORACLE
Cloud

Try Oracle Cloud today 4

The business of tomorrow is a **trusted business.**
This study reveals:

- How well organisations globally are coping with the deluge of data

- Whether we are truly getting the value from the data we have

- The ethical mindset – and the three steps to *ethicality*

- The role of intelligent databases – how to maximise their potential and control bias

- How far do business leaders appreciate the importance of responsible data use?

Let's find out more...

Below is a snapshot of the key take-aways:

- **Marketing leaders believe data management is a burden on businesses:** Above any other line of business, less than 40% of marketers consider themselves to be highly confident in their ability to manage data. Looking ahead three years, they do not feel that this level of confidence will improve.

- **Yet less than half of organisations have a data management strategy in place:** How data is used and who is consuming that data is essential to the security and innovation of an organisation. Decision-makers within organisations should understand this and ensure even basic strategies are in place to manage data.

- **But data management strategies positively impact security across all lines of business:** Evidence shows an alignment between those that have a data management strategy and implementation of employee education – the issue is that not enough are doing this.

- **Data security protocols are not understood or, more worryingly, not abided by:** One-quarter of respondents say that their biggest concerns around data security across the organisation is blindness about how data is supposed to be used, internal disregard about the application of data regulations and, most concerning, the failure to enforce company security policies. Good practice requires basic protocols to reduce uncertainty and make it manageable, and 'managed'.

- **Key departments are still not accepting both accountability and responsibility for data management:** There is clear confusion about who is meant to take the lead. Less than half, across all lines of business including marketing, accept accountability for their data, and a further third take responsibility for key actions only. IT leads the way in this respect. There is an opportunity to resolve this challenge but critically all actions should start with taking accountability.

- **Security is a concern for all:** Only 41% of marketing leaders (43% across all respondents) are highly confident in their security of the data that their organisation holds. Although marketing is ahead HR it is still some way short of where we would expect this to be.

- **Only 50% of marketing leaders agree that managing data security was very important to their organisation:** These findings may demonstrate the ongoing fight between short-term department goals, and longer-term security considerations.

- **Overall, respondents are getting too little from their data:** Only 37% of marketing leaders, and 39% of respondents globally, are highly confident that their organisation can manage data to generate meaningful insights. Smaller organisations are struggling the most to extract insights out of the data, likely due to the lack of infrastructure. However, larger organisations are not faring as well as we'd expect, potentially due to the quantity of data they must deal with.

- **Only 39% of marketing leaders are highly confident in their organisation's ethical use of data:** Just under one-fifth of respondents overall are not confident at all. This is concerning given the fact that ethics and responsible use of data have a direct impact on reputation and trust.

- **Organisations must be able to lead with data, not be overwhelmed by it, but this is simply not the reality.** As we dug deeper into the findings, we discovered that departments were struggling with respect to their confidence levels around security, the insights they draw, ethical and responsible use, and their overall understanding of who was accountable for data.

ORACLE® Cloud

Data management

Ensuring quality to deliver greater value

Only 35% of marketing leaders believe that data is completely manageable.

Within your organisation, how manageable is the amount of data generated? – Completely manageable

* Reasonable expectation estimated at 80% or higher

100%	100%	100%	100%
80*	80*	80*	80*
35	**34**	**45**	**34**
Marketing	HR	IT	Finance

Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today   9

There is a new data paradigm.
Data is the new currency in the
digital age.

Poor data management practices inevitably lead to poor outcomes, with bad decisions based on bad data. Data must also be protected, with weak practices leading to cyber breaches. And the reputational damage to an organisation's brand cannot be underestimated. However, when managed well, data offers a competitive advantage.

In the current landscape, there is no denying that the responsibility of marketing leaders is shifting. They must do more than sell a product, they must orchestrate memorable experiences for customers; customer experiences (CX) that in turn build brand loyalty. In this 'experience economy' CMOs must become masters of data to deliver empathy at scale and build deep relationships with customers.

This requires better data, analytics, technology, aligned processes, and an organisational culture that supports it, but most important of all this requires ensuring that the data that is used is robust, accurate and up-to-date.

Now more than ever, marketing leaders must expertly manage consistent, realtime data across all channels and interactions with customers, to include third-party data as well as internal financial data, sales and digital analytics, and a host of sensor and edge-generated data. This requires the centralisation of data to get the single view of the customer and their behaviour.

The brand's unique personality and customer experience require CMO creativity, backed by scalable and responsive technologies that boost success. CMOs who feel accountable for brand protection and trustworthy data will have a crucial and positive impact on customer experience and loyalty, ultimately leading to brand trust.

ORACLE®
Cloud

IT teams are most likely to find the data generated across tasks to be completely manageable;
– marketing teams feel less capable in comparison. Financial reports and employee records
are among the top tasks considered most manageable across all lines of business.

%
- IT
- Finance
- Marketing
- HR

*Within your organisation, how manageable is the
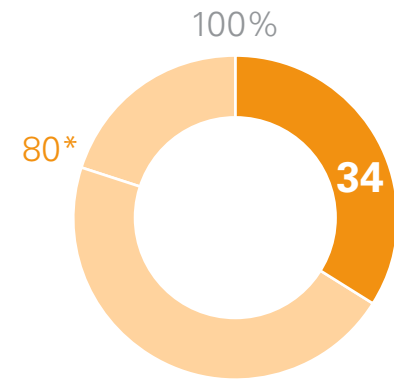amount of data generated by the following? – Completely manageable*

	Employee records	Financial reports	System logs	Service usage data	Customer data	Social conversation data	IoT and other sensor data	Third-party data
IT	52	50	47	46	45	41	42	38
Finance	41	40	35	34	35	31	29	29
Marketing	41	39	35	37	37	32	30	30
HR	43	38	34	34	35	30	30	27

*Base: Global population,
24 markets, nr. 5,539*

ORACLE
Cloud

Larger companies appear more capable of handling the amount of data generated by each task.

Data generated by routine tasks are considered the most commonly manageable, but capability drops with company size when data is derived from third-party needs or newer technologies.

%
- Employee records
- Financial reports
- System logs
- Service usage data
- Customer data
- Social conversation data
- IoT and other sensor data
- Third-party data

Within your organisation, how manageable is the amount of data generated by the following? – Completely manageable

Small
100 to 499 employees

Employee records	Financial reports	System logs	Service usage data	Customer data	Social conversation data	IoT and other sensor data	Third-party data
44	40	35	35	34	30	29	28

Medium
500 to 999 employees

Employee records	Financial reports	System logs	Service usage data	Customer data	Social conversation data	IoT and other sensor data	Third-party data
44	43	39	39	39	36	35	32

Large
1,000 to 49,999 employees

Employee records	Financial reports	System logs	Service usage data	Customer data	Social conversation data	IoT and other sensor data	Third-party data
50	49	45	43	44	38	37	35

Very large
50,000+ employees

Employee records	Financial reports	System logs	Service usage data	Customer data	Social conversation data	IoT and other sensor data	Third-party data
49	46	44	43	45	41	42	40

Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

Critically who is accountable? Nearly half of finance and IT decision makers say they're accountable for securing data within their organisation, **but those who execute on data – marketing and HR – are taking less accountability**.

What role does your department have in securing the data within your organisation?

%
- ■ We are accountable (we are in charge)
- ■ We are responsible (we do the work)
- ■ We are consulted (we are asked for input)
- ■ We are informed (we are kept up-to-date)
- ■ No role at all

Total
- 45
- 34
- 12
- 7
- 2

Marketing
- 34
- 41
- 14
- 8
- 2

HR
- 35
- 36
- 16
- 9
- 3

IT
- 52
- 34
- 9
- 4
- 1

Finance
- 47
- 31
- 13
- 8
- 2

Base: Global population, 24 markets, nr. 5,539

ORACLE
Cloud

Try Oracle Cloud today 13

When prompted to consider specific actions, **more respondents across all lines of business believe they are accountable** – especially IT.

Which of the following is your department held accountable or responsible for?

%	Accountable	Responsible
IT		
Finance		
Marketing		
HR		

Sharing data responsibility
- 67 / 46
- 56 / 44
- 56 / 47
- 59 / 48

Accessing data with proper privileges
- 67 / 46
- 56 / 45
- 54 / 49
- 62 / 43

Archiving data in respect of policies
- 66 / 47
- 58 / 44
- 54 / 47
- 60 / 46

Transferring and using data on trusted devices
- 65 / 47
- 54 / 46
- 57 / 46
- 59 / 47

Preserving data integrity
- 67 / 47
- 57 / 43
- 57 / 46
- 61 / 42

Enforcing the company security posture
- 65 / 48
- 58 / 42
- 52 / 50
- 61 / 45

Base: Global population, 24 markets, nr. 5,539

ORACLE Cloud

Data management – Analysis

Data as the new currency

The increasing pace of the move to the cloud means that organisations have more sophisticated systems in place to help them to better manage, and utilise, their data than in the past.

If data truly is the new currency – then how well are organisations protecting their future wealth? We asked respondents how confident they were in the security of data that their organisation holds. Industry best practices should be the minimum in this respect. However, despite these systems, less than 50% across all business sizes and all forms of data collected find data to be completely manageable. If we look at third-party data across medium-sized companies, this figure falls to 28%.
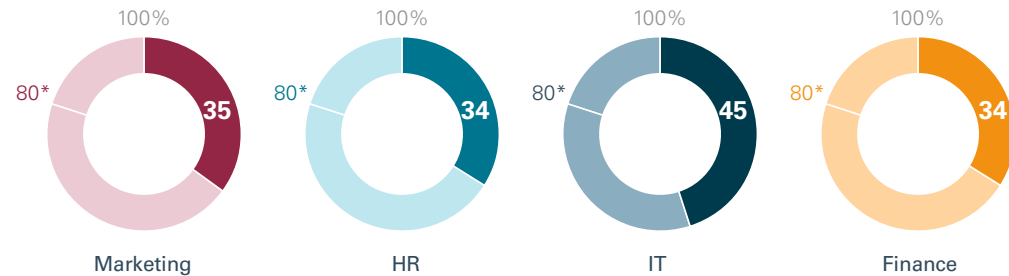
The source of the issue?

Only 30% to 41% of marketing leaders, across various sources of data, believe that data is highly manageable. Additionally, when it comes to the management of customer data and third-party data, the trust within marketing teams is low. This gives an indication that there are still issues with managing, controlling or utilising data in a timely manner.
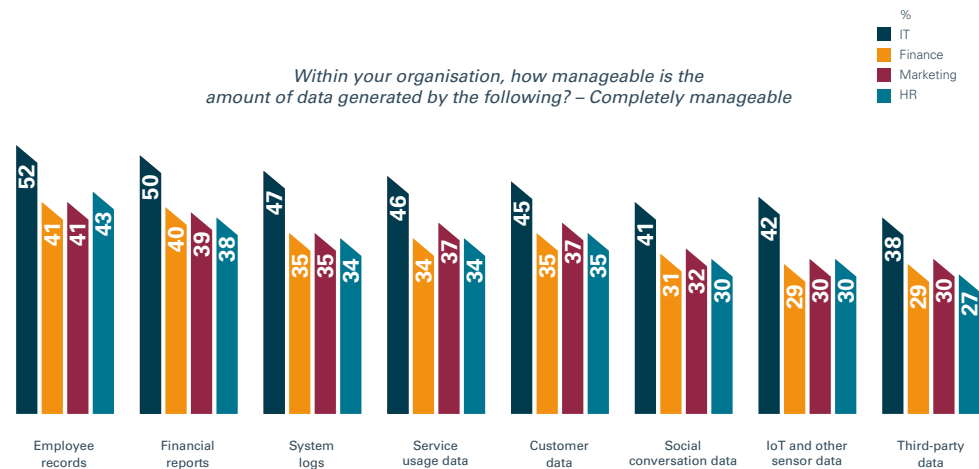
This means, at best, half of the value this data could offer goes untapped. While IT is ahead in this respect, no line of business excels or feels highly capable. This challenge spans the entire organisation.

