Developing trust in your people data

Measuring the confidence of **HR leaders** in their data management practices

Your Tomorrow, **Today**

ORACLE Cloud

Methodology

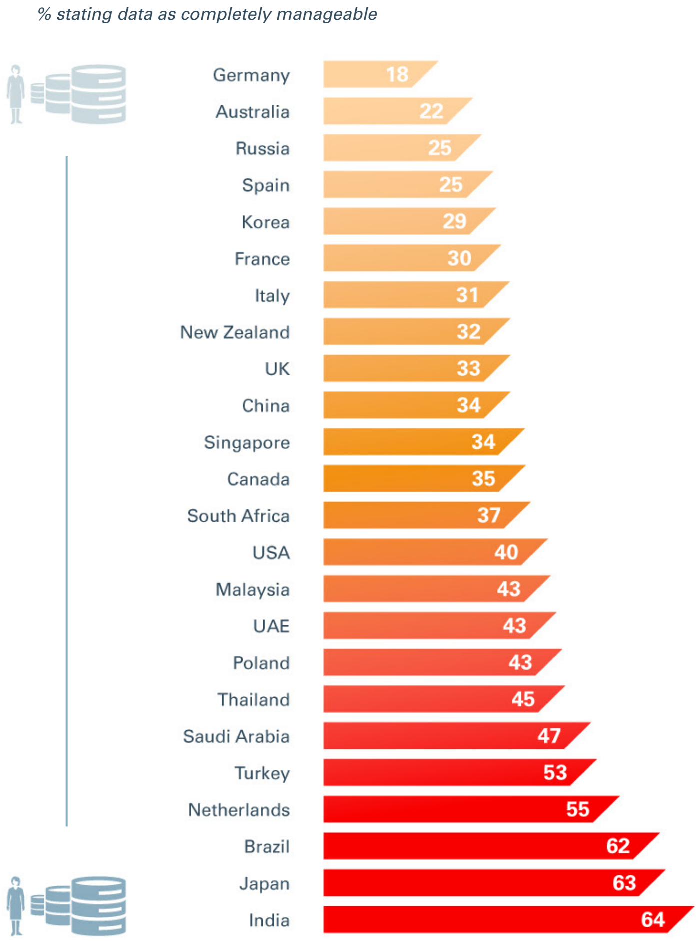
The results presented in this report are based on a mobile-only, 23-question global survey. This survey targeted Manager, Director, Vice President or C-Level executives with influence in the decision-making process of cloud solutions, platforms, and infrastructure or department specific software. Respondents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

Contents

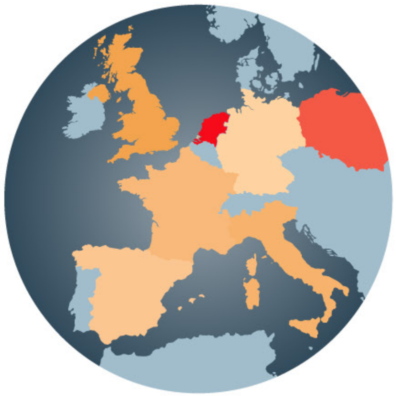
Who believes they are truly capable of managing this deluge of data? Decision makers in **Brazil, India, and Japan say they are the most capable of managing the data they generate**.

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

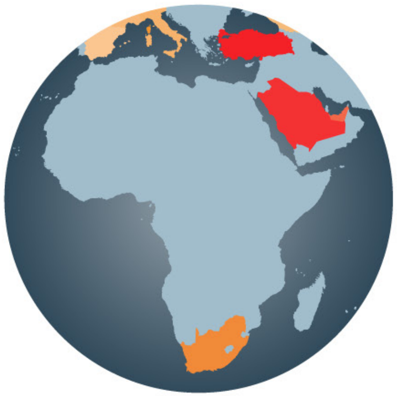
Base: Global population, 24 markets, nr. 5,539

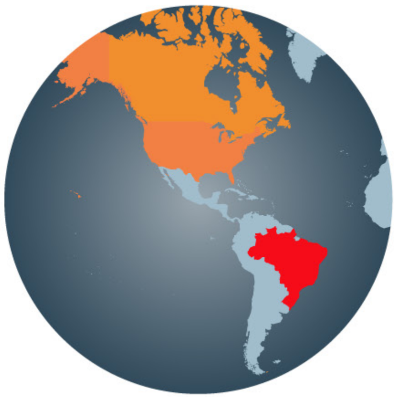


Europe

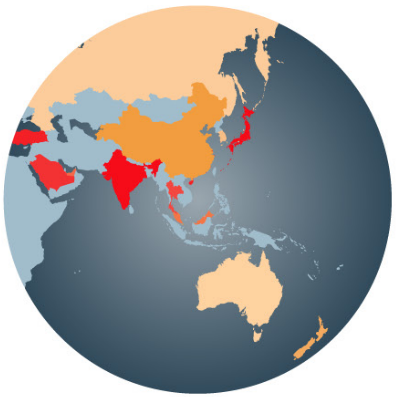


Africa





North, Central and South America



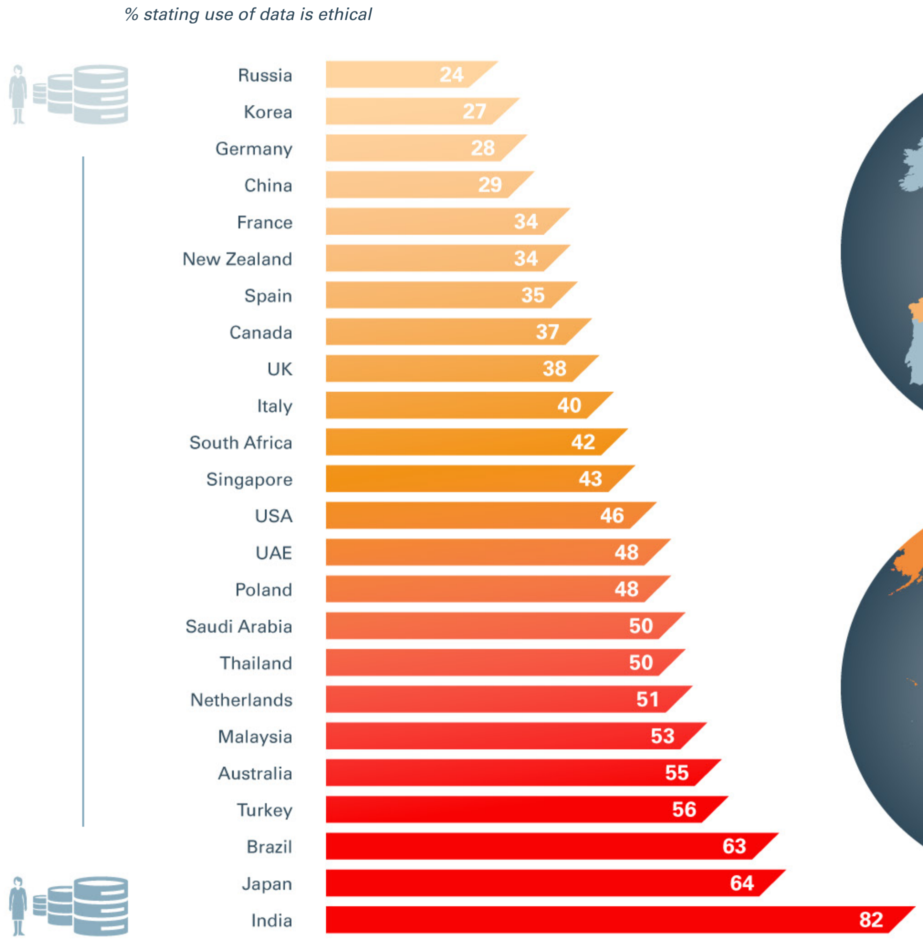
Asia, Japan and Pacific

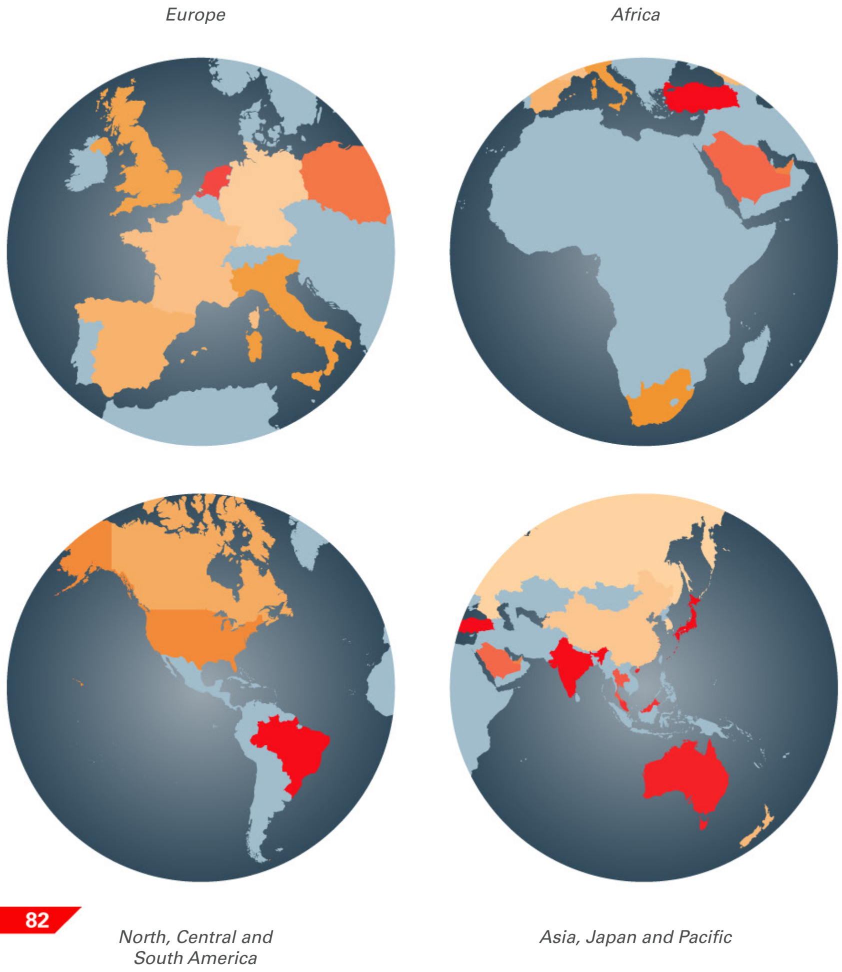
Ethical use heat map

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





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

- How well organisations are globally 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:

- **HR leaders believe data management is a burden on businesses:** Only 35% 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 often 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 both manageable, and 'managed'.

- **Key departments like HR 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 HR, accept accountability for their data, and a further third take responsibility for key actions only. IT lead 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 35% of HR leaders (43% of all respondents) are highly confident in their security of the data their organisation holds – lowest of all departments surveyed.

- **Only 54% of HR 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 32% of HR 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 38% of HR 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.

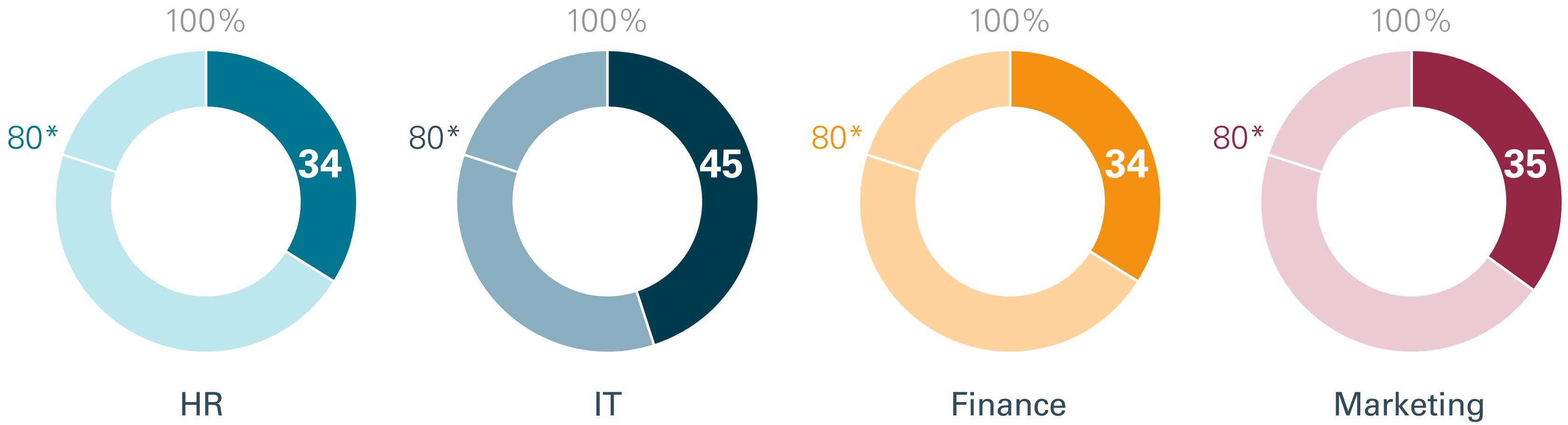
Data management

Ensuring quality to deliver greater value

Only 34% of HR 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*



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

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.

