Building trust in your information and security

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

Your Tomorrow, **Today**

ORACLE Cloud

Methodology

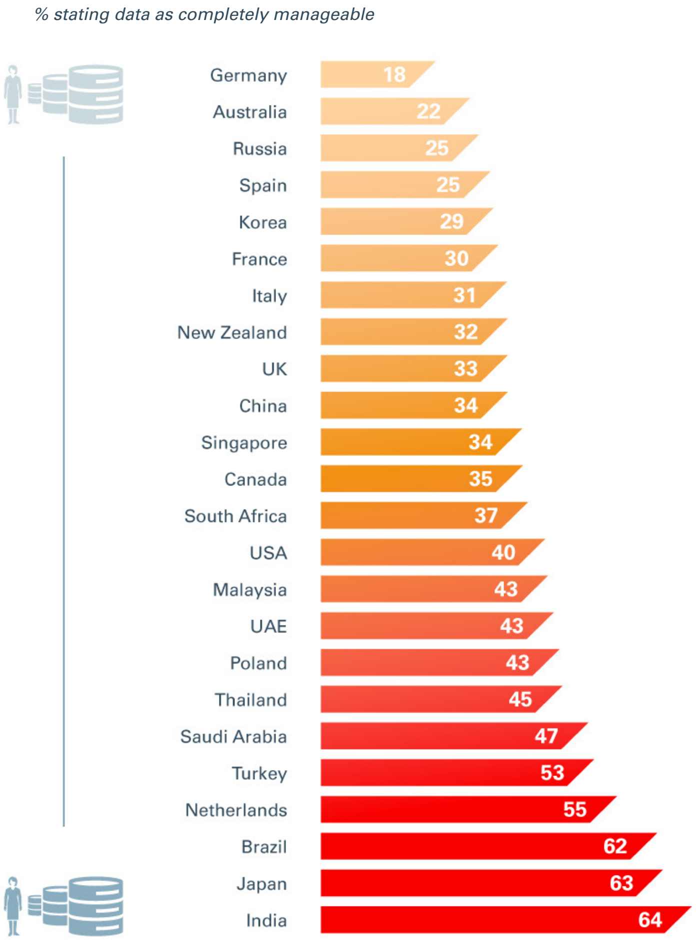
The results presented in this report are based on a mobile-only, 23-question global survey. This survey targeted Manager, Director, Vice President or C-Level executives with influence in the decision-making process of cloud solutions, platforms, and infrastructure or department specific software. Respondents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