If organisations want to find opportunities for competitive advantage then managing, integrating and interrogating these data sources should offer new opportunities to better understand their customers, markets, employees and supply chains, and provide a source of confidence for the future. For many organisations this appears a long way off at the moment.

Within your organisation, how manageable is the amount of data generated? – Completely manageable

Marketing	HR	IT	Finance
35	34	45	34

Within your organisation, how manageable is the amount of data generated by the following? – Completely manageable

%
- IT
- Finance
- Marketing
- HR

	IT	Finance	Marketing	HR
Employee records	52	41	41	43
Financial reports	50	40	39	38
System logs	47	35	35	34
Service usage data	46	34	37	34
Customer data	45	35	37	35
Social conversation data	41	31	32	30
IoT and other sensor data	42	29	30	30
Third-party data	38	29	30	27

Data management – Analysis (cont.)

It all starts with being accountable

When it comes to essential tasks such as 'enforcing the company security protocols' or 'preserving data integrity,' the research shows a relatively even split between those who take responsibility for these actions and those who accept overall accountability.

The management of data can be divided into three main functions: data security, data quality and data usage. Historically, the former has been IT's responsibility, and the latter the role of the data user. Data quality has often been a grey area.
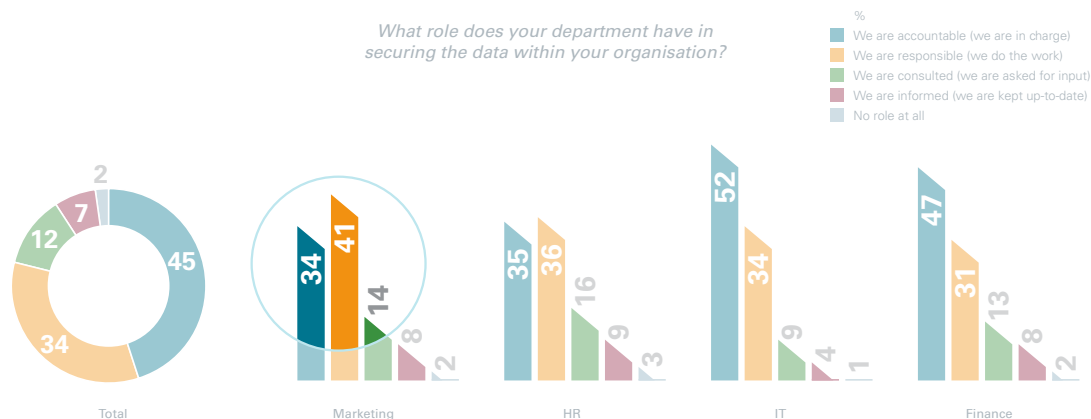
However, with the advent of the cloud, the importance of data to business success, combined with new regulations, means that more accountability for security, quality and usage needs to be accepted across all lines of business.

That's why the percentage of respondents who consider themselves accountable for data security is concerning. IT and finance hold themselves more accountable than other lines of business, however this is to be expected given their historical role in this space; as such it is surprising that their perceived accountability is not higher.

Additionally, we cannot forget that it is marketing and HR who hold the people data and are responsible for the customer experience; they therefore need to be accountable.
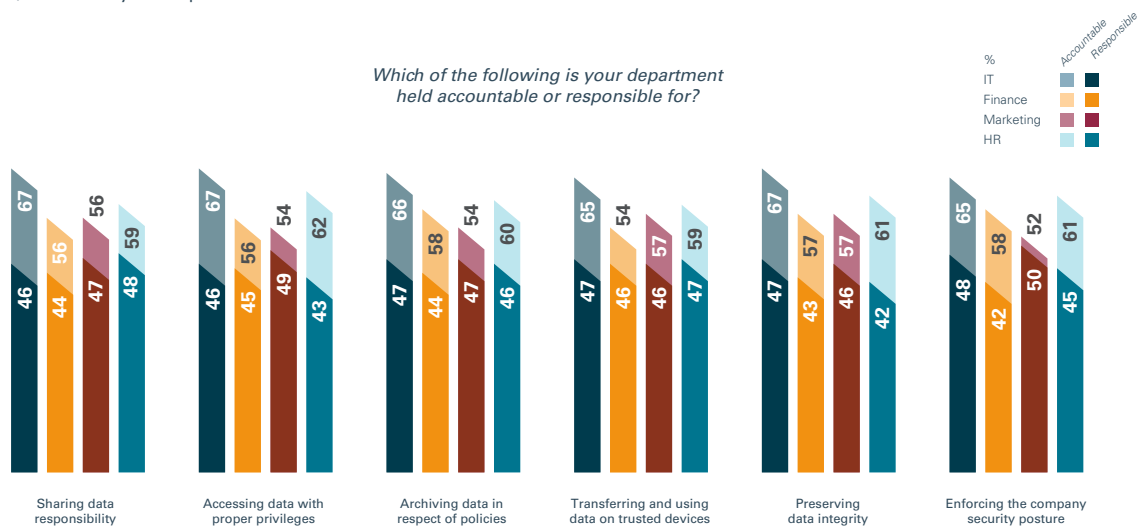
The data shows that marketing and HR do not understand how their roles are changing and that accountability, as well as responsibility, must shift. The old mindset has been 'we use the data, but IT owns it.' This is no more; and yet organisations are struggling to keep up.

What role does your department have in securing the data within your organisation?

%
- We are accountable (we are in charge)
- We are responsible (we do the work)
- We are consulted (we are asked for input)
- We are informed (we are kept up-to-date)
- No role at all

45% of respondents feel they are accountable for data integrity – one of the lowest scores for questions on responsible use. This suggests that inter-department strategy and protocols, with usage both driven and supported by ethics, insights and education, are not yet in place.

Which of the following is your department held accountable or responsible for?

%
	Accountable	Responsible
IT		
Finance		
Marketing		
HR		

Try Oracle Cloud today

Only 41% of marketing teams are 'highly confident' in the security of their organisation's data.

How confident are you in the security of the data your organisation holds? – Highly confident

* Reasonable expectation estimated at 80% or higher

100%
80*
41
Marketing

100%
80*
35
HR

100%
80*
47
IT

100%
80*
43
Finance

Base: Global population, 24 markets, nr. 5,539

ORACLE
Cloud

Try Oracle Cloud today   17

Looking at the cause of this lack of confidence – how well are best practices being adopted? Less than half of business leaders believe these are being implemented. They're more frequently implemented by IT, whilst **marketing are 10% points or more behind**.

To what extent are the following actions implemented regarding internal protocols within your organisation? – Always

%
- IT
- Finance
- Marketing
- HR

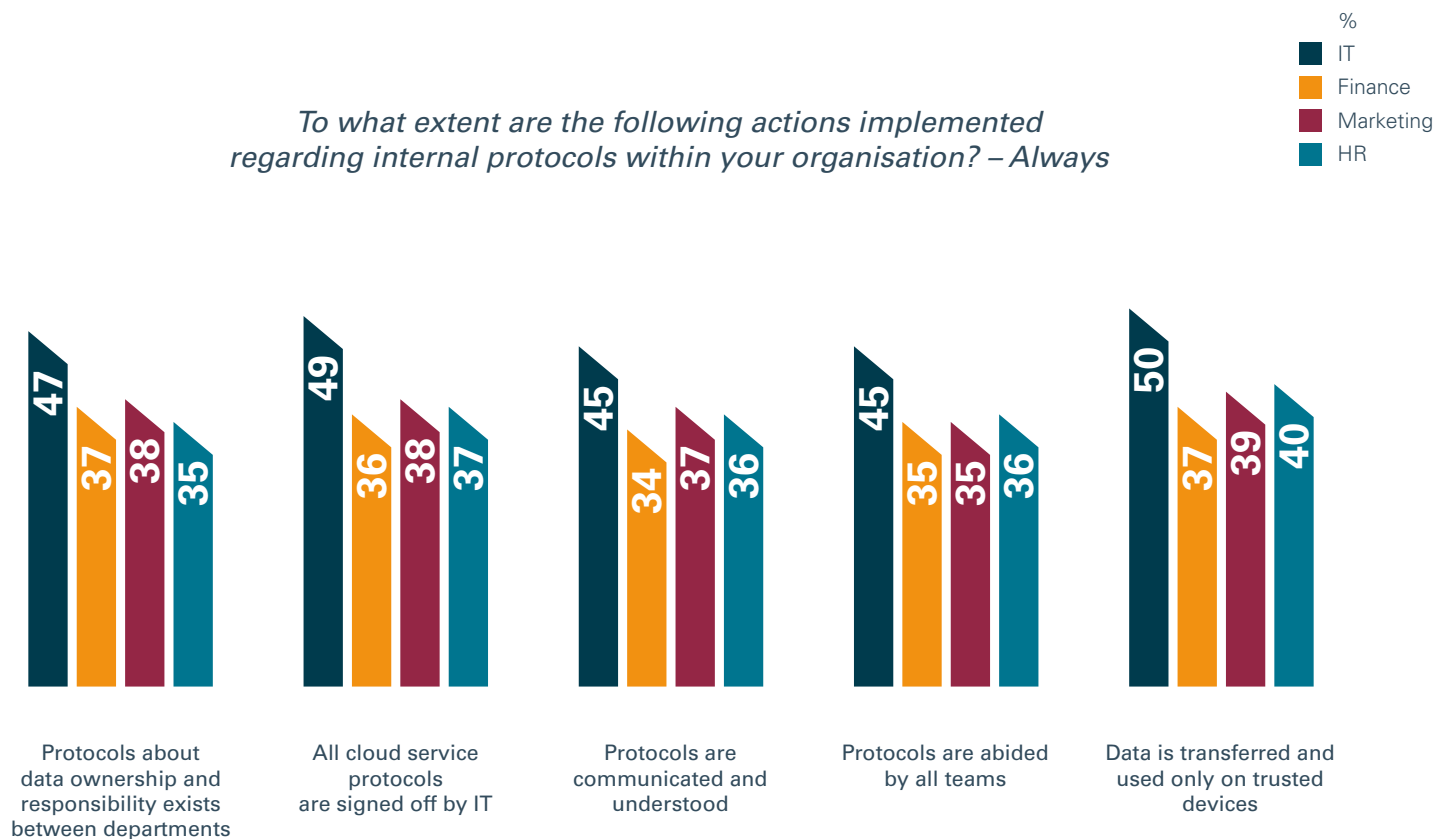|	Protocols about data ownership and responsibility exists between departments	All cloud service protocols are signed off by IT	Protocols are communicated and understood	Protocols are abided by all teams	Data is transferred and used only on trusted devices
IT	47	49	45	45	50
Finance	37	36	34	35	37
Marketing	38	38	37	35	39
HR	35	37	36	36	40

Base: Global population, 24 markets, nr. 5,539

ORACLE
Cloud

Try Oracle Cloud today 18

So what keeps us awake at night? The use of both mobile/social platforms and untrusted devices, as well as weak control on who can access data, are the **top internal behaviours that compromise trust**.

Please identify the top behaviours by internal departments and then external vendors that compromise your trust in how they manage data.