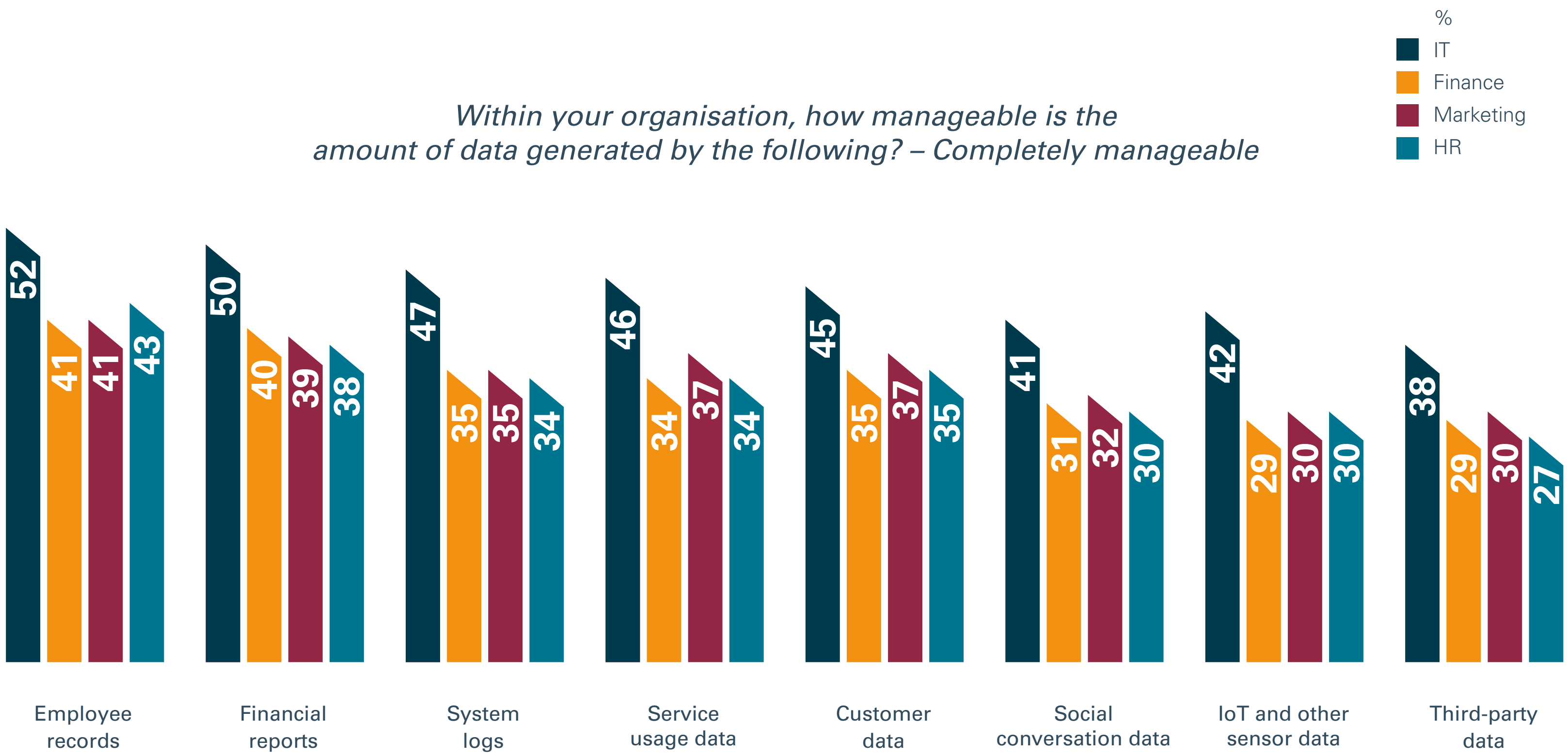
In the past, data was typically informed historical reporting, with internal needs and compliance taking priority. Today, HR leaders require far more external data for security, predictive thinking, and to innovate for the future. Compliance and risk management are still key, but the field of data has got bigger and far more complex. Digital risk will be a standard financial reporting mechanism, with the culture of analytics becoming a necessity for data-driven insights.

Businesses have been forced to adapt their organisational models, and this creates a wave of opportunities in which data can enable the business: role based mobile permissions, connection and networking, and personalised communications. HR leaders are now trying to catch up with opening communications within their business, whilst staying compliant and enhancing employee trust. As well as trust, there is the question of accuracy for CEOs, analysts and investors.

Meanwhile the transfer to the cloud means that IT's role is changing – with security becoming more of a collective responsibility between the central IT function and those that use and execute on the data. Responsible use and management of data are key elements of a digital economy. CHROs need the support of CIOs and technology to effectively monitor and manage the risk organisation's digital use, and therefore manage risk.

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

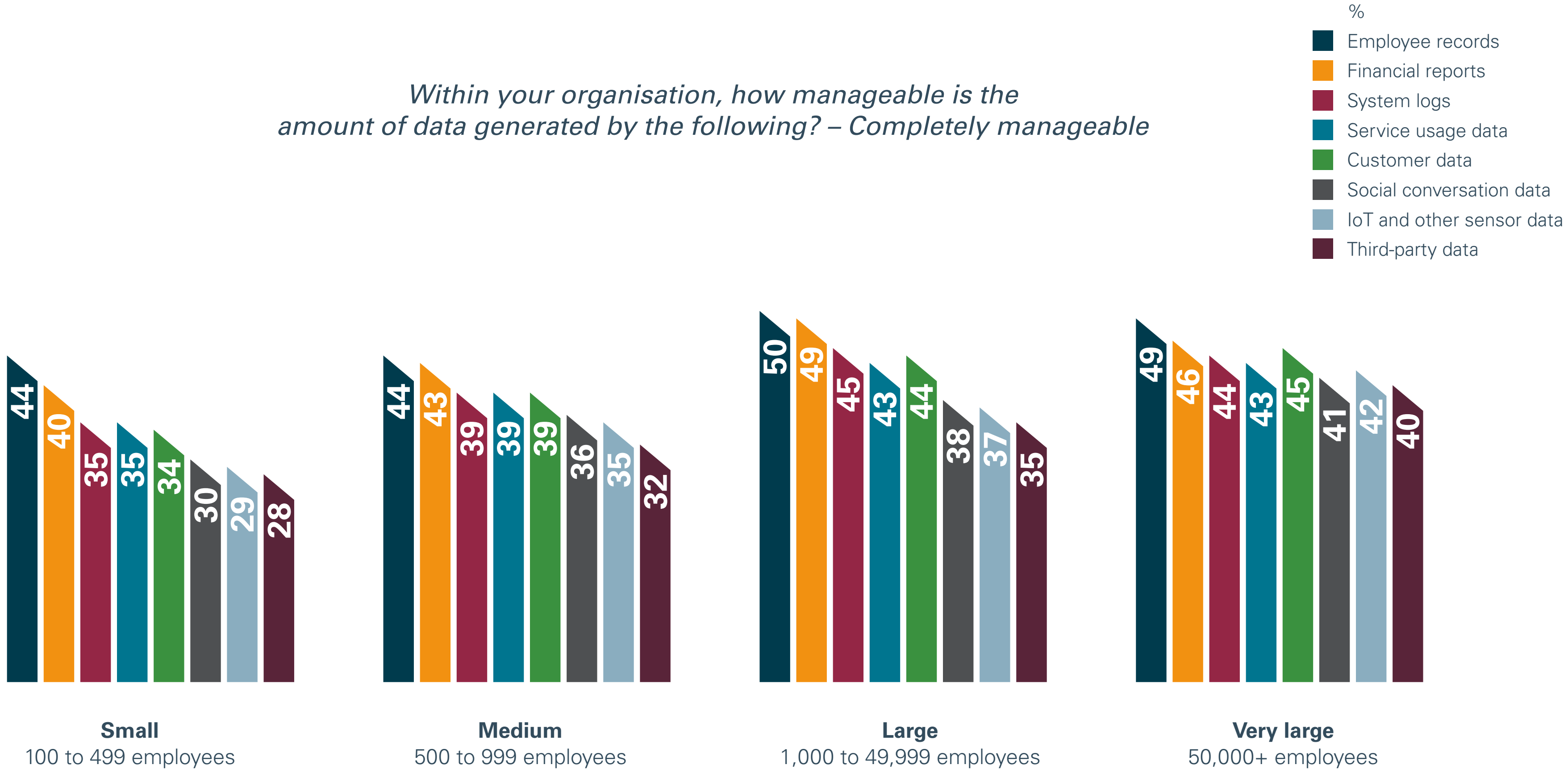
Within your organisation, how manageable is the amount of data generated by the following? – Completely manageable



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

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.

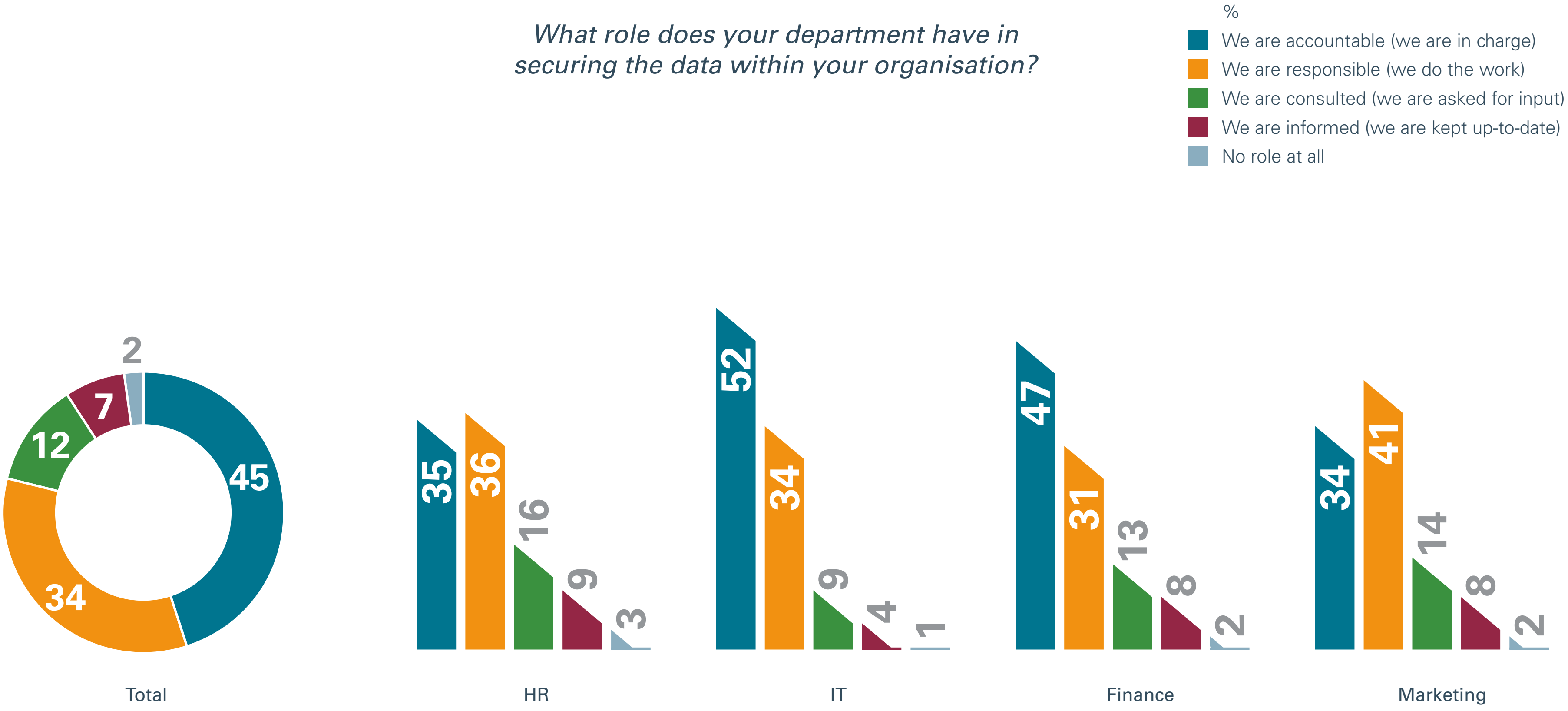


Within your organisation, how manageable is the amount of data generated by the following? – Completely manageable

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

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 – HR and marketing – are taking less accountability**.