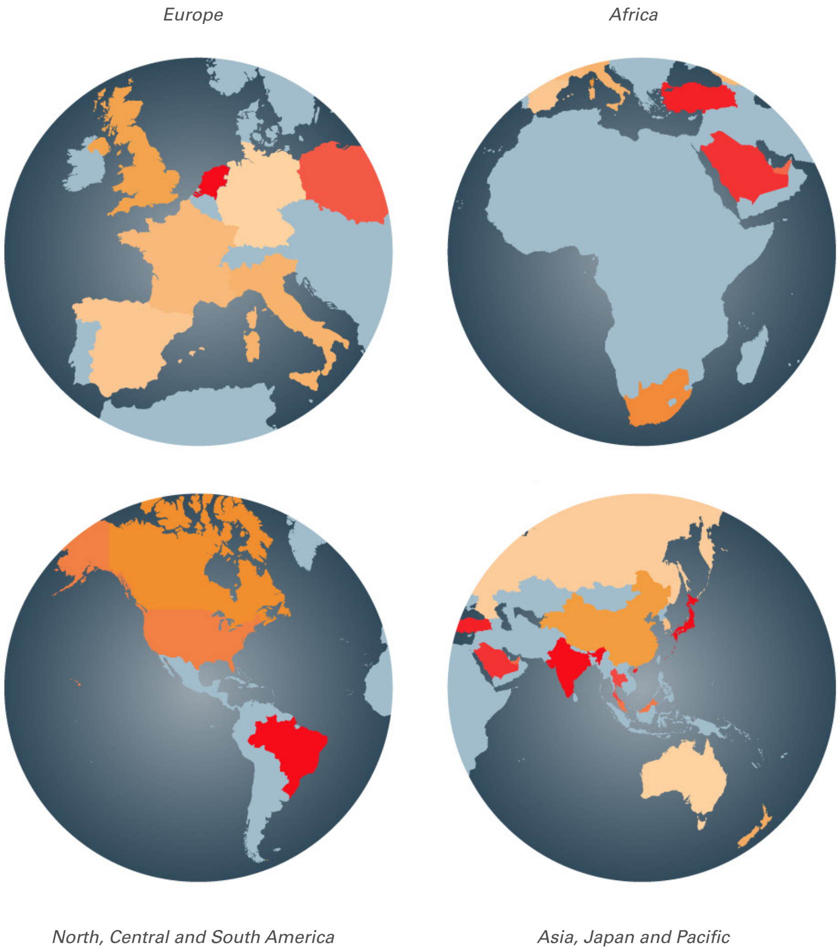
Contents

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

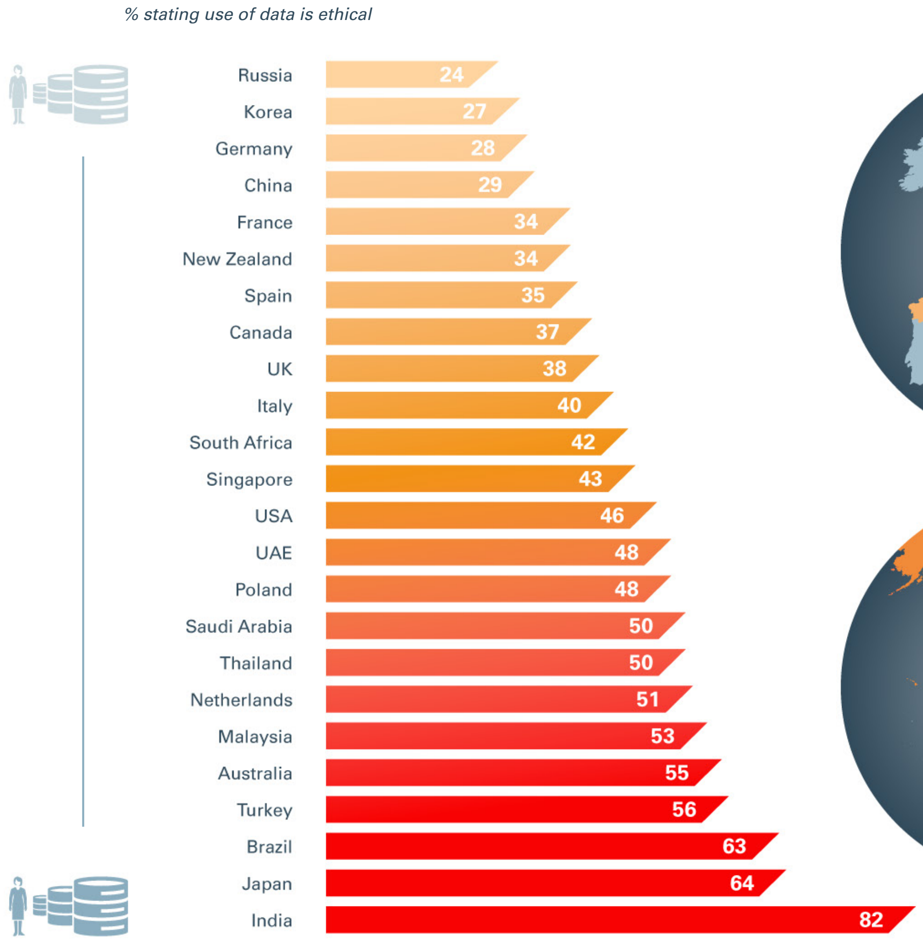


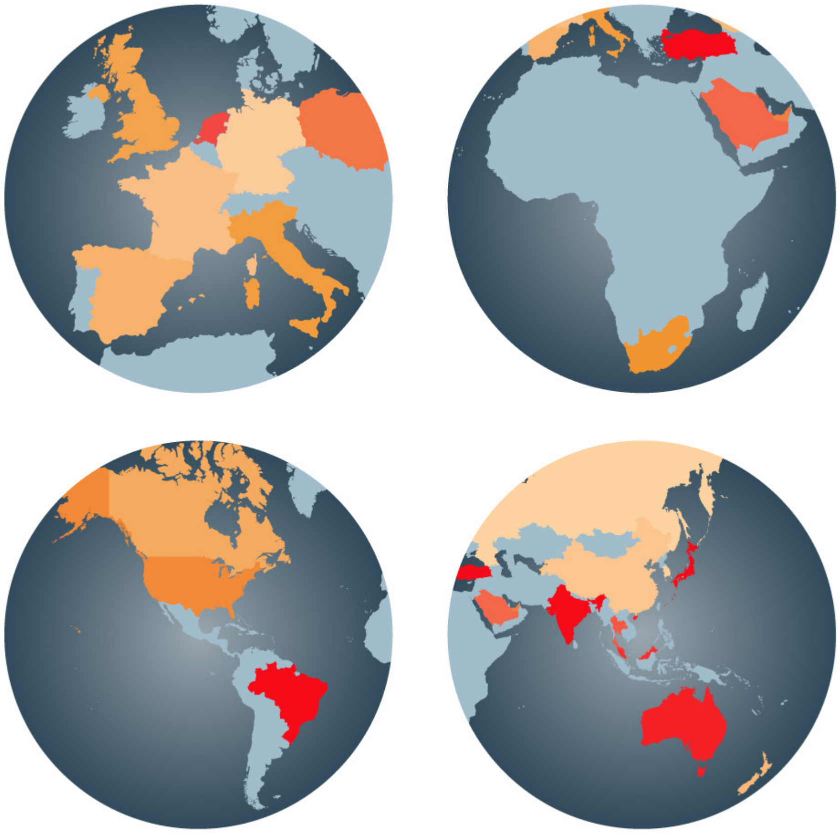


Perhaps of greater sensitivity – who tells us they are most confident that their use of data is ethical? Decision makers in **Russia score themselves the lowest alongside Korea, Germany and China** – whilst again India, Japan and Brazil hold themselves in high regard. Coincidence, or is there a cause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





Europe

Africa

North, Central and South America

Asia, Japan and Pacific

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:

- **IT leaders believe data management is a burden on businesses:** Less than 50% of IT leaders consider themselves to be highly confident in their ability to manage data. Though this percentage is low, this result comes in higher than any other line of business.

- **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, accept accountability for their data, and a further third take responsibility for key actions only. While IT leads the way in this respect, significant improvements must be made. Critically all actions should start with defining which line of business(es) should take accountability.