%
■ Internal departments
■ External providers/vendors

| 29 | 23 | 25 | 21 | 27 | 20 | 26 | 25 | 24 | 23 | 23 | 24 | 21 | 21 | 21 | 22 |

Willingness to manage data through mobile devices or social platforms

Low attention to data confidentiality

Use of untrusted devices/connections in data management

Weak control on who can access data

Blindness on how data is supposed to be used

Misuse of critical data

Disregard for applicable data regulations

Failure to enforce company security policies

Base: Marketing population, 24 markets, nr. 630

ORACLE
Cloud

Try Oracle Cloud today   19

Data management – Analysis

Security confidence

If data management practices are not optimal, then it is perhaps not surprising that confidence in security is also far below the required levels. As is the case with the ability to manage data, the bar should be set high in this respect. However, only 41% of marketing leaders, and less than half, (43%) of overall respondents can attest to being highly confident. Of more concern is the fact that one in four respondents are not confident at all. With data becoming the lifeblood of businesses today, this confidence gap is disconcerting at best, particularly when the lowest two respondents – HR and marketing – are the ones who hold the audience data.
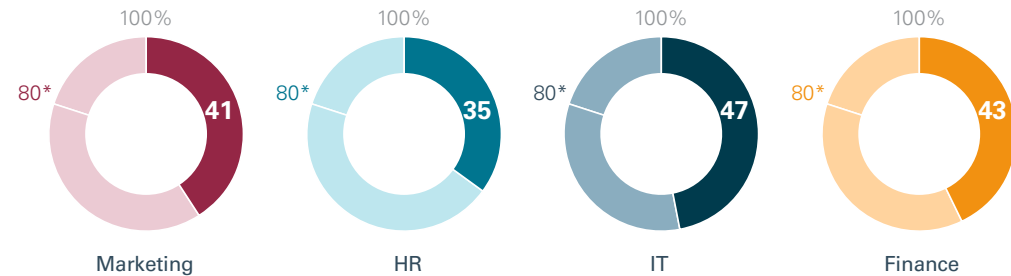
It's a team game

Why aren't respondents feeling more confident in the security of their data? We suggest this relates, at least in part, to internal protocols – or the lack thereof – implemented within the organisation. The findings point to this; less than half of respondents believe that critical actions are being fully implemented within their organisations.
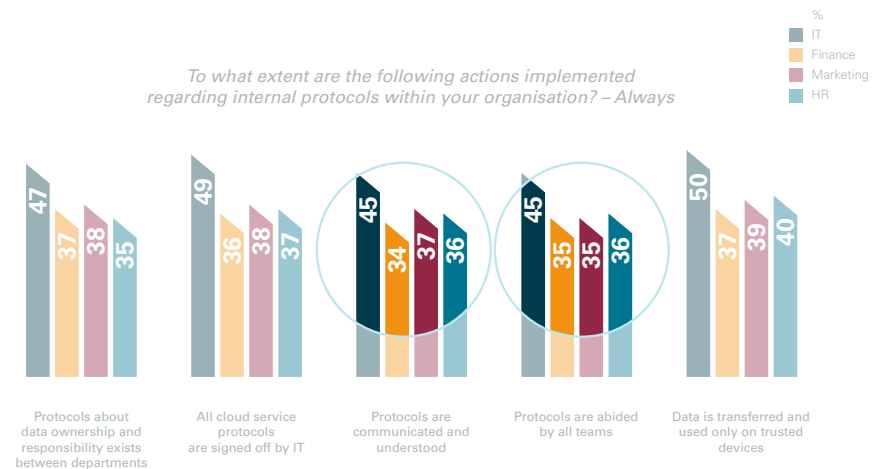
While it is certainly positive that all departments are now attempting to put some protocols in place, there is still much progress to be made. For example, only 37% of marketing leaders believe that protocols are communicated and understood by their teams, and only 35% believe these protocols are abided by. Given these findings, it is no surprise that marketing leaders are not highly confident in the security of their data.

19% of total decision makers state that protocols are abided by sometimes, rarely, or never. Such findings prove that organisations are currently open to threat due to the identified practices of their own people.

How confident are you in the security of the data your organisation holds? – Highly confident

100%	100%	100%	100%
80*	80*	80*	80*
41	**35**	**47**	**43**
Marketing	HR	IT	Finance

To what extent are the following actions implemented regarding internal protocols within your organisation? – Always

%
■ IT
■ Finance
■ Marketing
■ HR

Protocols about data ownership and responsibility exists between departments	All cloud service protocols are signed off by IT	Protocols are communicated and understood	Protocols are abided by all teams	Data is transferred and used only on trusted devices
47 37 38 35	49 36 38 37	45 34 37 36	45 35 35 36	50 37 39 40

ORACLE®
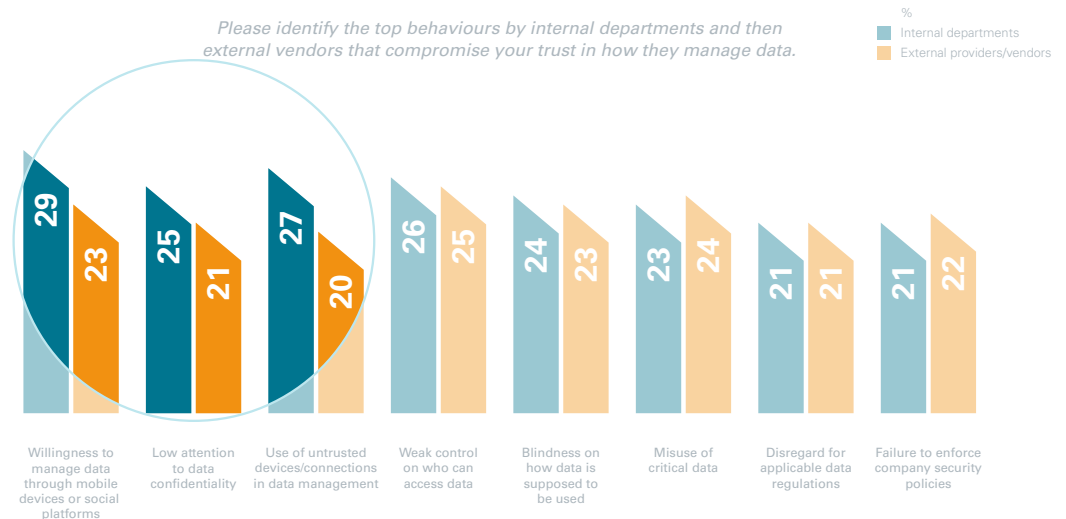Cloud

Data management – Analysis (cont.)

The pain points

Looking at internal departments, nearly one-third say that the biggest concern around data security across the organisation is a 'Willingness to manage data through mobile devices or social platforms' (29%), 'Low attention to data confidentiality' (25%), and 'Use of untrusted devices and connections' (27%).

Add to this, nearly one-quarter of respondents say that top behaviours compromising their trust in how data is managed include 'Blindness on how data is supposed to be used' and the 'Misuse of critical data'. While these latter findings could be put down to a general lack of insight and understanding into how data is truly managed, approximately one-quarter of respondents are concerned about the 'Disregard for applicable data regulations' and 'Failure to enforce company security policies.'

IT is well ahead of marketing and all other lines of business when it comes to enforcing such protocols. This is to be expected as, historically, IT would be charged to put protocols in place. For other departments however, everyday business and short-term targets can override the perceived priority of protocols. Therefore, IT understandably believes that there are protocols, and all lines of business should be enforcing them.

Please identify the top behaviours by internal departments and then external vendors that compromise your trust in how they manage data.

%
■ Internal departments
■ External providers/vendors

Behaviour	Internal departments	External providers/vendors
Willingness to manage data through mobile devices or social platforms	29	23
Low attention to data confidentiality	25	21
Use of untrusted devices/connections in data management	27	20
Weak control on who can access data	26	25
Blindness on how data is supposed to be used	24	23
Misuse of critical data	23	24
Disregard for applicable data regulations	21	21
Failure to enforce company security policies	21	22

ORACLE
Cloud

Data management – Summary

All marketing departments now have data. As a result, the base competency is going up. And yet, what is considered to be 'good' in execution is not yet within reach.

- **Quantity over quality:** The sheer volume of data across multiple sources, and bringing them together in a meaningful way, remains a challenge for marketers. They need coherent findings and insights at the sweet spot in time with data that is joined up. In an ideal world, data around awareness creation and lead creation would point to opportunity. But we are a long way from this; marketing leaders are operating with a lot of data without a coherent presentation of it.

- **Responsible use and management of data are key elements of a digital economy:** CMOs need the support of CIOs to effectively monitor and manage digital use, and thus manage risk. However, if organisations truly want marketing leaders to take full accountability and responsibility for data security, they need to offer both time and resources. It is only then that marketing decision makers can drive innovation with emerging technologies underpinned by data security and trust.

- **Confidence in the security of data is low and not expected to increase.** Given the exponential growth of data, this raises the question as to how organisations can scale whilst maintaining desirable security levels. Marketers appear largely unaware that AI can deliver the analysis and recommendations that they need. This fact applies as much to B2B as it does to B2C; we all want the same experience realtime, highly personalised experience.

- **Good data management practice requires basic protocols to reduce uncertainty** and make it manageable, and 'managed.' Admittedly, data strategies are somewhat new; protocols therefore need to catch up with the new reality and be enforced within all lines of business. The concept is that a common protocol should be running across the business, but at the moment it is clearly not being embedded or embraced.
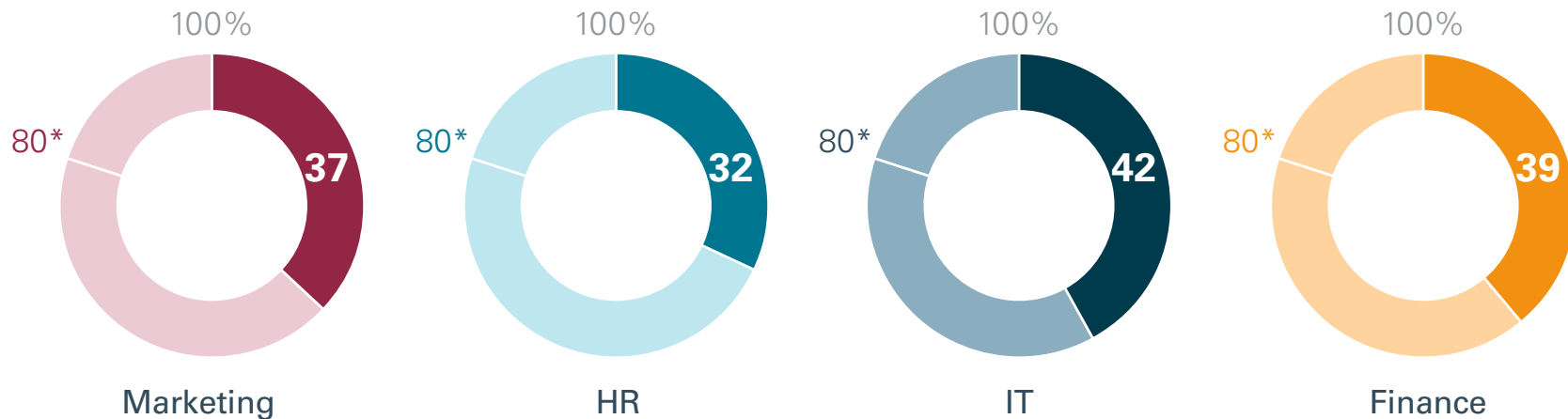
ORACLE
Cloud

Insights

Using data to its maximum potential

Only 37% of marketing leaders are highly confident that their organisation's ability to manage data to generate meaningful insights. IT and finance have the strongest confidence in their organisation's ability to manage data to achieve greater insights. More than 50% are are less confident or not confident at all.

Based on the last six months, how confident are you that your organisation is managing the deluge of data to generate meaningful insights? – Highly confident

100%	100%	100%	100%
80*	80*	80*	80*
37	**32**	**42**	**39**
Marketing	HR	IT	Finance

* Reasonable expectation estimated at 80% or higher

Base: Global population, 24 markets, nr. 5,539

ORACLE®
Cloud

Only 37% of marketing leaders are highly confident in their organisation's ability to manage data to generate meaningful insights.

Delivering competitive advantage through data trust requires the combination of quality customer and prospect insights in realtime. This in turn drives productivity of the marketing function by providing greater customisation, innovation and agility while offering an undoubted advantage to gain, retain and cross-sell.