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

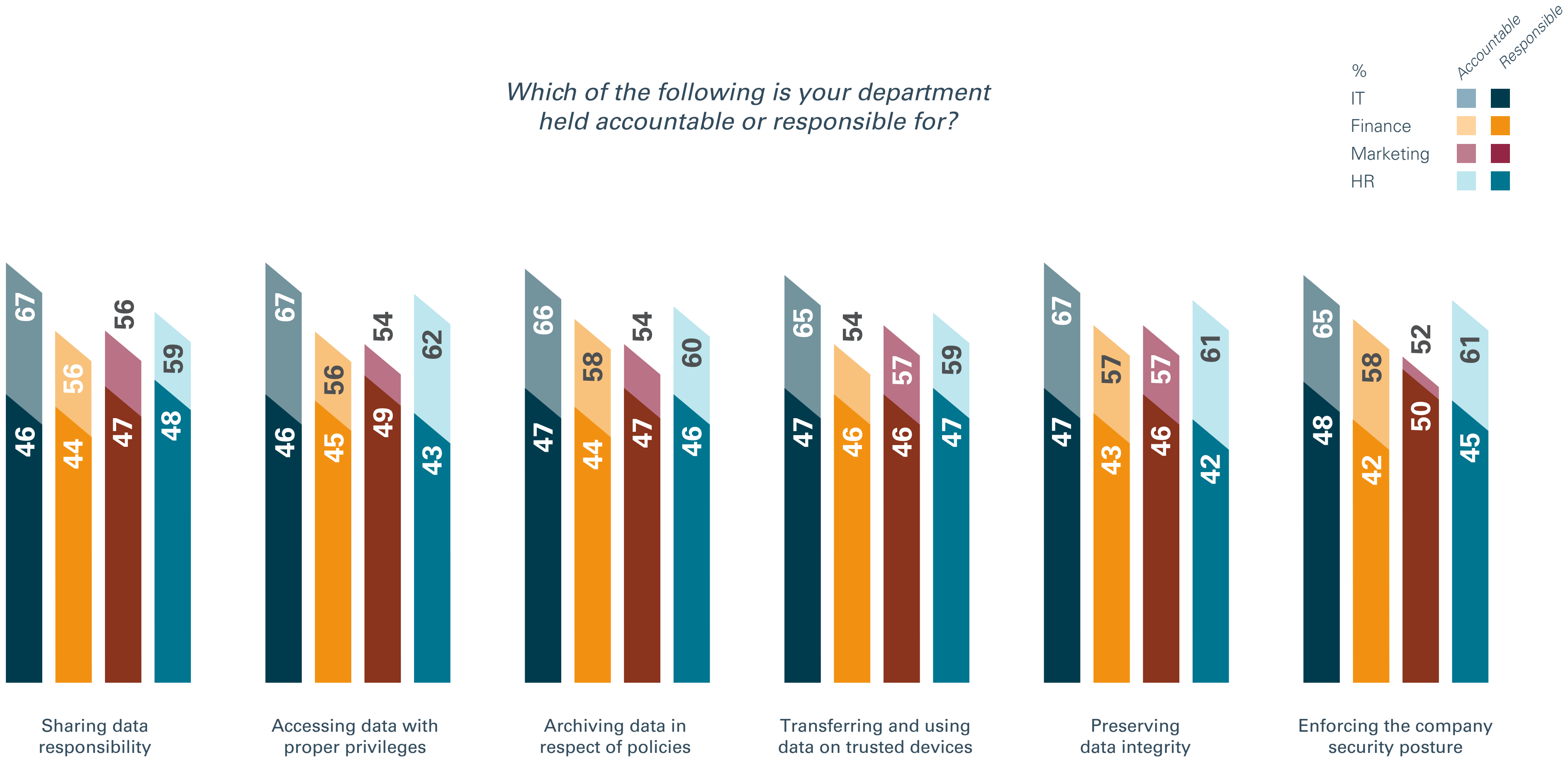


Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

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?



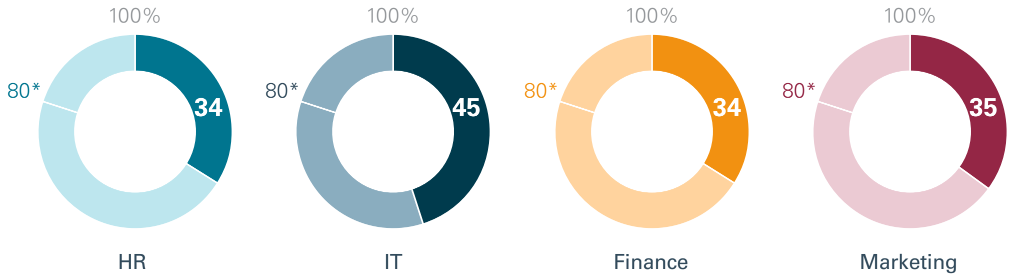
Base: Global population, 24 markets, nr. 5,539

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. However, despite these systems only 34% of HR leaders, and less than 50% across all business leaders and all forms of data, believe their data to be completely manageable.

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.

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



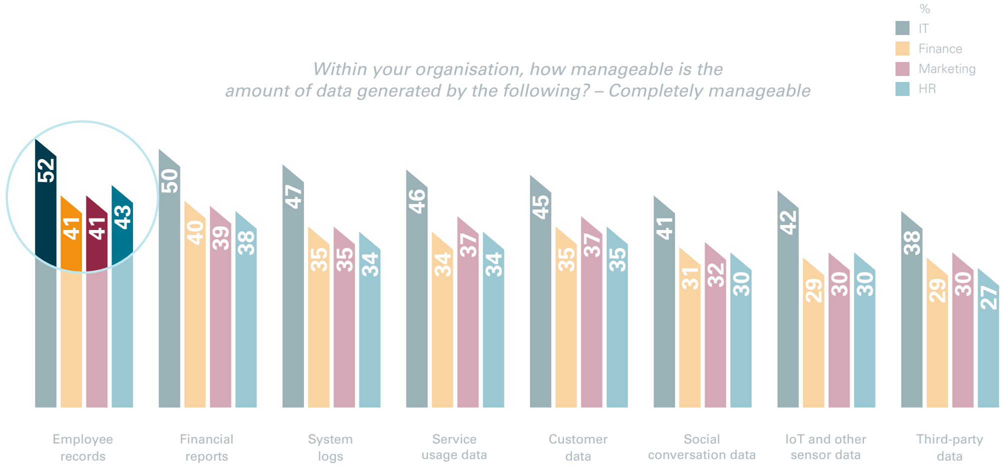
The source of the issue?

However, despite these systems, less than 50% across all business sizes and all forms of data collected find data to be completely manageable.

This comes to light particularly when we look at the management of employee records. Employee records and financial reports are among the top tasks considered most manageable across all lines of business, but even here, only 43% of HR respondents believe that they are completely manageable. While we can account for why IT feels more capable, given their historic role, it is alarming that 57% of HR decision makers fail to find employee records – their key area of responsibility – to be completely manageable.

This means, at best, half of the value from insights and analysis 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.

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



It all starts with being accountable

Responsibility means taking ownership for key actions – but accountability means accepting ownership of the outcome.

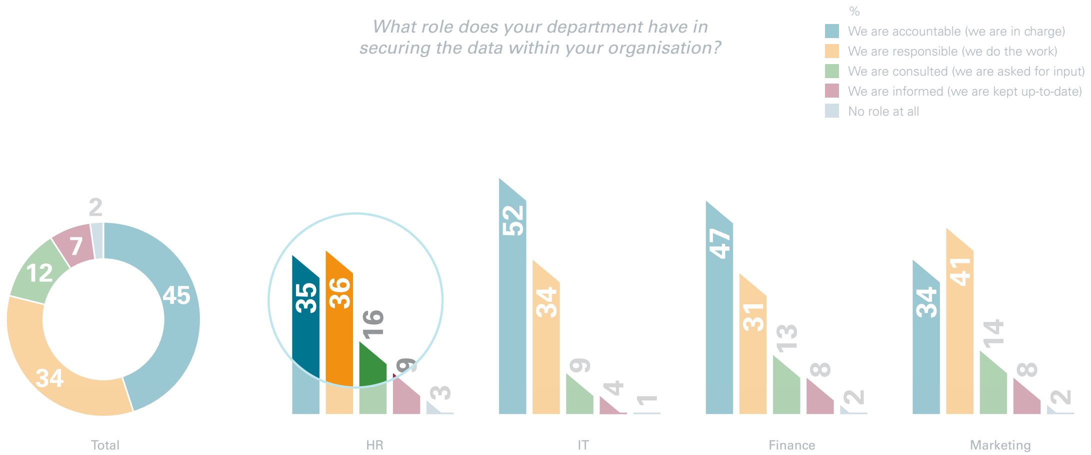
The management of data can be divided into three main functions: data security, data quality and data usage. Historically, the former has been IT's responsibility, and the latter the role of the data user. Data quality has often been a grey area.

With the advent of the cloud, and the importance of data to business success, combined with new regulations, means that more accountability needs to be accepted across all lines of business. 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.

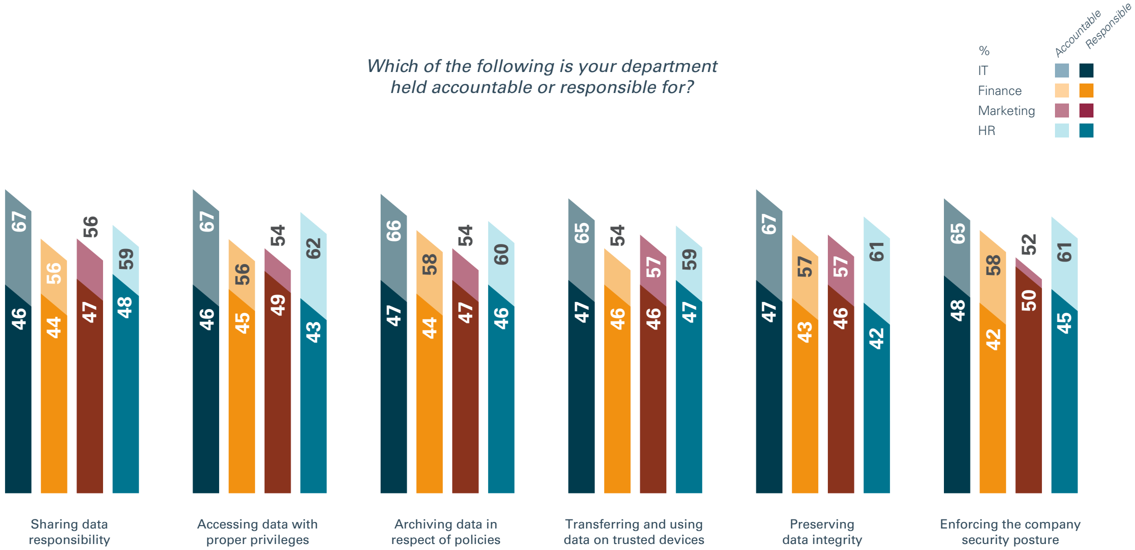
The data shows that marketing and HR do not understand how their roles are changing and that accountability, as well as responsibility, must shift.

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

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



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



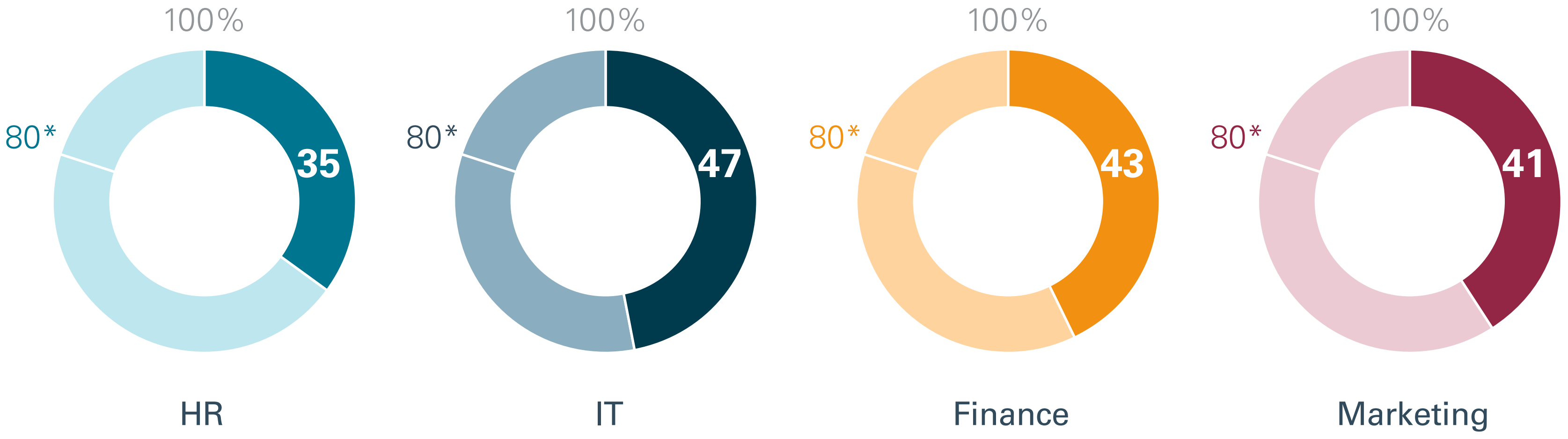
ORACLE Cloud

Try Oracle Cloud today

Only 35% of HR 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*

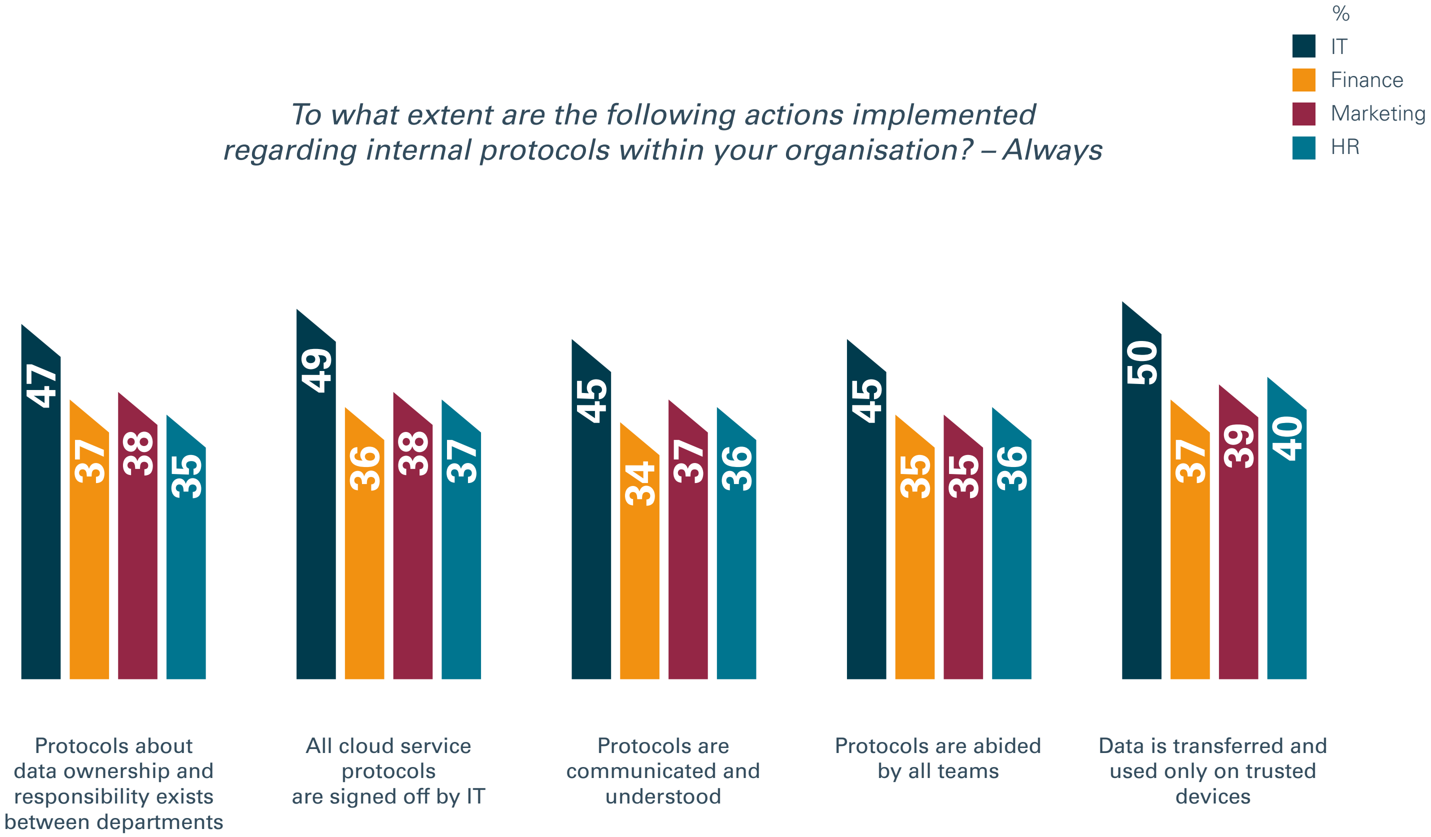


Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

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 **HR are 10% points or more behind**.

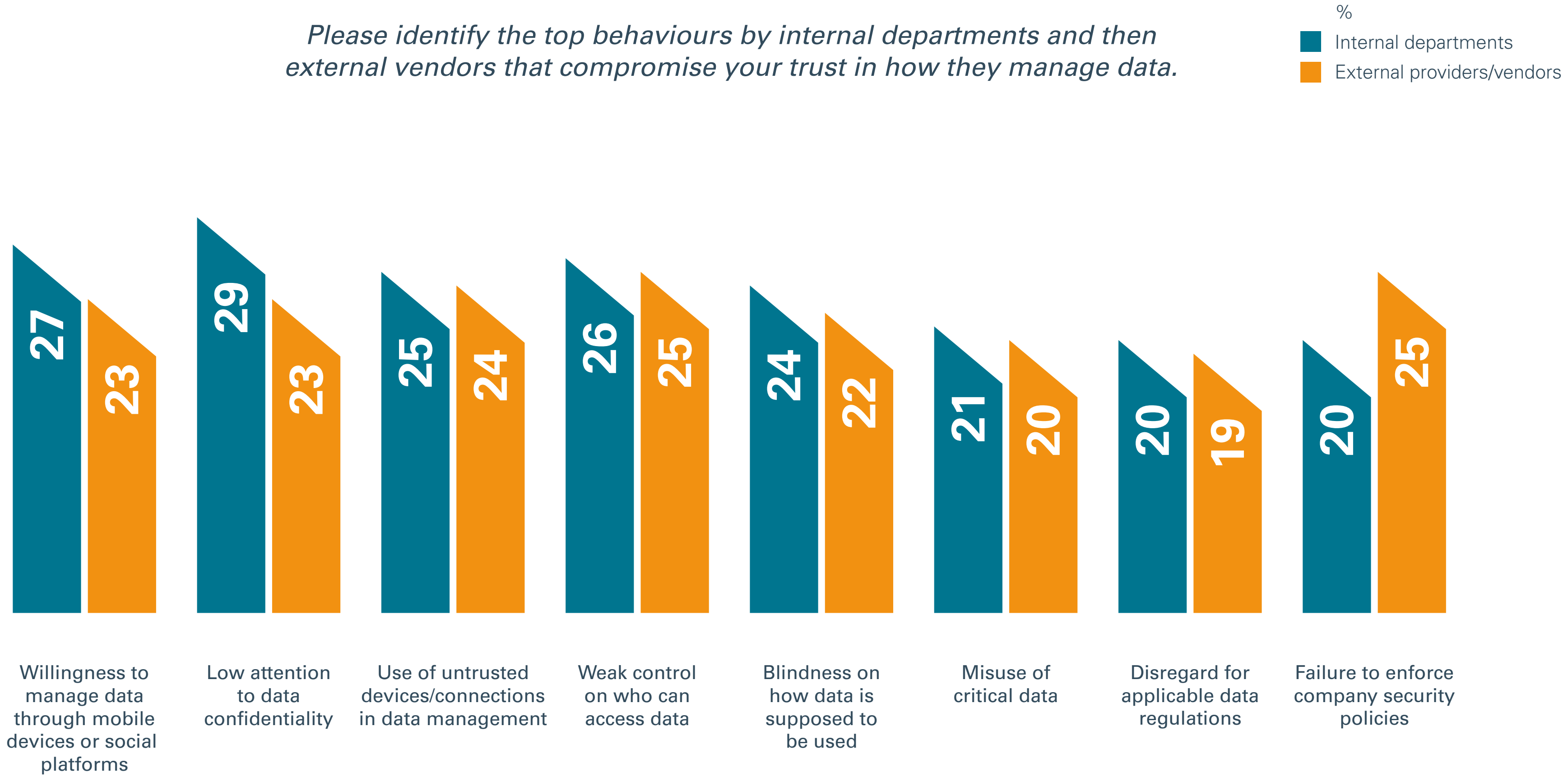
To what extent are the following actions implemented regarding internal protocols within your organisation? – Always



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

So what keeps us awake at night? Low attention to data confidentiality and the use of both mobile/ social platforms, 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.



Base: HR population, 24 markets, nr. 680

Security confidence

With respect to data security, data breach damages aren't as clear-cut as you might imagine, and the impact to a company's bottom line can be devastating. As a result, this issue should be kept under control.

However, when we asked organisations how confident they were in the security of data that their organisation holds, only 35% of HR leaders, and less than half, (43%) of overall respondents can attest to being highly confident.

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

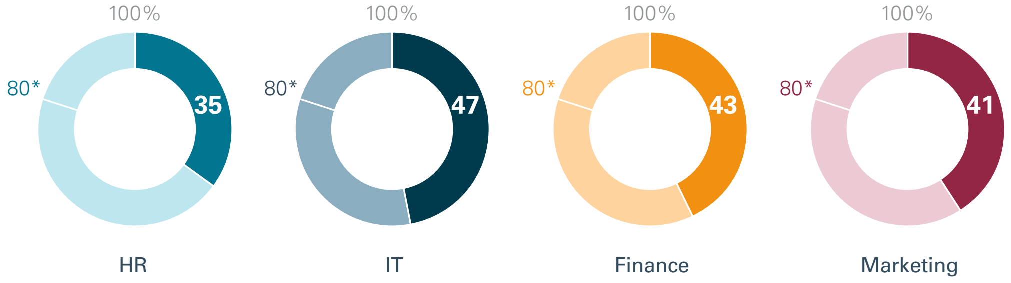
Why aren't respondents feeling more confident in the security of their data? We suggest this relates, at least in part, to internal protocols implemented within the organisation; with less than half of respondents believing any of these critical actions are being fully implemented.

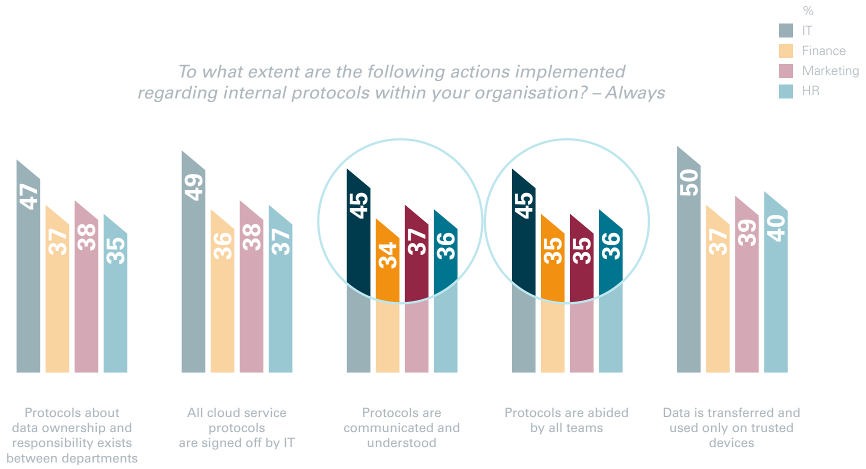
While it is certainly positive that all departments are now attempting to put some protocols in place, there is still much progress to be made.

Organisations cannot expect their people to feel highly confident about the security of their data if only 36% of HR leaders believe that protocols are communicated and understood by their teams, and only 36% believe these protocols are abided by all the time.

The solution lies in organisations creating common protocols, supported by cross-functional teams, to ensure rigour and ownership of organisation-wide policies and programmes.

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




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

Data management – Analysis (cont.)

The pain points

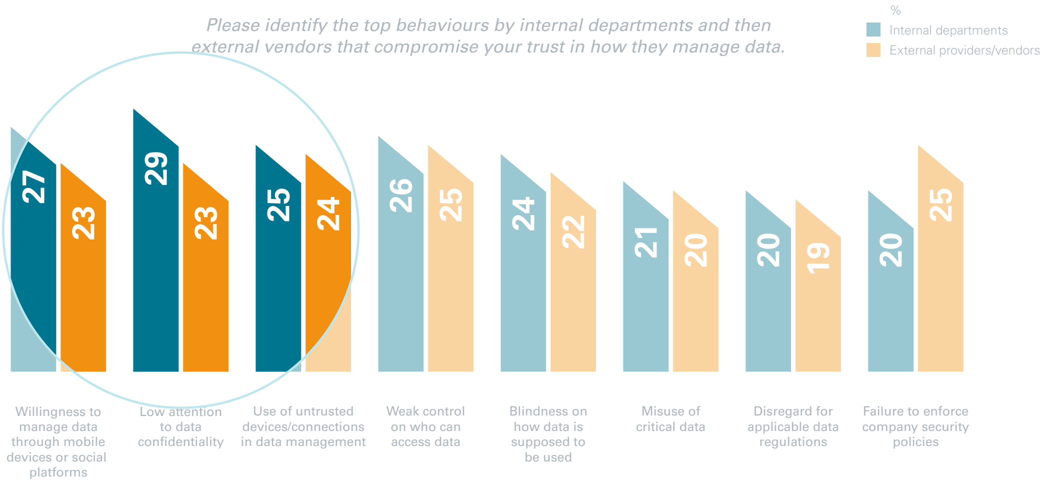
Looking at internal departments, nearly one-third say that the biggest concern around data security across the organisation is a 'Willingness to manage data through mobile devices or social platforms' (27%), 'Low attention to data confidentiality' (29%), and 'Use of untrusted devices and connections'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

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.'

19% of all decision makers state that protocols are abided by all teams sometimes, rarely or never.

Such findings suggest that organisations are currently open to threat due to the identified practices of their own people.

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



Base: HR population, 24 markets, nr. 680

- **HR leaders need to be far more confident in the security of data:** HR is managing the data of its own employees, the fuel for a strong organisation. It should be assumed this data is within their control, which does not account for the low confidence levels. HR needs to get to grips with data management and security before it can take a leading role. To truly embrace the digital economy, culture change is a must.

- **HR is struggling to keep up with expectations.** The basic requirement of HR is to be adaptable while connecting to employees, using data to identify if people are under-utilised or to close the skills gap. This opportunity is lost if the majority of data is not being sufficiently integrated, analysed and managed. HR needs to step up and make themselves accountable to build the workforce of the future.

- **Responsible use and management of data are key elements of a digital economy.** CHROs need the support of the CIOs and technology to effectively monitor and manage the organisation's digital use, and therefore manage risk. If organisations want them to take full accountability and responsibility for data security, they need to free up their time so they can drive innovation with emerging technologies underpinned by data security and trust.