However, our CMOs continue to struggle with challenges for both data quality and execution:
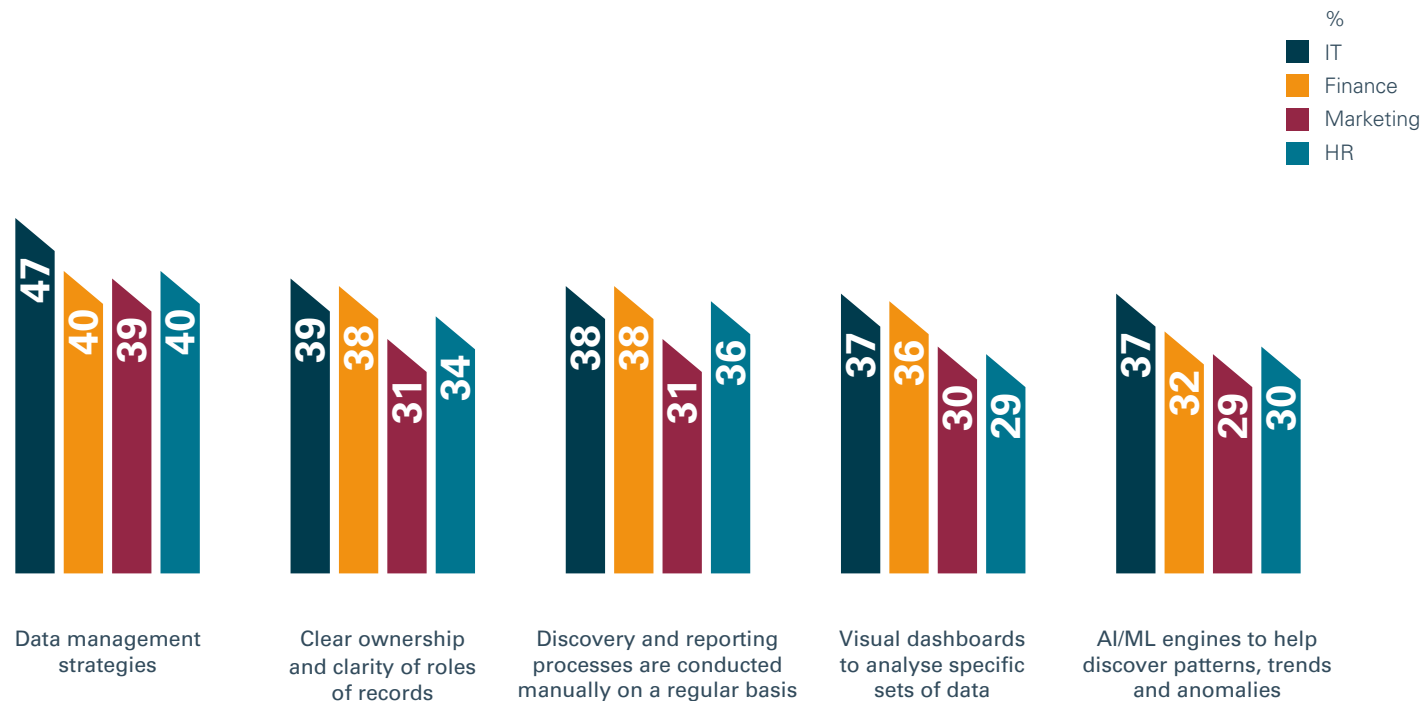
- **How to ensure the data used is of sufficient quality for the best chance of success**
- **How to ensure they are targeting the right audiences**
- **How to personalise experiences with relevant content**
- **How to track and analyse lead profile and behavioural information**
- **How to run multiple lead scoring models or best manage lead scoring**

CMOs need to be reminded of their priority to extract trustworthy insights and value from their data. They must also keep in mind that AI/ML can have a massive impact on personalised, cross-channel communications. Data is the new currency for most, if not all, organisations. Those not able to obtain the maximum value of their data will fall behind. Therefore, the focus must be on automation and speed in enabling the business to leverage technology, machine learning, AI and automation to empower organisations with the insights this data brings.

When considering the findings, we recognise that marketing may be responding to new legislation, which impacts their confidence levels. However, we argue that regulation such as GDPR should not be required to encourage and inform organisations on how to manage data properly; this should be an organisation mindset. Initiatives like GDPR or other regulatory compliance policies should merely serve as great examples of how to drive the responsible usage of data.

Across all departments, putting in place **a data management strategy is the greatest priority**, but this is still not commonplace. IT lead the way on enabling insights, marketing and HR in particular need to catch up with their capabilities in this area.

What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?

%
- IT
- Finance
- Marketing
- HR

	IT	Finance	Marketing	HR
Data management strategies	47	40	39	40
Clear ownership and clarity of roles of records	39	38	31	34
Discovery and reporting processes are conducted manually on a regular basis	38	38	31	36
Visual dashboards to analyse specific sets of data	37	36	30	29
AI/ML engines to help discover patterns, trends and anomalies	37	32	29	30

Base: Global population, 24 markets, nr. 5,539

ORACLE Cloud

Organisations of all sizes are putting strategies in place to improve data management, **but taking key actions lessens with company size**.

Size of organisation

- Small: 100 to 499 employees %
- Medium: 500 to 999 employees %
- Large: 1000 to 49,999 employees %
- Very large: 50,000+ employees %

What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?

	Small	Medium	Large	Very large
Data management strategies	42	43	46	43
Clear ownership and clarity of roles of records	35	36	39	38
Discovery and reporting processes are conducted manually on a regular basis	34	34	38	40
Visual dashboards to analyse specific sets of data	29	33	37	39
AI/ML engines to help discover patterns, trends and anomalies	28	32	36	42

Base: Global population, 24 markets, nr. 5,539

ORACLE Cloud

Education is key (for both security teams and employees) **and so training is the preferred route for teaching employees to use data responsibly**.
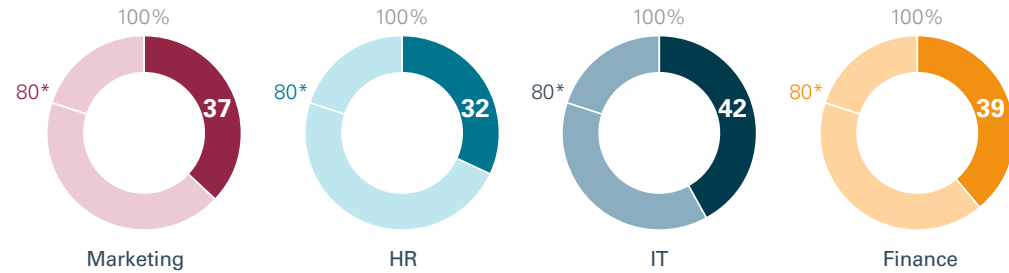
Which initiatives does your organisation take in teaching people to use data responsibly?

%
- ■ IT
- ■ Finance
- ■ Marketing
- ■ HR

	IT	Finance	Marketing	HR
Training security teams on new threat types and best practices	43	38	36	40
Regular employee training on both new and old threats	41	40	38	38
Online learnings for record management and data quality processes	39	38	34	34
Security workshops mixing together people from different lines of business	40	34	31	33
Hands-on labs about secure usage of devices and connections	35	34	30	31
Creative incentives to promote best practices on security	34	30	31	31

Base: Global population, 24 markets, nr. 5,539

ORACLE
Cloud

Try Oracle Cloud today 28

Seeing the value

Only 37% of marketing leaders are highly confident in their organisation's ability to manage data to generate meaningful insights. IT and finance have the strongest confidence in their organisation's ability to manage data to achieve greater insights. Over one in five are less confident or not confident at all.

Based on the last six months, how confident are you that your organisation is managing the deluge of data to generate meaningful insights? – Highly confident

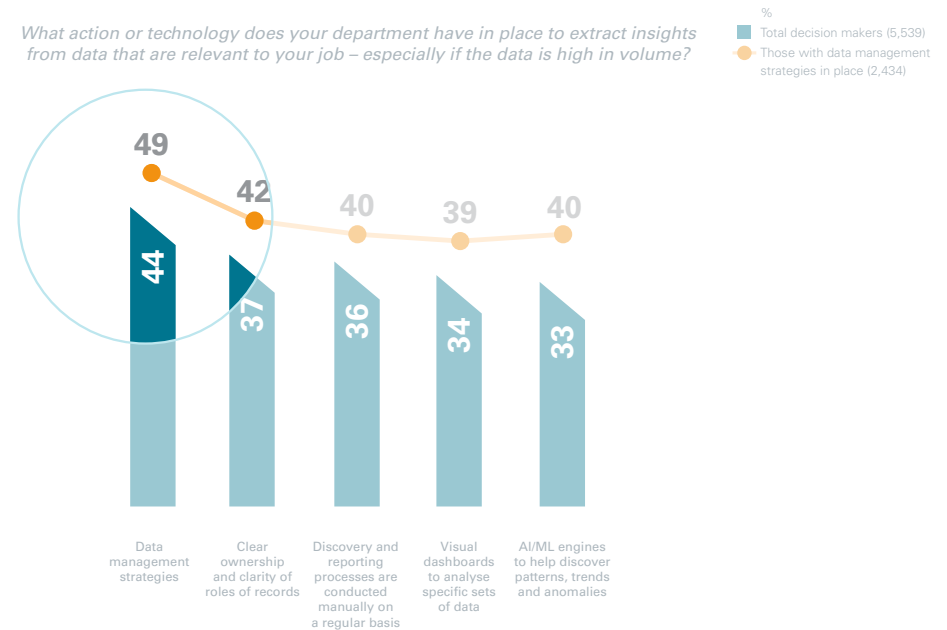Marketing 37 · HR 32 · IT 42 · Finance 39

Accountability also leads to stronger data strategies

A deeper dive into the results shows that those who believe they are accountable are more likely to then put data management strategies in place.

Of the four lines of business, IT and finance come ahead with respect to data management strategies. This is not surprising, but this transfer of responsibility should now be moving through other departments. Marketing teams are less likely to have data management strategies.
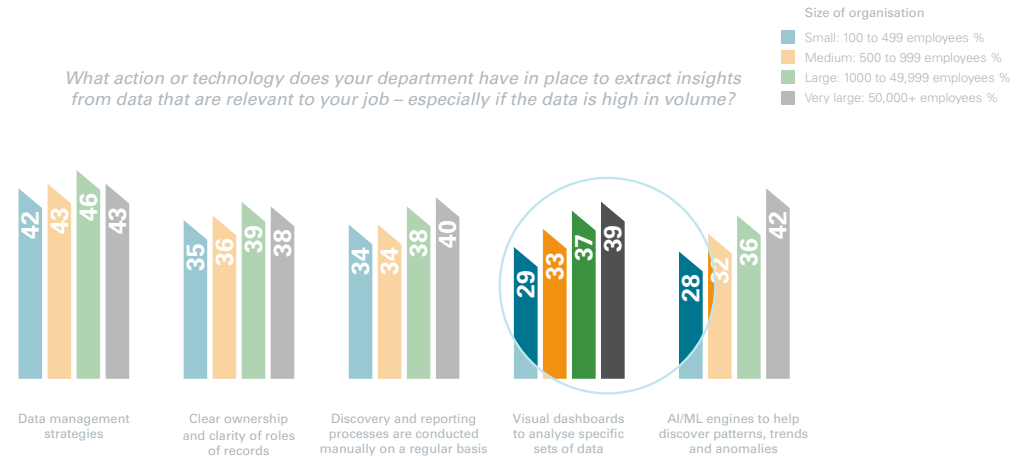
The evidence is clear – taking ownership of these issues starts with taking accountability.

What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?

%
Total decision makers (5,539)
Those with data management strategies in place (2,434)

44 · 37 · 36 · 34 · 33 (bars); 49 · 42 · 40 · 39 · 40 (line)

Data management strategies | Clear ownership and clarity of roles of records | Discovery and reporting processes are conducted manually on a regular basis | Visual dashboards to analyse specific sets of data | AI/ML engines to help discover patterns, trends and anomalies

Insights – Analysis (cont.)