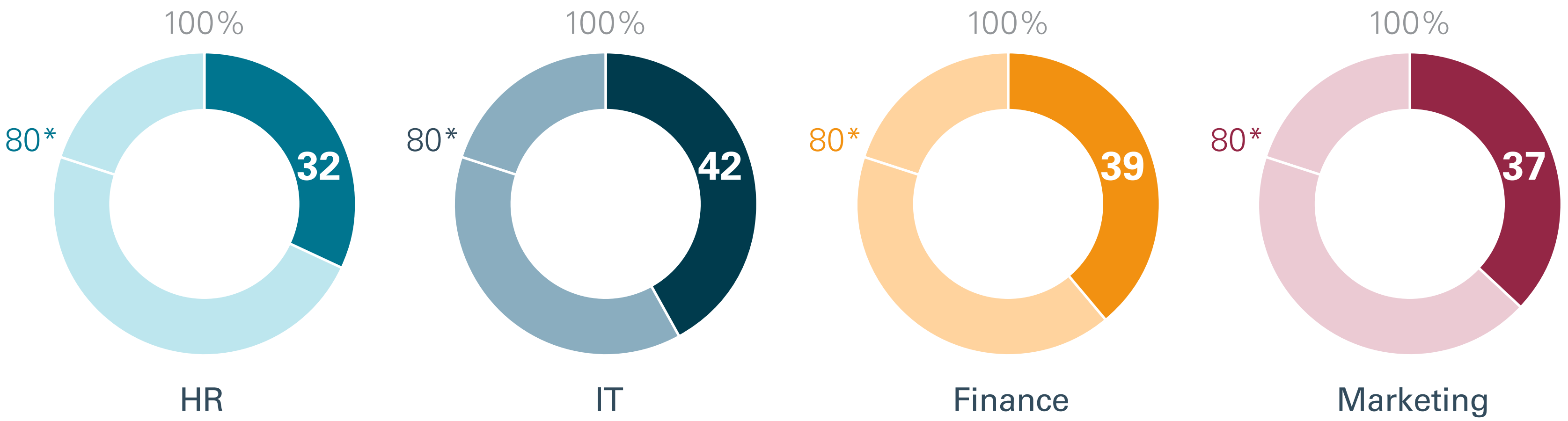
- **Good data management practice requires basic protocols to reduce uncertainty** and make it manageable, and 'managed.' Admittedly, data strategies are somewhat new; protocols therefore need to catch up with the new reality and be enforced within all lines of business. The concept is that a common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

Insights

Using data to its maximum potential

Only 32% of HR 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 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



** Reasonable expectation estimated at 80% or higher*

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

While we are talking about a deluge of data, we are not referring to 'big data'. The challenge is more focused on the accuracy and speed of translating data into effective insights.

The key questions that the C-suite team are asking: Are organisations able to generate maximum insight from the deluge of people data? Is this trustworthy? Is this 'data' or 'insight'?

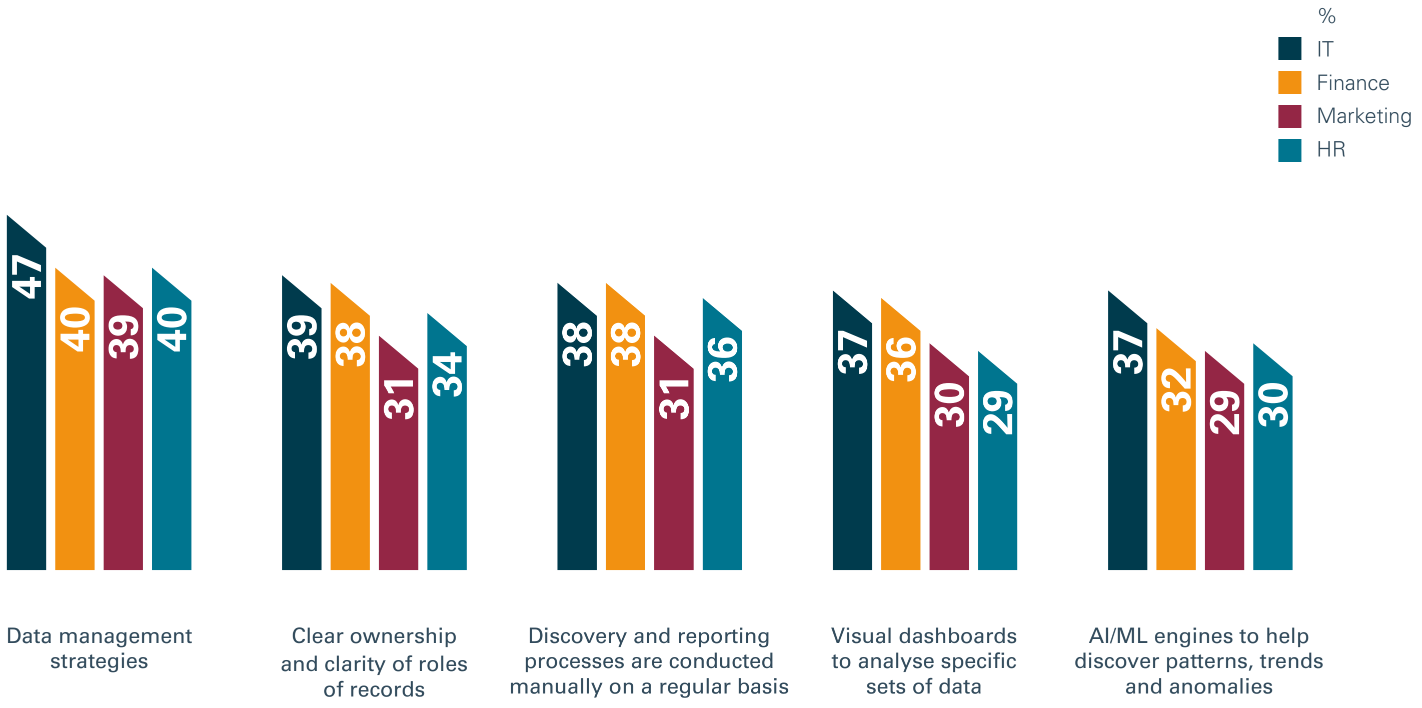
To ensure the survival of their business and secure growth, companies have considerably shifted their models: as a priority that focus has translated into workforce planning and talent needs identification to help win the ongoing war for talent, delivering a personalised working experience, and creating a culture of innovation – however the back-office was not readied to absorb the change and deliver value.

As a result, we are seeing a strong dependency between the expected value from new data and the technology needed to deliver it. Data is spread in different repositories and in semi-automated talent functions. At the moment many functions are still focused on historical reporting only, with little or no forward-looking modelling taking place. There is a lack of measurement of the value created – linking investments in talent to either productivity or engagement. However technology platforms that enable businesses to see and measure their progress and value can be put in place.

Try Oracle Cloud today

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?

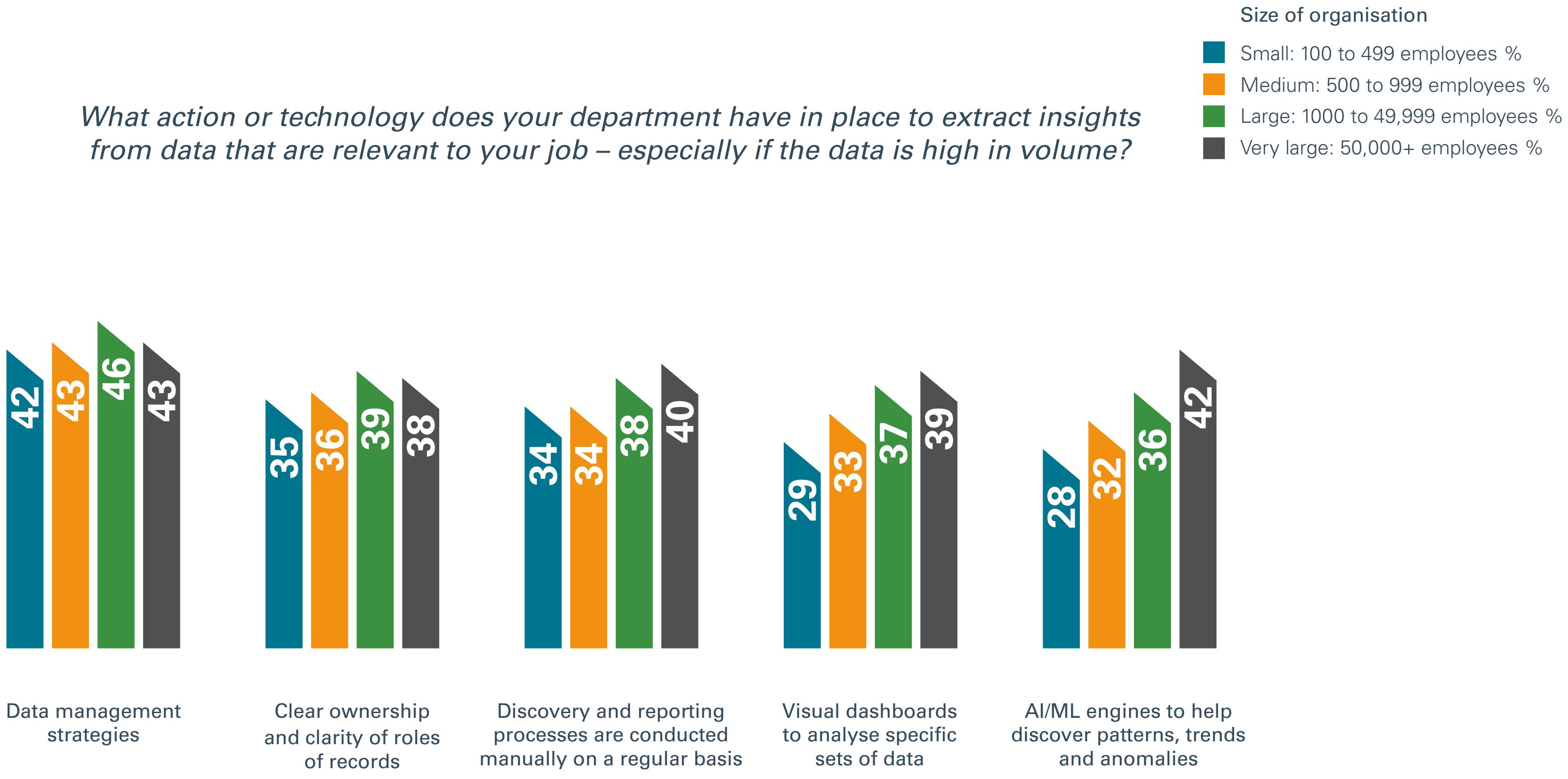


Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

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

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?

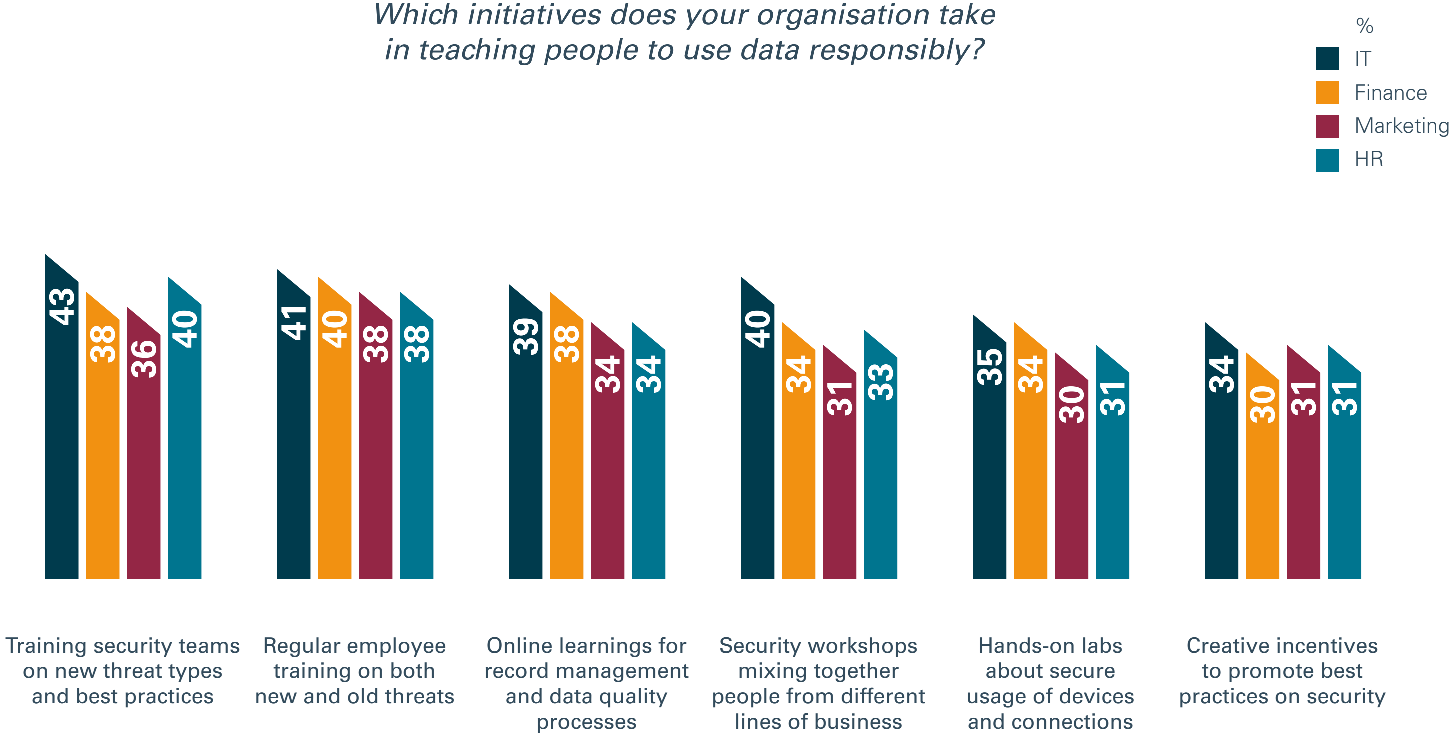


Action	Small: 100 to 499 employees %	Medium: 500 to 999 employees %	Large: 1000 to 49,999 employees %	Very large: 50,000+ employees %
Data management strategies	42	43	46	43
Clear ownership and clarity of roles of records	35	36	39	38
Discovery and reporting processes are conducted manually on a regular 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

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?



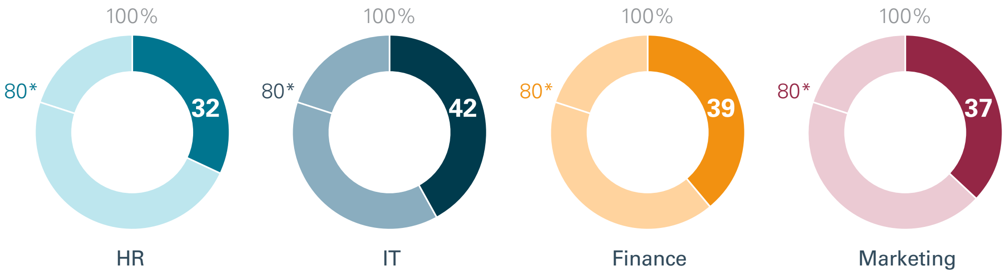
Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

Seeing the value

Only 32% of HR 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

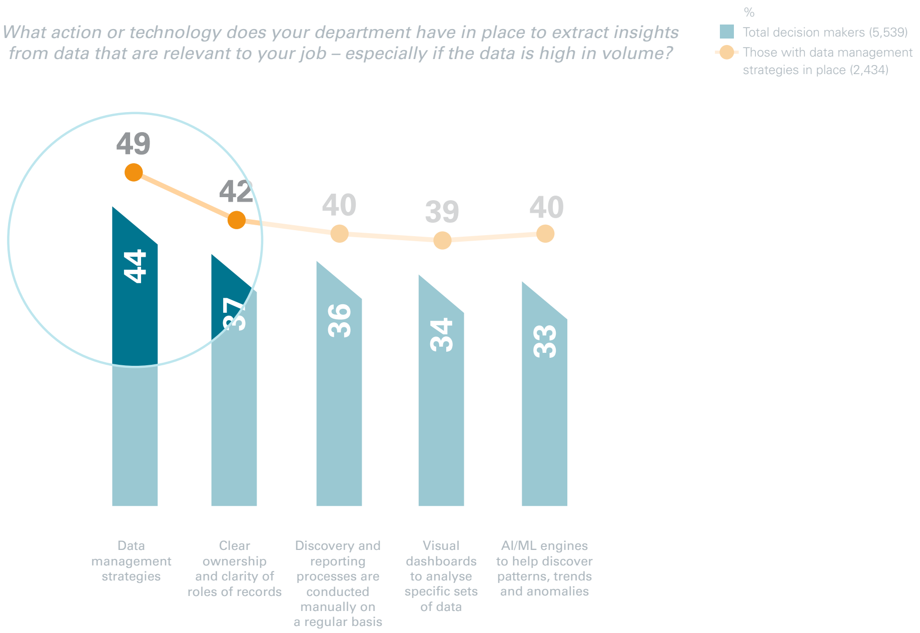


Accountability also leads to stronger data strategies

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.

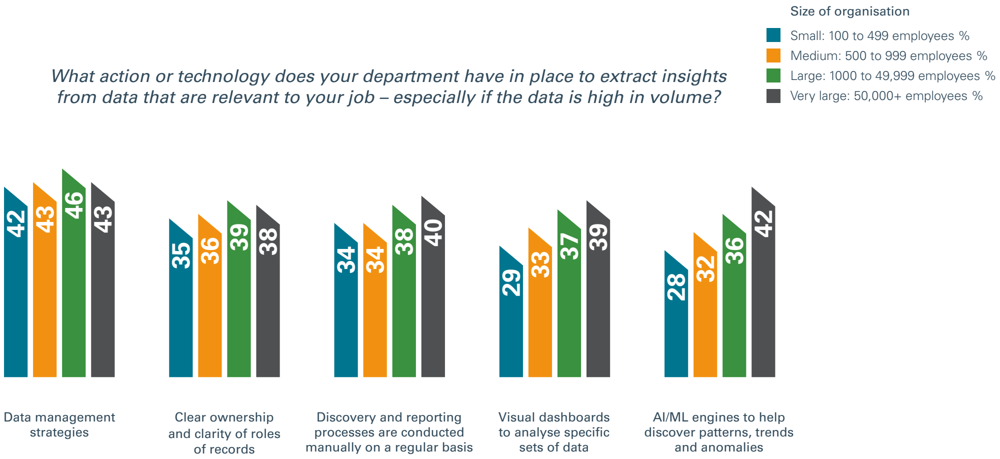
Of the four lines of business, IT and finance come ahead with respect to data management strategies. This is not surprising, but this transfer of responsibility should now be moving through other departments. Marketing teams are less likely to have data management strategies.

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?

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.



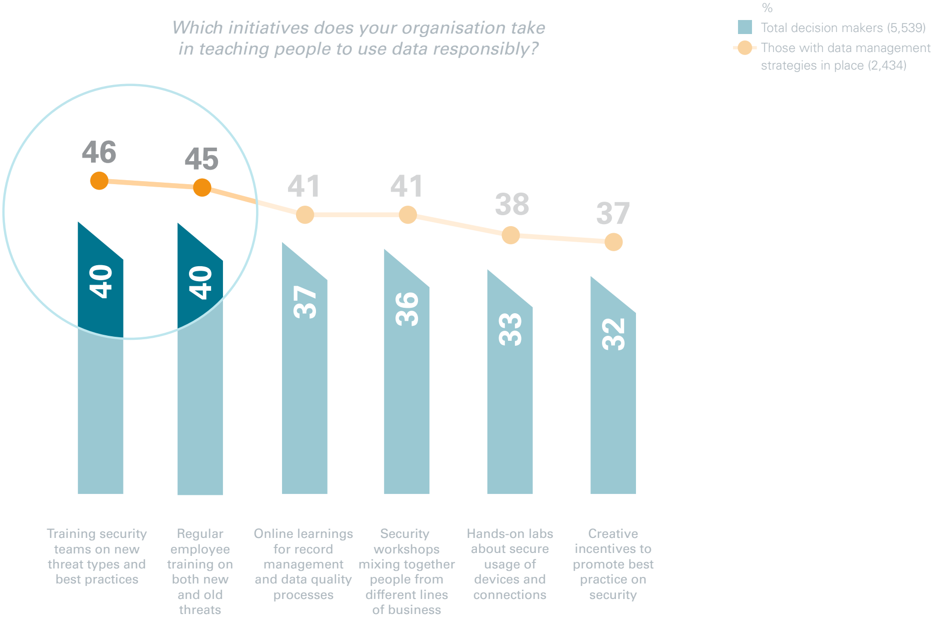
What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?

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.

The evidence suggests that well 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.



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

- **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. HR needs to support 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 CHROs needs to automate data as much as possible; otherwise, there is too much data for a human to compute and protect.

- **Data-driven business and operating models are on the rise.** Therefore, an important consideration is measuring HR performance with metrics and data that business leaders can derive insights from, while working in partnership with other back-office functions like finance. HR leaders need to adopt the same metrics and ensure the data used by the business to measure performance is well aligned.

- **Data is the thread that ties all the lines of business and IT functions together:** Data and technology need to work for organisations by decreasing risk and enabling better, more accurate and more confident decision making with a stronger human/machine partnership. Autonomous technologies and artificial intelligence and machine learning are a means to upscale and amplify the benefits; however, the majority are not relying on these tools.

- **As IT and other departments come together,** empowering people to use data responsibly and training them on threats and data quality processes become more essential than ever. The increasing interest and focus across the board are twofold: ethical data usage and data-driven business models.

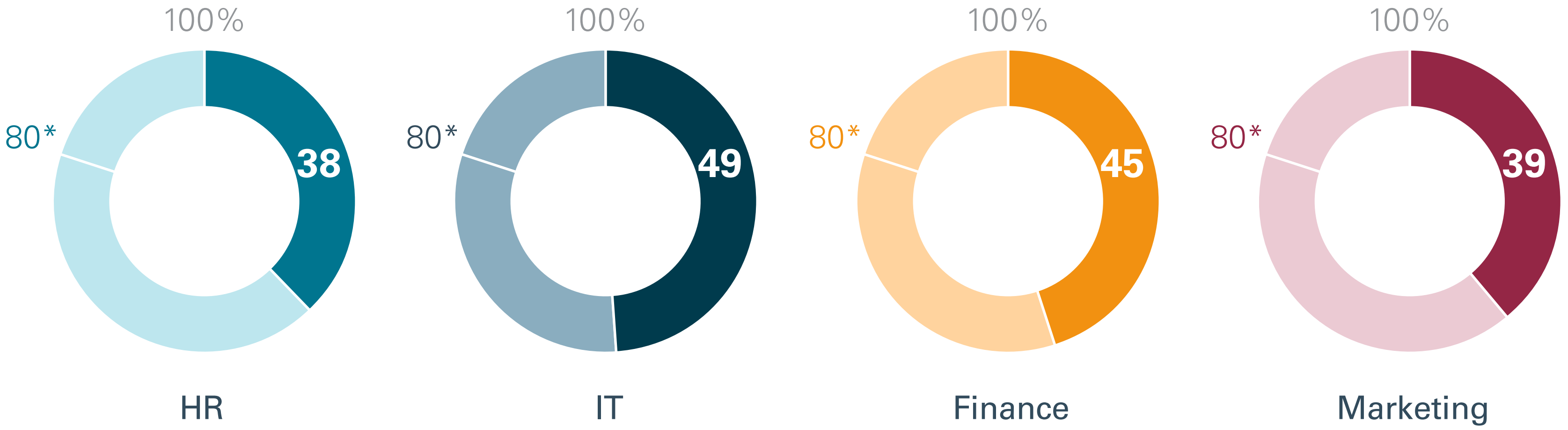
Ethics

The mindset to maintain trust

The majority across all lines of business are not highly confident that their organisation's use of data is ethical – **HR is the lowest at 38% confidence**.

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*



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 employee data from behaviours and work patterns to sensitive performance and worklife data, to sentiment analysis, and leaving triggers, CHROs 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 to derive effective insights to deliver value to the business, and trust to the employees.

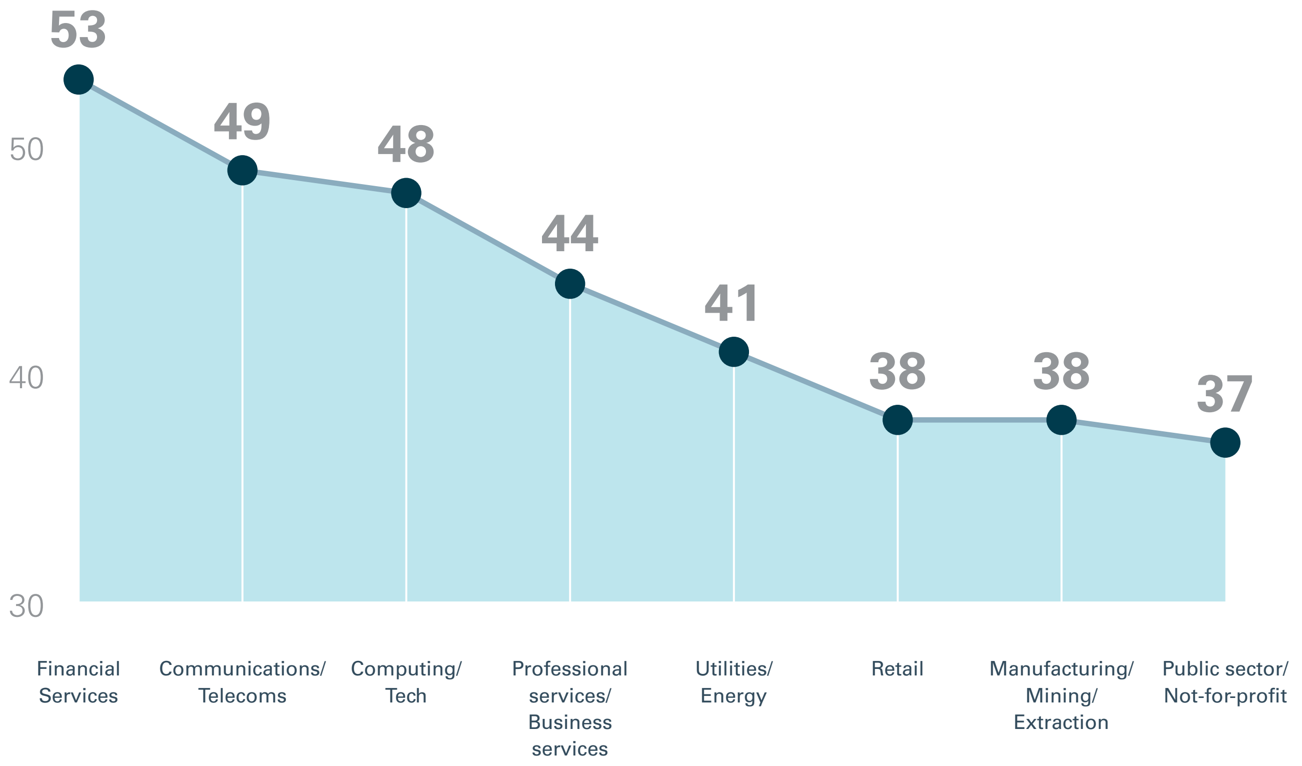
A key consideration for HR leaders is how to ensure that data is being used ethically whilst delivering the experiential programmes that employees value and drive engagement. Ethical usage of marketing data is strongly tied to people's trust in the brand.

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

New generations of employees come with different behaviours and different expectations from the workplace. The more we understand about them the more we can meet those expectations, anticipate their needs, and build employee brands that people feel proud of.