Who can see the value most?

Smaller organisations are struggling the most to extract insights out of the data. However, larger organisations are not faring as well as we'd expect, likely due to the quantity of data they must deal with. These findings remind us that mass data is not quality data. The ability to draw insights is what matters.
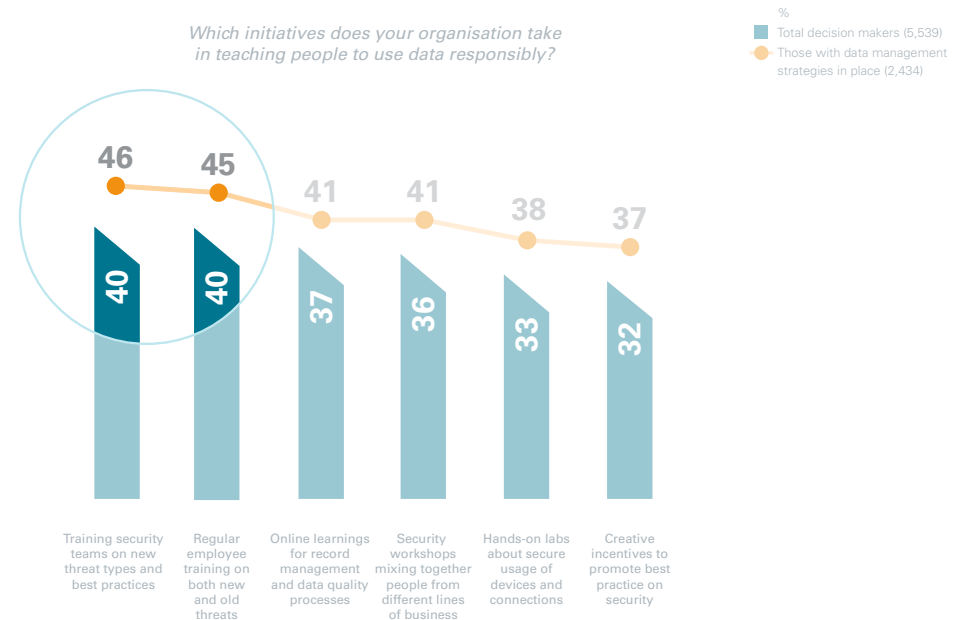
Education for all

Those who state they are accountable for securing their organisation's data are more likely to implement employee education and training on security threats. This is critical to ensuring greater adherence to security protocols.

Over half of organisations state that they do not train their employees in any fashion when it comes to the responsible use of data.

Whether this training relates to new threat types and best practices, or hands-on labs about the secure usage of devices and connections, there is a clear gap in education.

It is no wonder then that teams suffer from a lack of high confidence and do not complete the necessary tasks to keep data safe.

Their training on the responsible use of data is not a sufficiently high priority and they are not being incentivised to promote best practices.

What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?

Size of organisation
- Small: 100 to 499 employees %
- Medium: 500 to 999 employees %
- Large: 1000 to 49,999 employees %
- Very large: 50,000+ employees %

	Small	Medium	Large	Very large
Data management strategies	42	43	46	43
Clear ownership and clarity of roles of records	35	36	39	38
Discovery and reporting processes are conducted manually on a regular basis	34	34	38	40
Visual dashboards to analyse specific sets of data	29	33	37	39
AI/ML engines to help discover patterns, trends and anomalies	28	32	36	42

Which initiatives does your organisation take in teaching people to use data responsibly?

%
- Total decision makers (5,539)
- Those with data management strategies in place (2,434)

	Total decision makers	Those with data management strategies in place
Training security teams on new threat types and best practices	40	46
Regular employee training on both new and old threats	40	45
Online learnings for record management and data quality processes	37	41
Security workshops mixing together people from different lines of business	36	41
Hands-on labs about secure usage of devices and connections	33	38
Creative incentives to promote best practice on security	32	37

ORACLE® Cloud

Best practices on the responsible use of data is a combination and balance of two critical elements: In the first instance, employee attitude and understanding needs to be developed through education. Marketing needs to support HR and IT in educating the wider organisation, so that it can take on board its own role in managing the risks around customer data.

In the second instance, security enabled by technology CMOs need to automate data as much as possible; otherwise, there is too much data for a human to compute and protect.

Marketing leaders face the strongest gap in confidence with respect to drawing meaningful insights from data. Given the requirement of analytics to drive the digital experience – this needs to be addressed. After all, it is essential to get insights that are timely, relevant and of quality.

An insight turns into understanding, and turns that data into something you can use to upsell and retain a customer. It ultimately leads to a highly personalised experience.

- **Relevant metrics are critical.** In the massively scaled and complex infrastructure that supports large digital businesses, traditional monitoring and problem-solving approaches are proving to be inadequate. The only viable solution is to apply analytics to the burgeoning volumes of data to find hidden insights that help keep infrastructure and applications running.

- **Ensure the data used by the business to measure performance is well-aligned.** As IT and other lines of business come together, empowering people to use data responsibly and training them on threats and data quality processes becomes more essential than ever. The increasing interest and focus are twofold: ethical data usage and data-driven business models.

- **Data is the thread that ties all the lines of business and IT functions together:** Data and technology need to work for organisations as an aid to decision making by decreasing risk and enabling better, more accurate and more confident decision making with a stronger human/machine partnership. Marketing leaders need to take accountability for their data. However, such data should be considered an aid to human decision making and not an alternative.

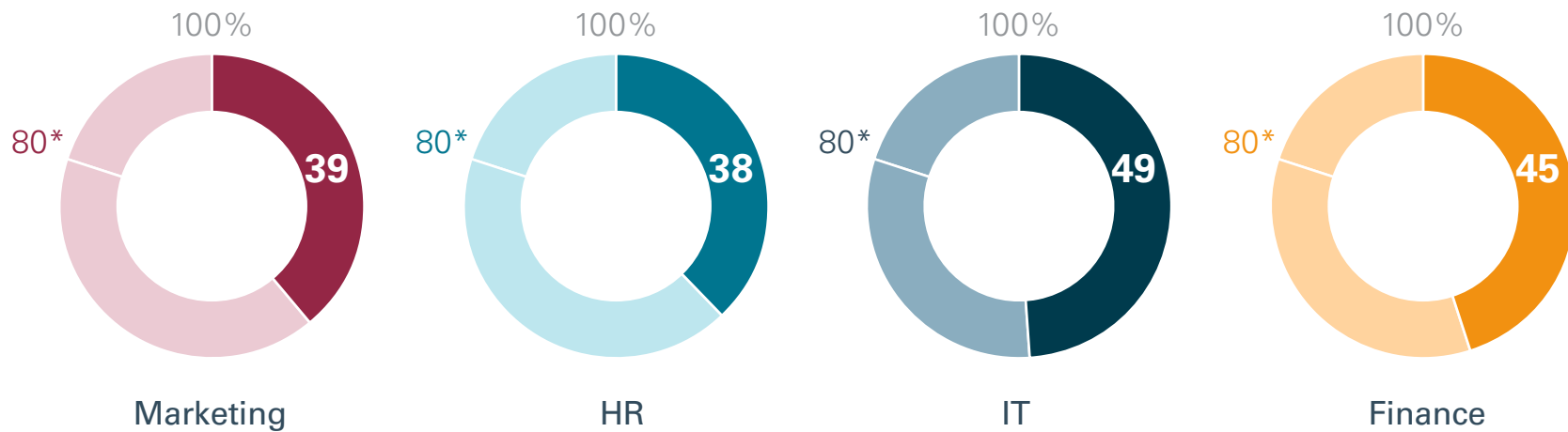# Ethics

The mindset to maintain trust

Across all lines of business, the minority say they are highly confident that the use of data in their organisation is ethical – **for marketers this falls to 39%**.

Based on the last six months, how confident are you that your organisation's use of data is ethical? – Highly confident

* Reasonable expectation estimated at 80% or higher

100%   100%   100%   100%

80* **39**   80* **38**   80* **49**   80* **45**

Marketing   HR   IT   Finance
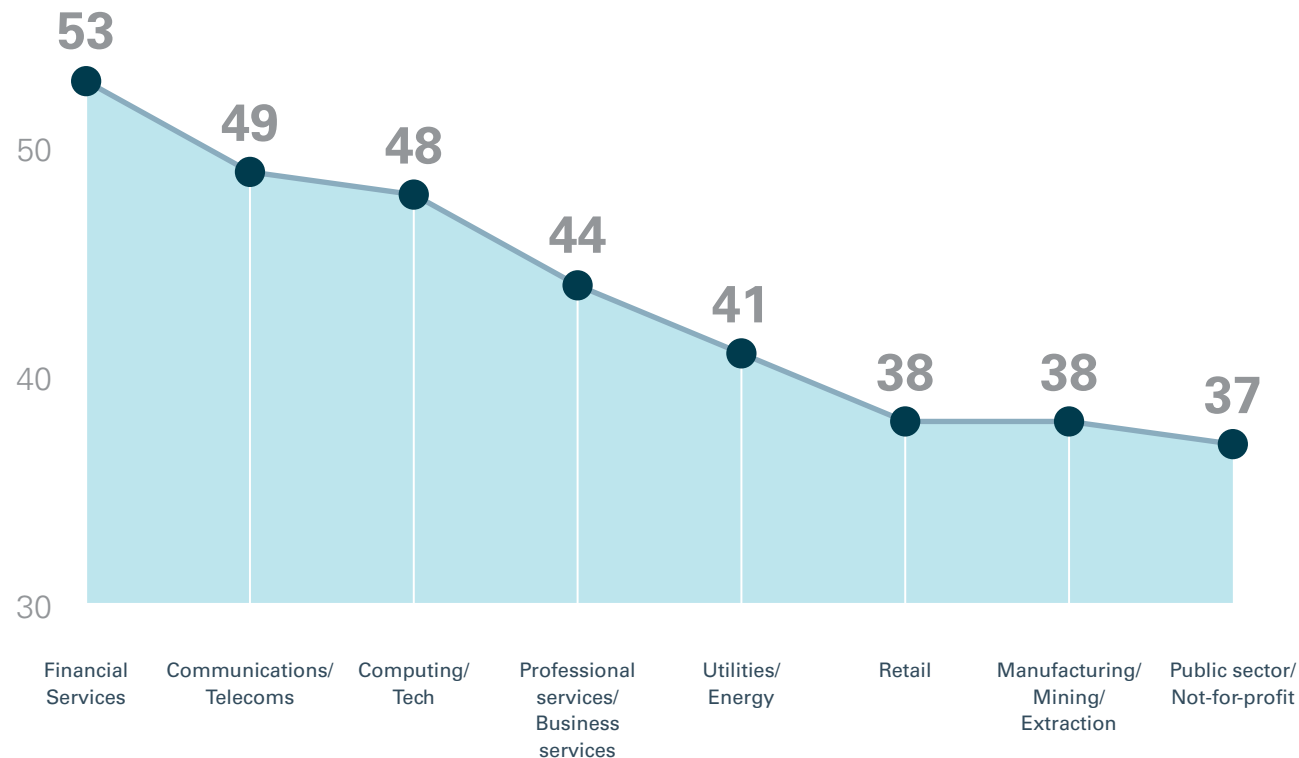
Base: Global population, 24 markets, nr. 5,539

An ethical mindset is a pre-requisite in today's digital and social economies. As organisations seek to generate maximum value from the deluge of customer, market and sales data, CMOs have a key role to play. They must ensure that this data is trustworthy and that it has been gained from clear, transparent, permission-based methods.

A key consideration for marketers is how to ensure that data is being used ethically whilst delivering the experiential programmes that customers are prioritising. Ethical usage of marketing data is strongly tied to customers' trust in the brand.