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

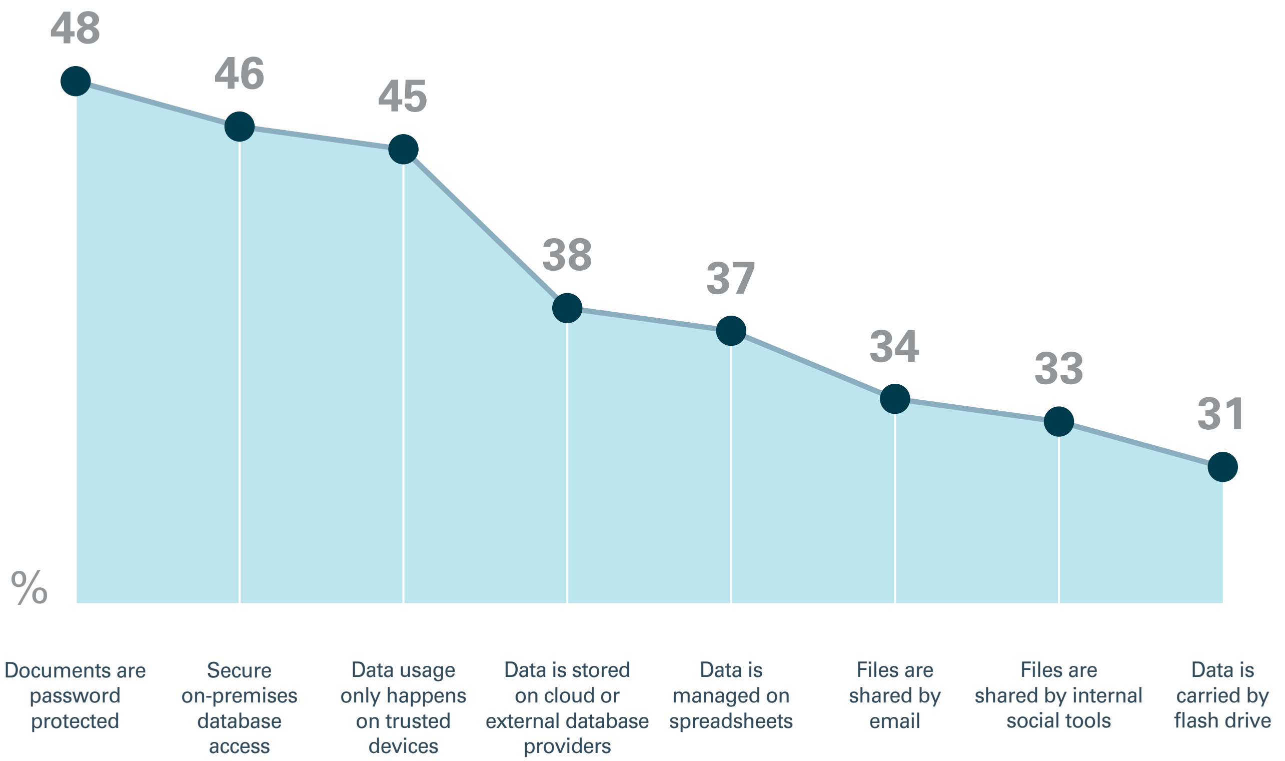


Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

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



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

Putting ethics top of the agenda

HR leaders must ensure that data is being used ethically whilst delivering on key people metrics such as monitoring employee performance, identifying talents needs and gaps, and measuring social sentiment.

This data has to be gathered and analysed for use by senior management and HR policies, whilst not crossing the line. Done correctly, it can add tremendous value to the employee experience. If implemented poorly, it can impact badly on employee perceptions. It is concerning then that only 38% of HR leaders are 'highly confident' that their organisation's use of data is ethical.

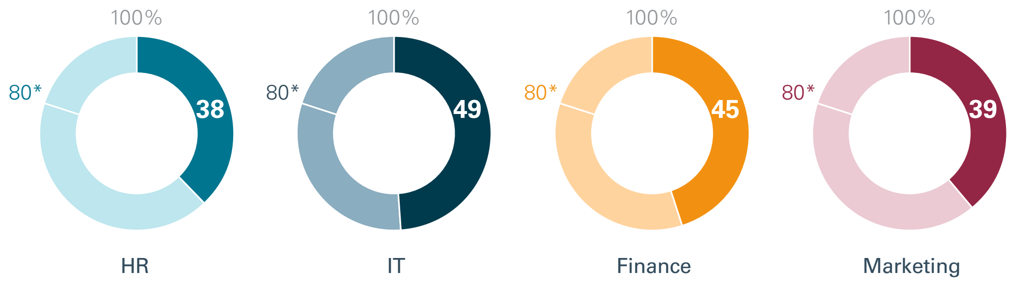
Overall HR's concern is consistent with the global themes: 45% of respondents are highly confident in their organisation's ethical use of data. Just under one-fifth of respondents are not confident at all. While the precise definition of 'ethical use' is complex, we had expected this percentage to be much higher. IT again scores highest (49%) – 10 percentage points above marketing and HR departments.

These findings signify that people are more aware of what unethical looks like and that data management strategies need to pick up.

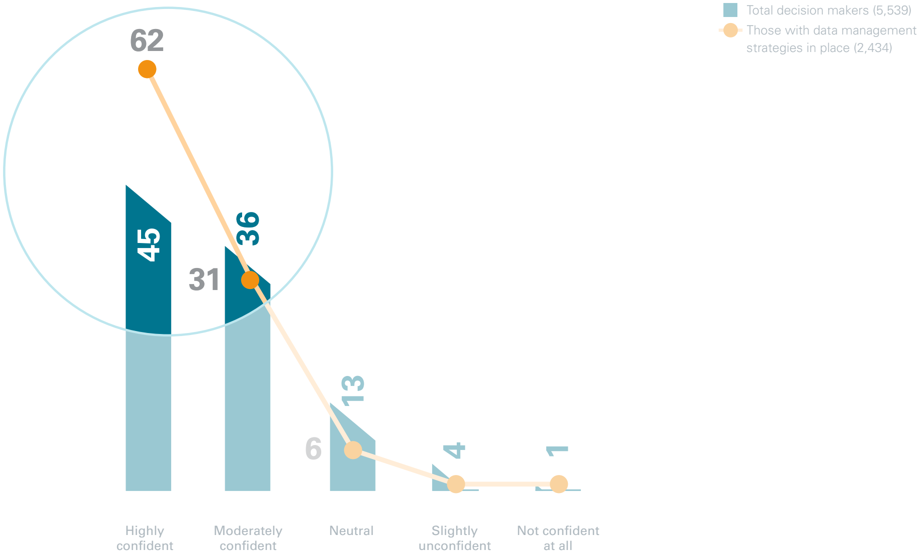
Stronger strategy improves confidence in ethics

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



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

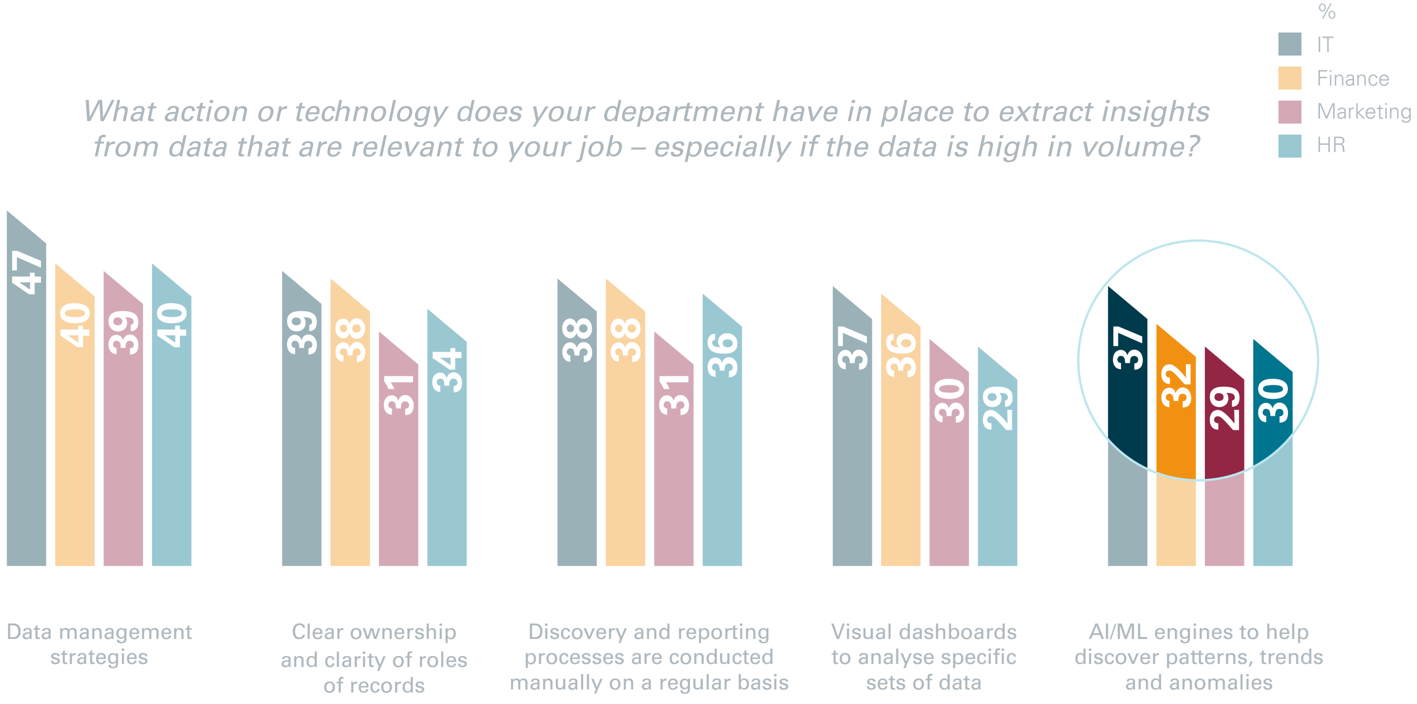


Controlling unconscious bias

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?



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.

Among those with data management strategies in place, a greater proportion say that documents are always password protected and data usage happens on trusted devices – whilst only 3 out of 10 say data is shared by flash drive.

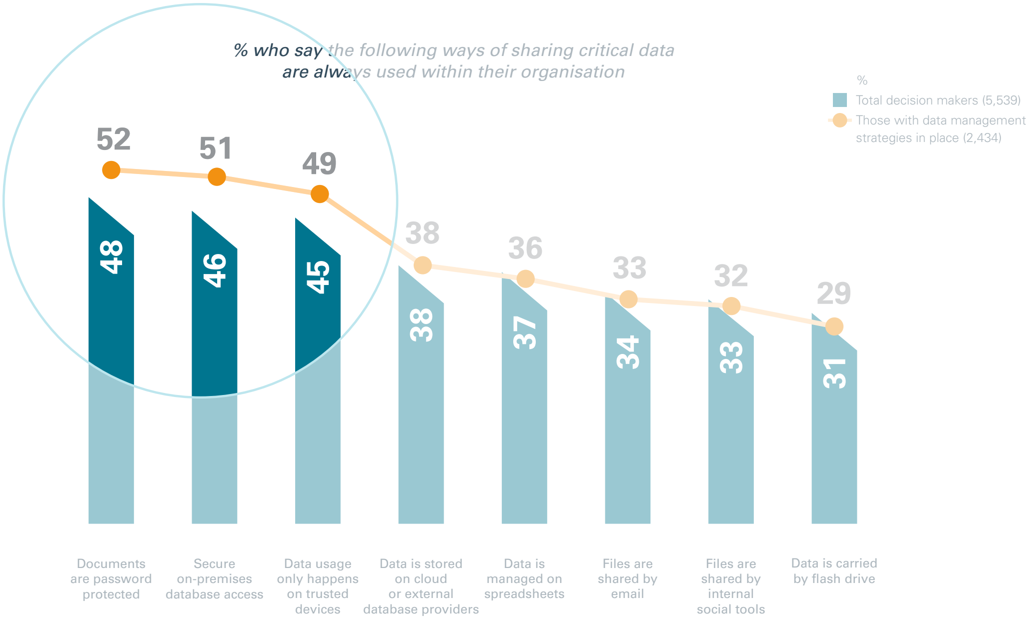
Organisations, and data handling functions within them, cannot afford to let short-term pressures dictate data management decisions that compromise ethical considerations.

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 topics 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.



The factors required 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.

HR needs to consider this not just as a threat, but an opportunity: HR can view this as a window to develop a code of conduct while successfully managing data through reasonable actions and trustworthy statements.