Indeed, even if you use data in a legal way – and of course customers should be able to assume this is always the case – your customers can still feel queasy if you demonstrate that you know too much about them. Keeping that balance right is crucial.

ORACLE
Cloud

Financial services have the most confidence that their organisation is using data ethically – for other industries, complete confidence is less than 50%. Has increased regulation improved process, or simply improved confidence levels?
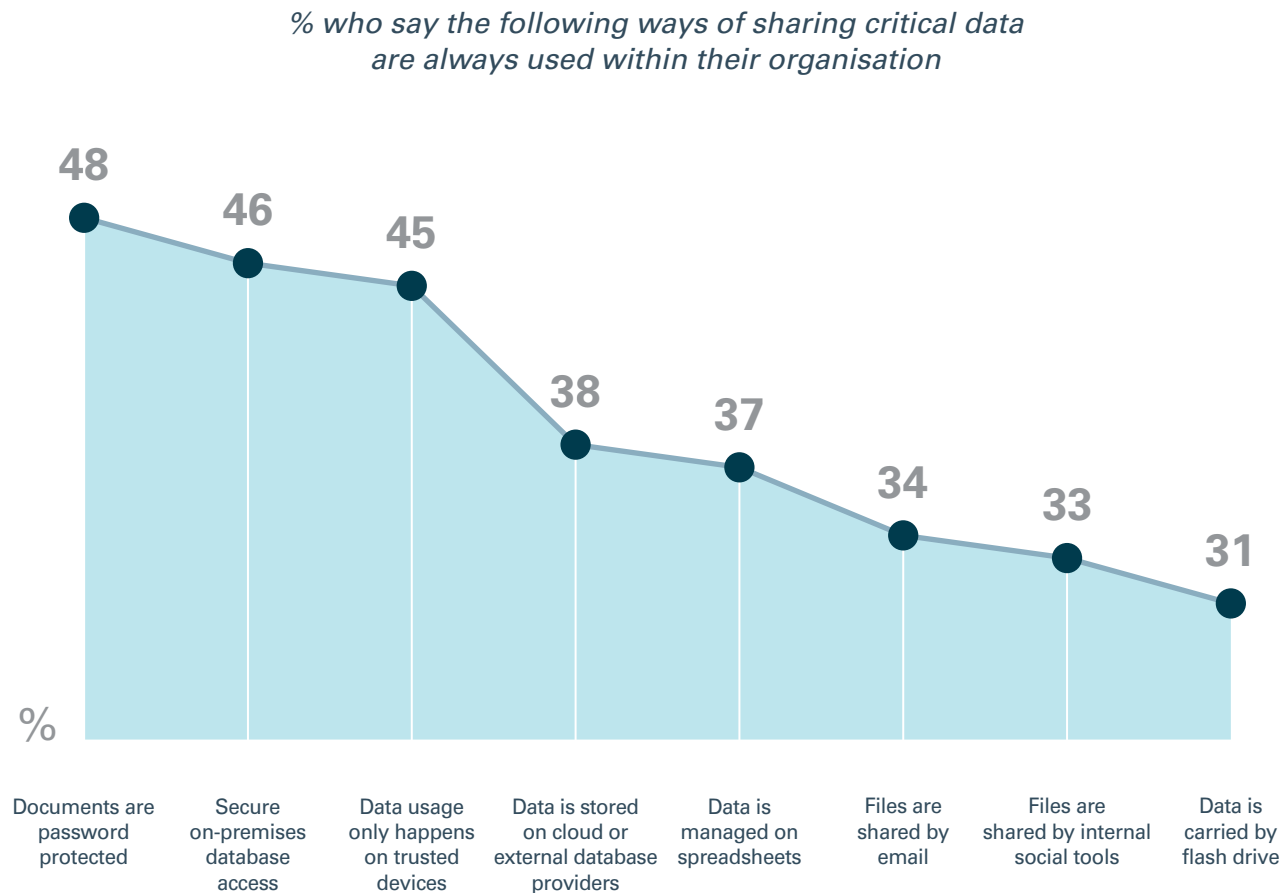
How confident are you that your organisation's use of
data is ethical, based on the last six months? – Highly confident

53 — Financial Services
49 — Communications/ Telecoms
48 — Computing/ Tech
44 — Professional services/ Business services
41 — Utilities/ Energy
38 — Retail
38 — Manufacturing/ Mining/ Extraction
37 — Public sector/ Not-for-profit

Base: Global population,
24 markets, nr. 5,539

ORACLE
Cloud

Try Oracle Cloud today   35

Good practice is improved with critical data and is most frequently shared via password protected documents and on-premises databases – **but this still needs more rigour**.

*% who say the following ways of sharing critical data
are always used within their organisation*

| 48 | 46 | 45 | 38 | 37 | 34 | 33 | 31 |

%

| Documents are password protected | Secure on-premises database access | Data usage only happens on trusted devices | Data is stored on cloud or external database providers | Data is managed on spreadsheets | Files are shared by email | Files are shared by internal social tools | Data is carried by flash drive |

Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

Ethics – Analysis

Putting ethics top of the agenda

We are facing a new generation of consumers with different behaviour and different expectations. The more we understand our customers the more we can meet those expectations and anticipate their needs.

Customer understanding comes hand in hand with the transparency and ethical usage of the customer data. Unfortunately, only 39% of marketing leaders are highly confident that their organisation's use of data is ethical. This is compared to the fact that only 45% of all respondents are highly confident in their organisation's ethical use of data. Just under one-fifth of respondents are not confident at all.
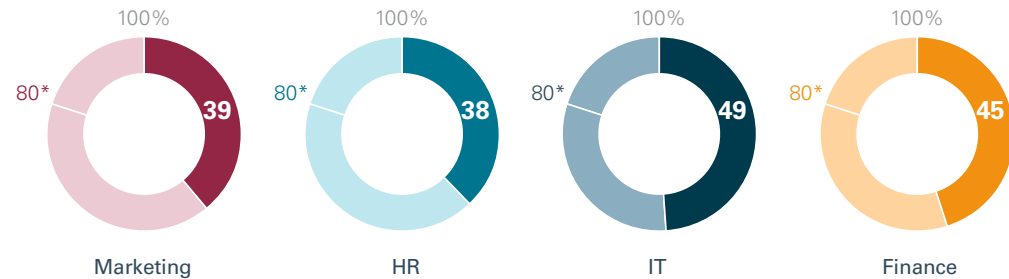
While the precise definition of 'ethical use' is complex, we had expected this percentage to be much higher. IT again scores highest (49%) – 10 percentage points above both marketing and HR departments.

This reveals that all departments recognise that data management practices are not as good as they could be within the organisations. It signifies that people are more aware of what unethical looks like and that their data management strategies need to pick up.
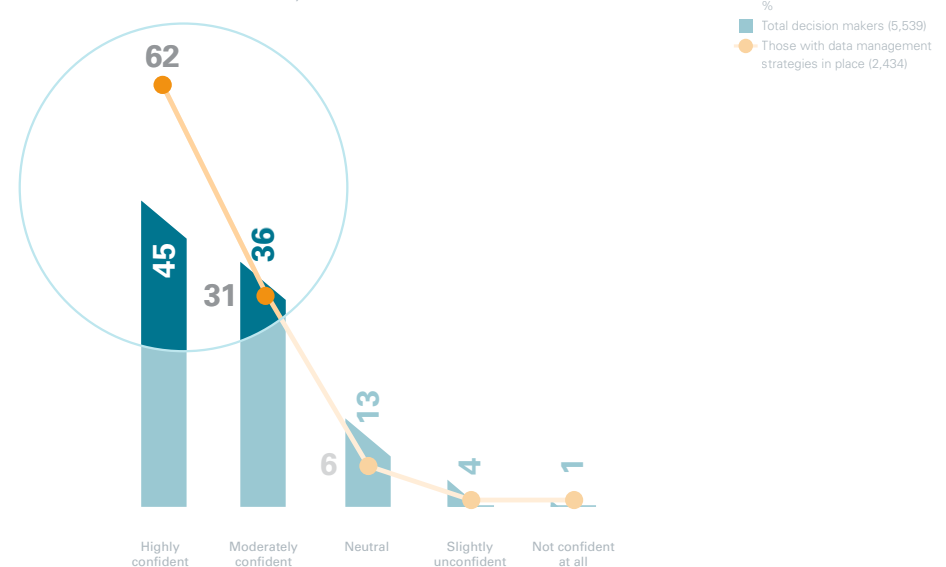
Stronger strategy improves confidence in ethics

Of those with data management strategies in place, 62% are highly confident that their organisation's use of data is ethical, compared to 45% across all respondents. And as we have already seen that data management strategies come from taking accountability for data… so we can conclude that ethical trust also starts with taking accountability.

Based on the last six months, how confident are you that your organisation's use of data is ethical? – Highly confident

Marketing	HR	IT	Finance
39	38	49	45

How confident are you that your organisation's use of data is ethical, based on the last six months?

%
- Total decision makers (5,539)
- Those with data management strategies in place (2,434)

Highly confident	Moderately confident	Neutral	Slightly unconfident	Not confident at all
45 / 62	31 / 36	6 / 13	4	1

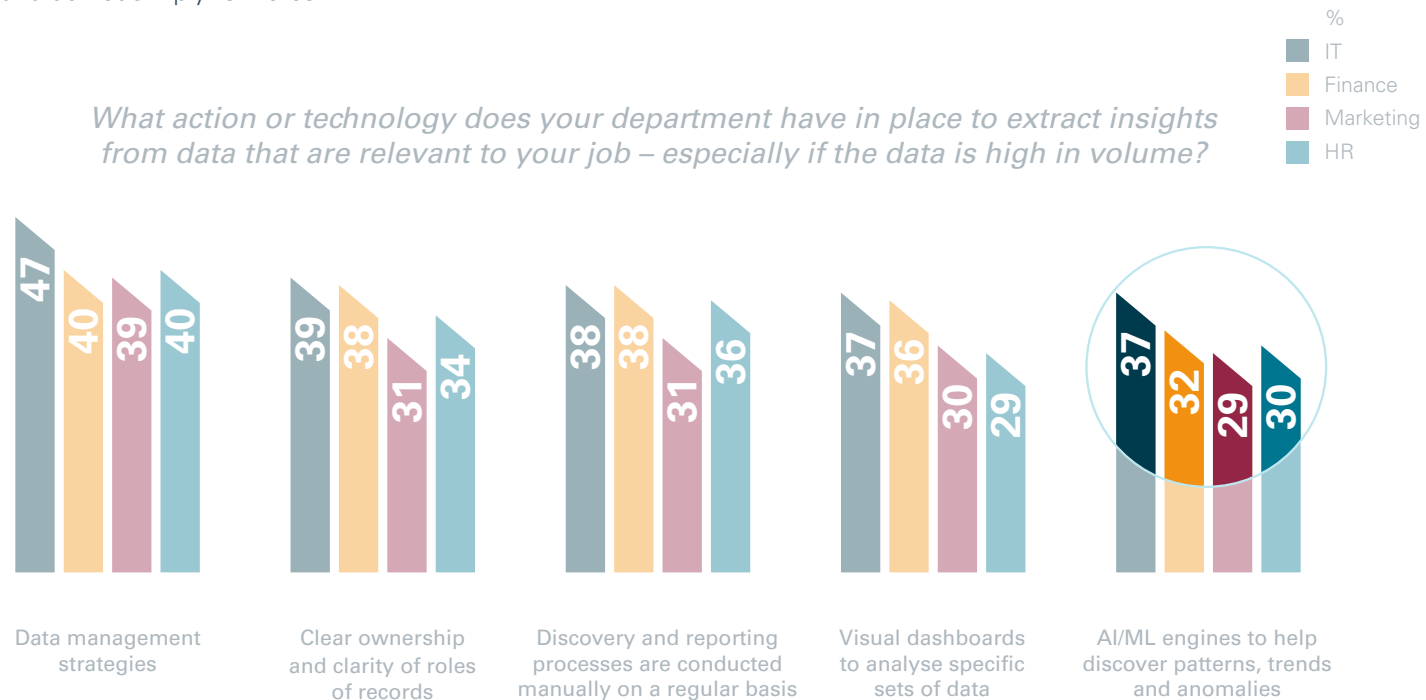ORACLE® Cloud

Ethics – Analysis (cont.)

Controlling unconscious bias

Although it is reassuring to see the progress being made in the use of intelligent technologies such as AI and ML, their use is still in its infancy, and often limited to pockets of innovation. Therefore, so are the controls on such technologies.

As their use grows, organisations will need to take greater control on monitoring the algorithms, data inputs, and analysis to ensure that they provide greater insight and understanding, and do not simply reinforce prior bias within data sets.

What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?

%
- IT
- Finance
- Marketing
- HR

	Data management strategies	Clear ownership and clarity of roles of records	Discovery and reporting processes are conducted manually on a regular basis	Visual dashboards to analyse specific sets of data	AI/ML engines to help discover patterns, trends and anomalies
IT	47	39	38	37	37
Finance	40	38	38	36	32
Marketing	39	31	31	30	29
HR	40	34	36	29	30

Sharing critical data

Those with data management strategies in place are 8% more likely to use password protected documents, 10% more likely to have access to secure on-premises databases, and 9% more likely to use data on trusted devices.

Organisations, and data handling functions within them, cannot afford to let short-term pressures dictate data management decisions that compromise ethical considerations.
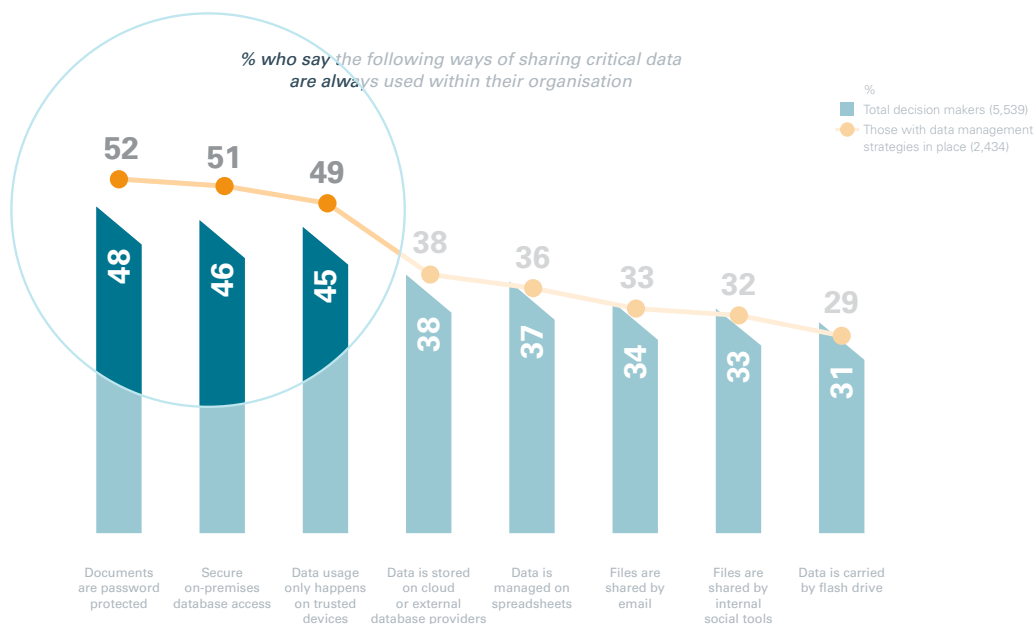
This is especially true when you bring in the many ways that organisations share data internally and externally across email, portable devices and other non-secure platforms and tools.

While half say that data is only shared on trusted devices, approximately a third say this data is shared across spreadsheets, email, internal social, and flash drives. There is directional positivity in the security practices respondents use, in that good practices are being demonstrated and improving, but there is much progress to be made.

The issue of ethical use, and whether best practices are abided brings us back to the topic of whether organisations have a data management strategy in place that is both managed and monitored.

The evidence shows that those with a data management strategy in place increase the prevalence of good practice – including password protection and use of trusted devices, and minimise areas of risk such as the transfer of data on memory sticks or other portable devices.

However, having a data management strategy in place is only part of the issue. Enabling line management and IT to monitor and police the implementation is critical to long-term success, and here again IT requires the infrastructure and platforms to implement robust monitoring, and minimising risks of exposure through bad practice that could lead to reputational damage.

% who say the following ways of sharing critical data are always used within their organisation

%
■ Total decision makers (5,539)
● Those with data management strategies in place (2,434)

	Documents are password protected	Secure on-premises database access	Data usage only happens on trusted devices	Data is stored on cloud or external database providers	Data is managed on spreadsheets	Files are shared by email	Files are shared by internal social tools	Data is carried by flash drive
Those with data management strategies	52	51	49	38	36	33	32	29
Total decision makers	48	46	45	38	37	34	33	31

ORACLE® Cloud

Ethics – Summary

The 3 factors to deliver *ethicality*:

- **Ethical behaviours originate from an ethical mindset;** this needs to start from the top of the organisation, where expectations are set and behaviours are demonstrated. Any organisation needs to believe that operating in an ethical and responsible manner will deliver business value – through trust and reputation both to internal and external audiences.

- **Good governance:** All lines of business need to work together to maximise the benefits of data; this means creating cross functional teams to develop ethical codes and common policies.

- **Adopt intelligent technology:** In today's mobile, multi-device and multi-channel world, digital intelligence offers the ability to transform digital data into realtime, actionable insights across the entire organisation.

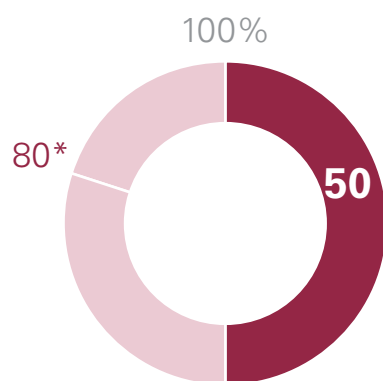**This all combines to deliver *ethicality*.**

Reputation

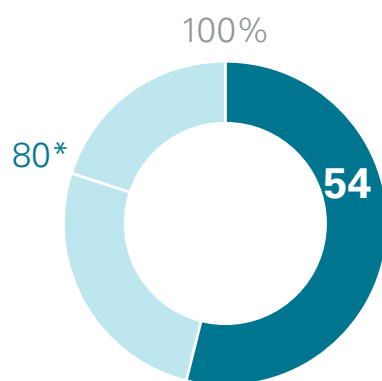Ensuring your organisation's reputation
is supported by data

50% of marketing leaders fully appreciate the importance of secure management of data to reputational risk.

How important is the secure management of data to the reputation of your organisation? – Very important
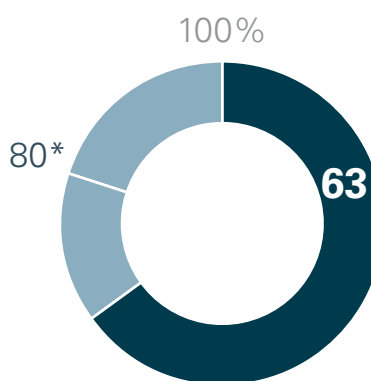
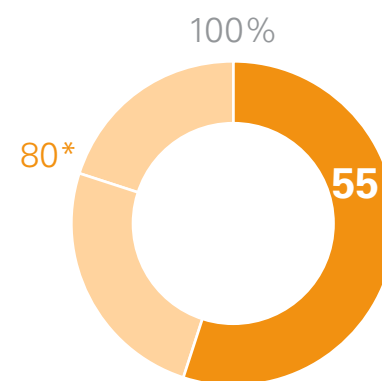** Reasonable expectation estimated at 80% or higher*

100%

80*

50

Marketing

100%

80*

54

HR

100%

80*

63

IT

100%

80*

55

Finance

Base: Global population, 24 markets, nr. 5,539

ORACLE Cloud

Try Oracle Cloud today   42

So with data management practices only just emerging, the demand for insight is far ahead of current capabilities, and the ethical mindset somewhat inconsistent. How do business leaders feel about the importance of secure management of data on their reputations?

It is more than concerning that only 55% of business leaders believe that the secure management of data is very important to reputational risk. With the pervasiveness of the threats, and the fact that one breach can cause significant damage to the brand, the importance of data management needs to be put at the top of any organisation's agenda.

Reputation – Secure management of data

Top three concerns

Protecting company reputation is a top concern across departments.
However, protecting personal identities is more prioritised among HR teams. Marketing leaders place equal value on reputation risk in front of the customer and compliance, but value respect for personal identity less.
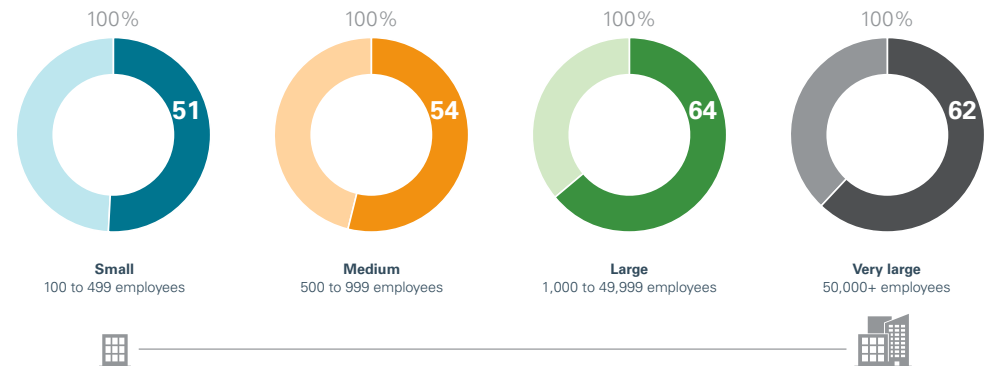
Importance by size of organisation

The risks to reputation, both internally and externally are real, particularly when protocols, training and data management strategies are not commonplace. **Those in larger organisations see these risks more – but those in smaller organisations have as much, if not more, to lose.**

What are the top three concerns regarding security of data within your organisation?

%
■ IT
■ Finance
■ Marketing
■ HR

42 37 39 38
Reputation risk
to customers

39 33 38 32
Compliance with company
policies and external regulations

34 30 33 37
Respect for
personal identity

How important is the secure management of data to the reputation of your organisation? – Very important

100% **51**
Small
100 to 499 employees

100% **54**
Medium
500 to 999 employees

100% **64**
Large
1,000 to 49,999 employees

100% **62**
Very large
50,000+ employees

*Base: Global population,
24 markets, nr. 5,539*

ORACLE
Cloud

Try Oracle Cloud today   44
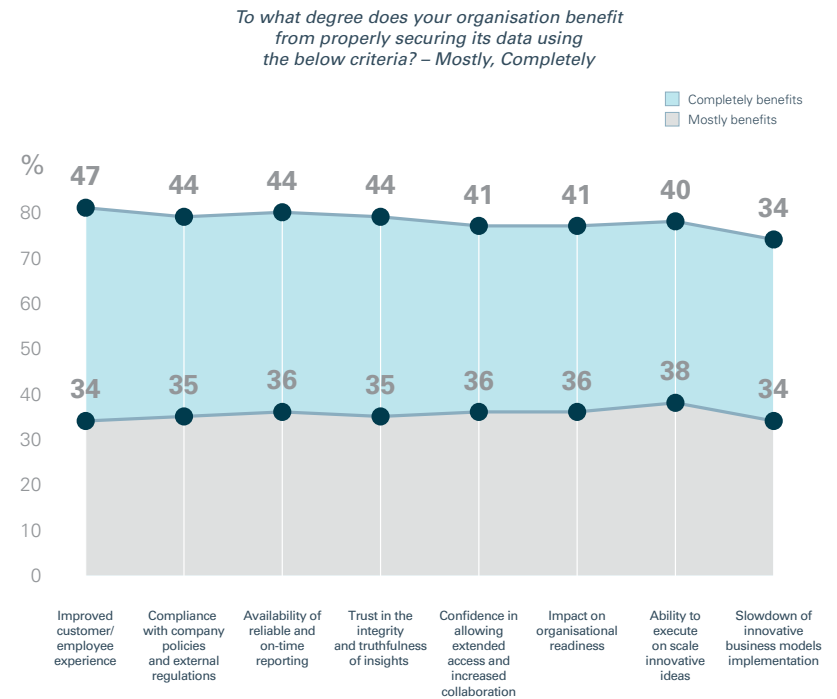
Reputation – Trust and benefits

Trust across audiences

To help achieve trust across audiences, **the proper transfer of data is considered most critical**.