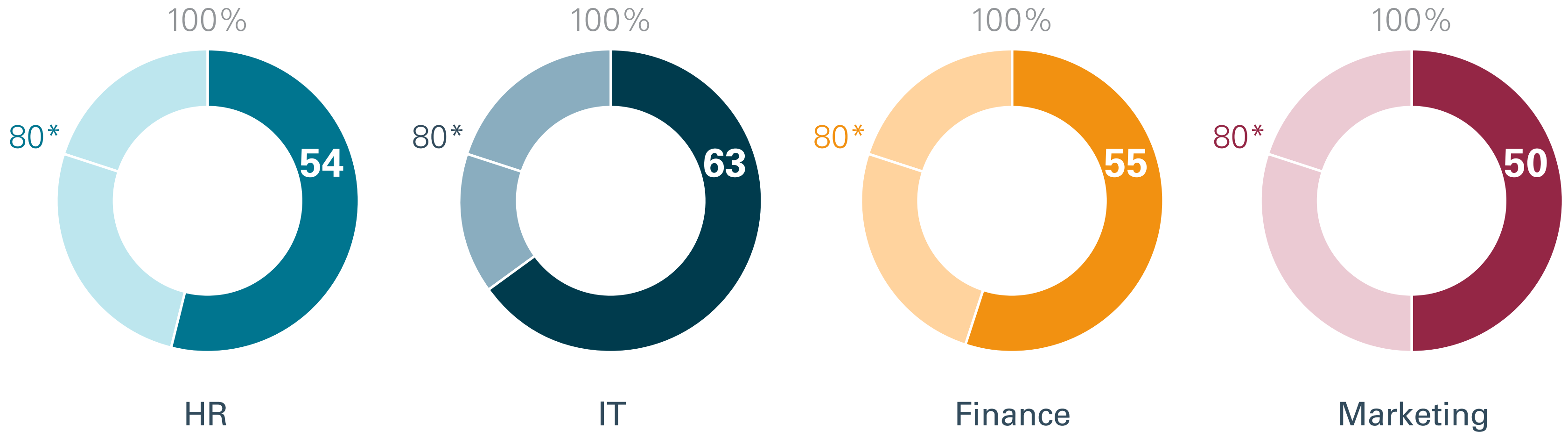
This all combines to deliver *ethicality*.

Reputation

Ensuring your organisation's reputation is supported by data

54% of HR leaders fully believe that the way they manage data is important to the reputation of the organisation.

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



** Reasonable expectation estimated at 80% or higher*

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

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

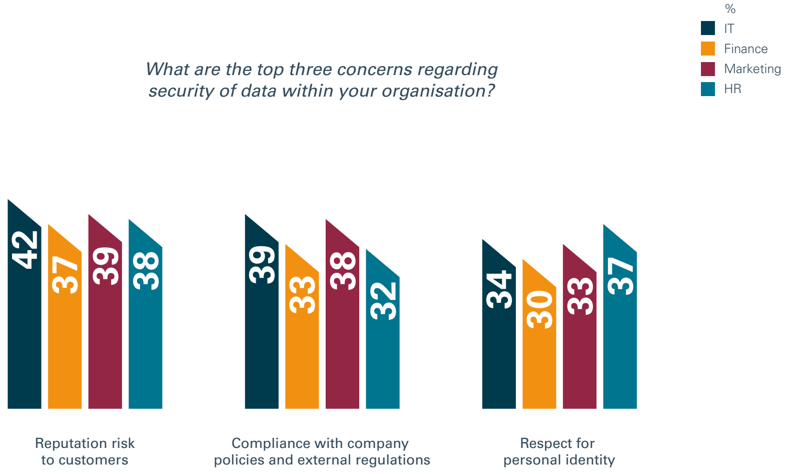
Top three concerns

Protecting company reputation is a top concern across departments. However, protecting personal identities is more highly prioritised among HR teams. HR leaders value reputation risk in front of the customer almost equal to respect for personal identity. Compliance comes in third in their list of concerns.

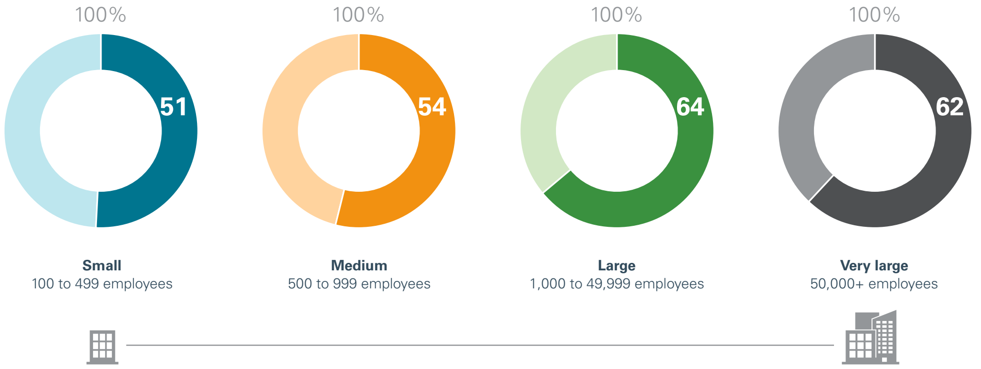
Importance by size of organisation

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?



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



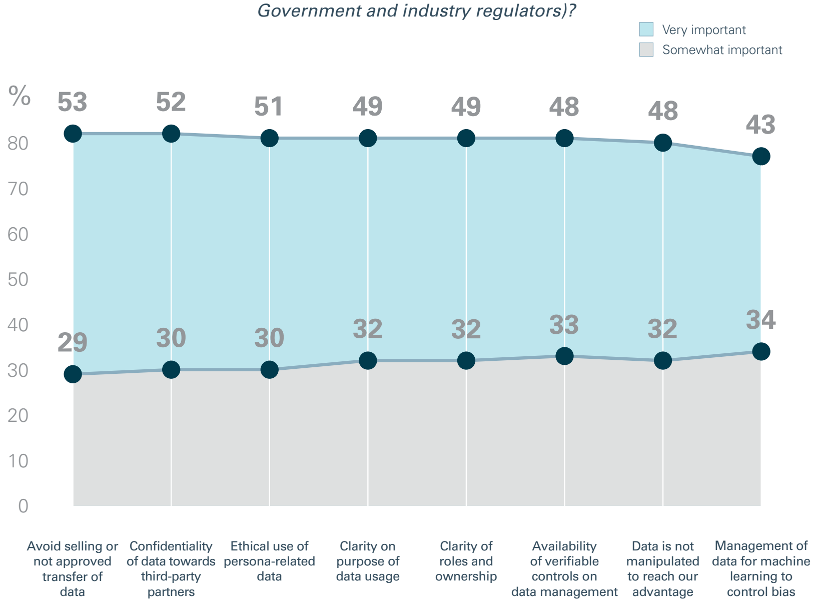
Base: Global population, 24 markets, nr. 5,539

Reputation – Trust and benefits

Trust across audiences

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

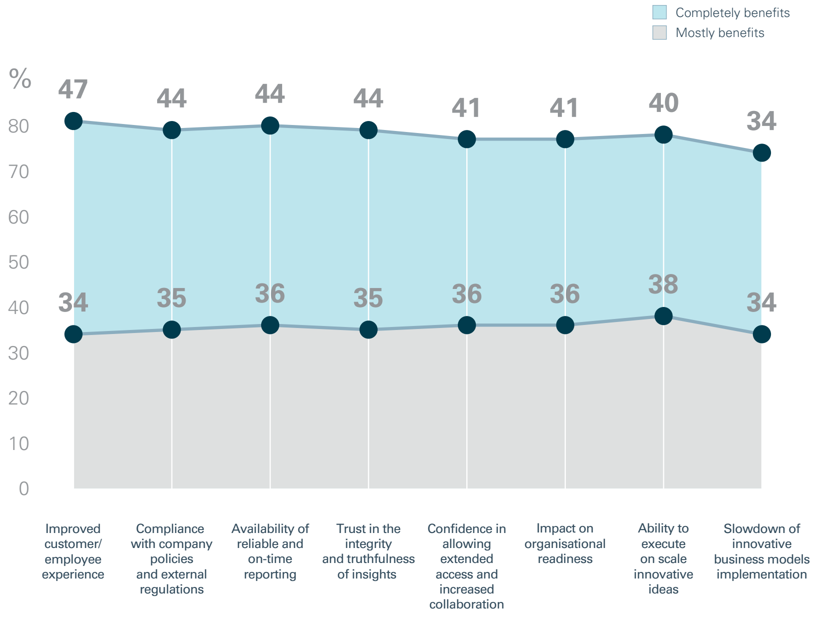
How important are the following factors in allowing your organisation to achieve trust with its audiences (customers/employees/managers/ Government and industry regulators)?



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.

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



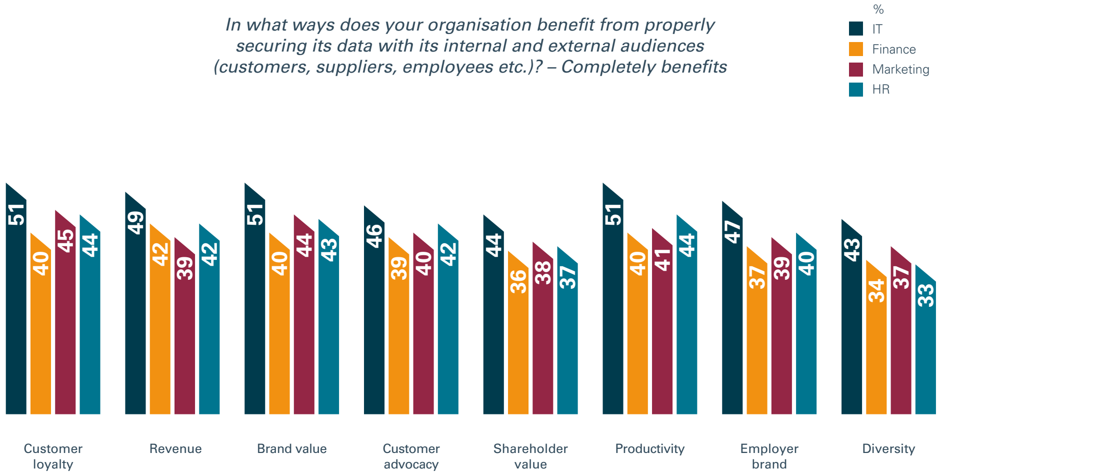
Base: Global population, 24 markets, nr. 5,539

Reputation – Internal/external audiences

Benefits by line of business

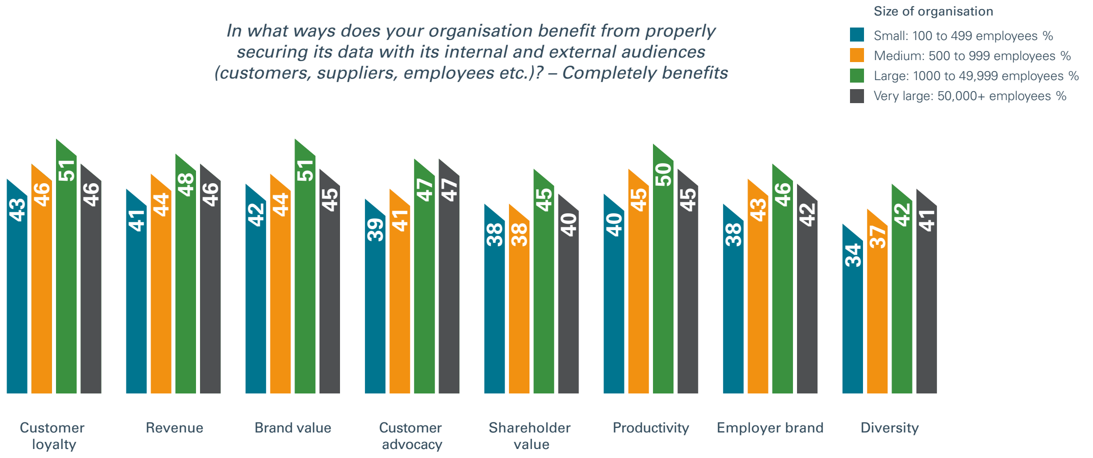
When it comes to the benefits of properly securing data, organisations recognise that gains were to be had from an improved customer/employee experience, along with the peace of mind in being compliant – the availability of reliable reporting is also considered as a plus.

Across all lines of business, IT was most likely to appreciate the gains to be had by the secure use of data, finance had the least appreciation of the potential.


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

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

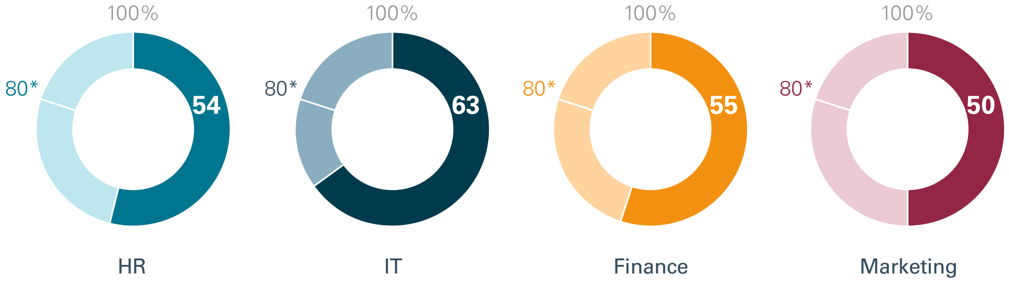
Base: Global population, 24 markets, nr. 5,539

Secure management of data

Employer branding is becoming as prevalent as organisation and product branding, and plays a far larger role than ever in attracting and retaining talent. Factors such as the perception of how data is managed has a direct impact on brand equity in the digital economy. However, more than half of HR leaders strongly believe that the way they manage data has an impact on the reputation of their organisation.

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.

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



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.

Next steps

A summary of next steps
and recommendations

It is a positive sign that CHROs, alongside all lines of business, place in their top three priorities enhancing security controls and procedures, and promote awareness and education to threats. **Most reassuring however is that HR is focused on internal education and awareness of threats.**

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

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

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

- **Work across the entire organisation** to put in place a data management strategy with common protocols
- **Educate employees** to ensure that threats are understood and common protocols are implemented and effectively monitored
- **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
- **Encourage autonomous technologies** where possible to relieve the burden of security and compliance, and improve confidence levels
- **Hire the right talent for the digital-age – competencies such as analytical thinking, creative problem solving and adaptability are skills for the agile organisation**

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

Oracle Cloud

ORACLE® Cloud