Benefits of securing data

By properly securing their data, **organisations benefit from an improved customer/employee experience and the peace of mind in being compliant** – the availability of reliable reporting is also considered as a plus.

How important are the following factors in allowing your organisation to achieve trust with its audiences (customers/employees/managers/ Government and industry regulators)?

■ Very important
■ Somewhat important

%

	Avoid selling or not approved transfer of data	Confidentiality of data towards third-party partners	Ethical use of persona-related data	Clarity on purpose of data usage	Clarity of roles and ownership	Availability of verifiable controls on data management	Data is not manipulated to reach our advantage	Management of data for machine learning to control bias
Very important	53	52	51	49	49	48	48	43
Somewhat important	29	30	30	32	32	33	32	34

To what degree does your organisation benefit from properly securing its data using the below criteria? – Mostly, Completely

■ Completely benefits
■ Mostly benefits

%

	Improved customer/ employee experience	Compliance with company policies and external regulations	Availability of reliable and on-time reporting	Trust in the integrity and truthfulness of insights	Confidence in allowing extended access and increased collaboration	Impact on organisational readiness	Ability to execute on scale innovative ideas	Slowdown of innovative business models implementation
Completely benefits	47	44	44	44	41	41	40	34
Mostly benefits	34	35	36	35	36	36	38	34

Base: Global population, 24 markets, nr. 5,539
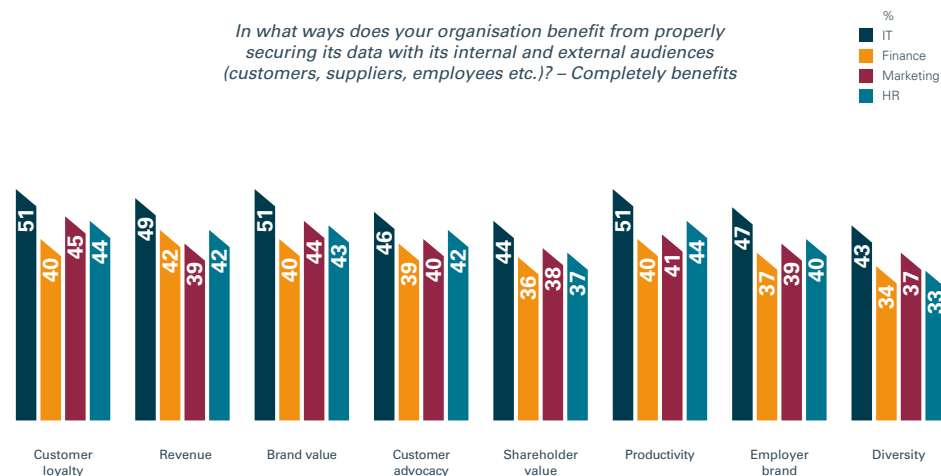
Reputation – Internal/external audiences

Benefits by line of business

Unsurprisingly marketing leaders value customer loyalty and revenue highly. **However, it is interesting that brand value falls 6% or more behind these factors.**

The availability of reliable reporting is also considered as a plus. Across all lines of business, IT was most likely to appreciate the benefits of secure use of data, while finance had least appreciation of the potential.

When it comes to the benefits of properly securing data, **organisations recognise that gains are to be had from an improved customer/employee experience**, such as brand value, customer loyalty and customer brand.
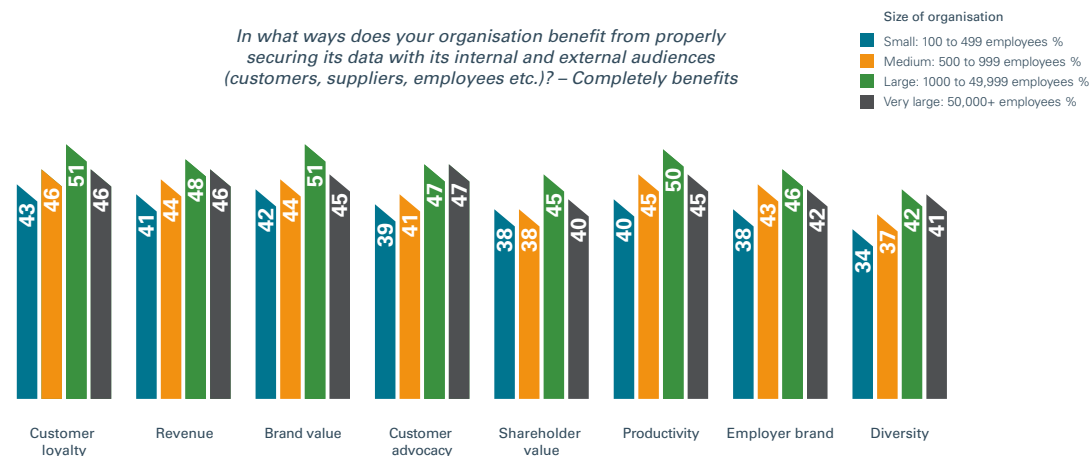
In what ways does your organisation benefit from properly securing its data with its internal and external audiences (customers, suppliers, employees etc.)? – Completely benefits

Legend:
- IT
- Finance
- Marketing
- HR

	Customer loyalty	Revenue	Brand value	Customer advocacy	Shareholder value	Productivity	Employer brand	Diversity
IT	51	49	51	46	44	51	47	43
Finance	40	42	40	39	36	40	37	34
Marketing	45	39	44	40	38	41	39	37
HR	44	42	43	42	37	44	40	33

Benefits by size of organisation

When it comes to properly securing their data, smaller companies believe they benefit less in terms of customer advocacy, employer brand and diversity.

In what ways does your organisation benefit from properly securing its data with its internal and external audiences (customers, suppliers, employees etc.)? – Completely benefits

Size of organisation:
- Small: 100 to 499 employees %
- Medium: 500 to 999 employees %
- Large: 1000 to 49,999 employees %
- Very large: 50,000+ employees %

	Customer loyalty	Revenue	Brand value	Customer advocacy	Shareholder value	Productivity	Employer brand	Diversity
Small	43	41	42	39	38	40	38	34
Medium	46	44	44	41	38	45	43	37
Large	51	48	51	47	45	50	46	42
Very large	46	46	45	47	40	45	42	41

Base: Global population, 24 markets, nr. 5,539

ORACLE Cloud

Secure management of data

So how do business leaders feel about the potential risks to their organisation's reputation from data management practices? Managing data securely is considered highly important according to 58% of respondents overall. Again, IT leaders lead with this understanding – no doubt a reflection of being closer to the issues and concerns surrounding security and potential breaches.

However, in today's world, where the potential value of data is so significant, along with the value of an organisation's reputation, this needs to be significantly higher across all departments.

It is quite astonishing that only 50% of marketing leaders – the owners of the external audience reputation – are not far out in front. Is this a sign of complacency or apathy?

Based on the last six months, how confident are you that your organisation's use of data is ethical? – Highly confident

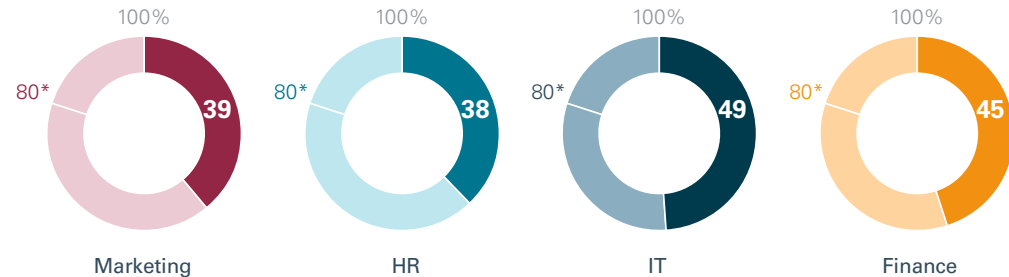| Marketing	HR	IT	Finance
100%	100%	100%	100%
80*	80*	80*	80*
39	38	49	45

Summary

The findings suggest that the areas where reputation can be enhanced are well understood, such as reputation in front of the customer and compliance, and the potential positive impact can be felt on the brand and customer loyalty. However, the degree of impact is less appreciated with only a little over half of business leaders believing this significantly impacts the reputation of their organisation.

Business leaders across functions and organisations, need to recognise the opportunity presented by being truly in control of their data. By demonstrating best practices for securely managing data, ensuring ethical and responsible use, and maintaining integrity in data quality and insights, they can deliver significant business value through building trust. This will be felt not only from organisational reputation and trust, but also in greater insight, decision making, and personalised and relevant interaction.

The alternative is that these lessons are learnt through negative experiences.

Base: Global population, 24 markets, nr. 5,539

ORACLE Cloud

Next steps

A summary of next steps
and recommendations

ORACLE Cloud

It is a positive sign that **all lines of business place first or second priority on enhancing security controls and procedures, alongside the need for greater insights**. Also on the list of priorities was accelerating a move to the cloud – with the cloud now recognised as a solution to greater security.

Please confirm your top three security and data priorities for the year ahead

	Marketing Rank from 1-8 (%)	HR Rank from 1-8 (%)	IT Rank from 1-8 (%)	Finance Rank from 1-8 (%)
Enforce technologies enabling insight availability instantly/anyplace/anytime – securely	1 (35)	4 (30)	2 (35)	1 (34)
Enhance security controls and procedures	2 (33)	1 (37)	1 (36)	2 (32)
Promote internal awareness and education to threats	3 (30)	2 (34)	7 (29)	3 (30)
Accelerate move to cloud for enhanced security performance	4 (28)	3 (30)	3 (32)	5 (27)
Integrate AI and machine learning to drive actionable insights from data	5 (27)	7 (25)	4 (31)	4 (28)
Adopt secure platforms to scale services	6 (27)	6 (26)	8 (26)	7 (26)
Use machine learning capabilities to self-patch and secure data	7 (25)	5 (27)	5 (29)	8 (19)
Ensure controls on AI and machine learning algorithms to reduce bias	8 (24)	8 (22)	6 (29)	6 (26)

Base: Global population, 24 markets, nr. 5,539

- **Marketers need to become cognisant with the implications of data** – and shape marketers' behaviour to manage poor quality data, manage too much data and too many sources, and align with business unit financials to broaden marketing beyond traditional campaigns and programmes

- **Educate employees** to ensure that threats are understood and common protocols are implemented and effectively monitored

- **Work across the entire organisation** to put in place a data management strategy with common protocols

- **Prioritise insights to enable better decision making** with a focus on forward-looking analytics and prediction to improve speed, accuracy, agility and productivity – but ensure any bias is managed at source

- **Build ethicality within your culture** – an ethical mindset starts with leadership and should be documented into an ethical framework, and potentially overseen by a Chief Ethics Officer

- **Marketers should encourage the use of technologies that** relieve the administrative burden and enable them to respond to customer needs in realtime

To learn how transformational technologies can help innovate your marketing department, **why not try Oracle Cloud today?**

Oracle Cloud

ORACLE®
Cloud