- **Security is a concern for all:** Only 47% of IT leaders are highly confident in their security of the data their organisation holds – ahead of other parts of the business, but still some way short of where we would expect this to be.

- **63% of IT leaders, compared to only 58% of total decision makers, agreed 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 42% of IT leaders, and 39% of respondents globally, are highly confident that their organisation can manage data to generate meaningful insights. Not surprisingly, 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.

- **Only 49% of IT leaders are highly confident in their organisation's ethical use of data:** Despite the fact that ethics and the responsible use of data have a direct impact on reputation and trust, just under one-fifth of respondents overall are not confident at all.

- **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.

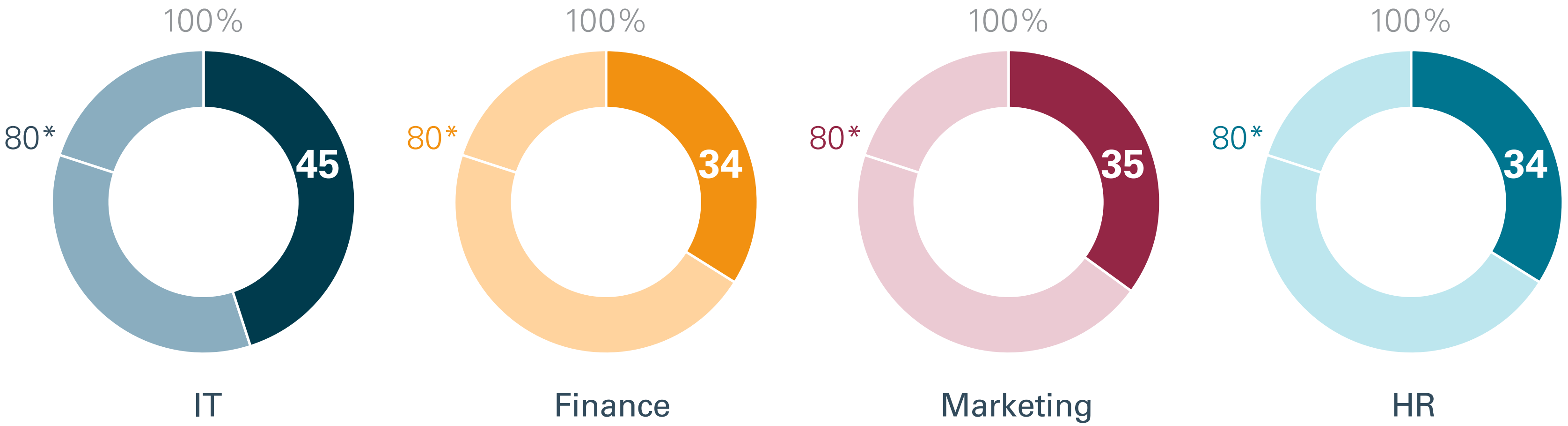
Data management

Ensuring quality to deliver greater value

Only 45% of IT 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.

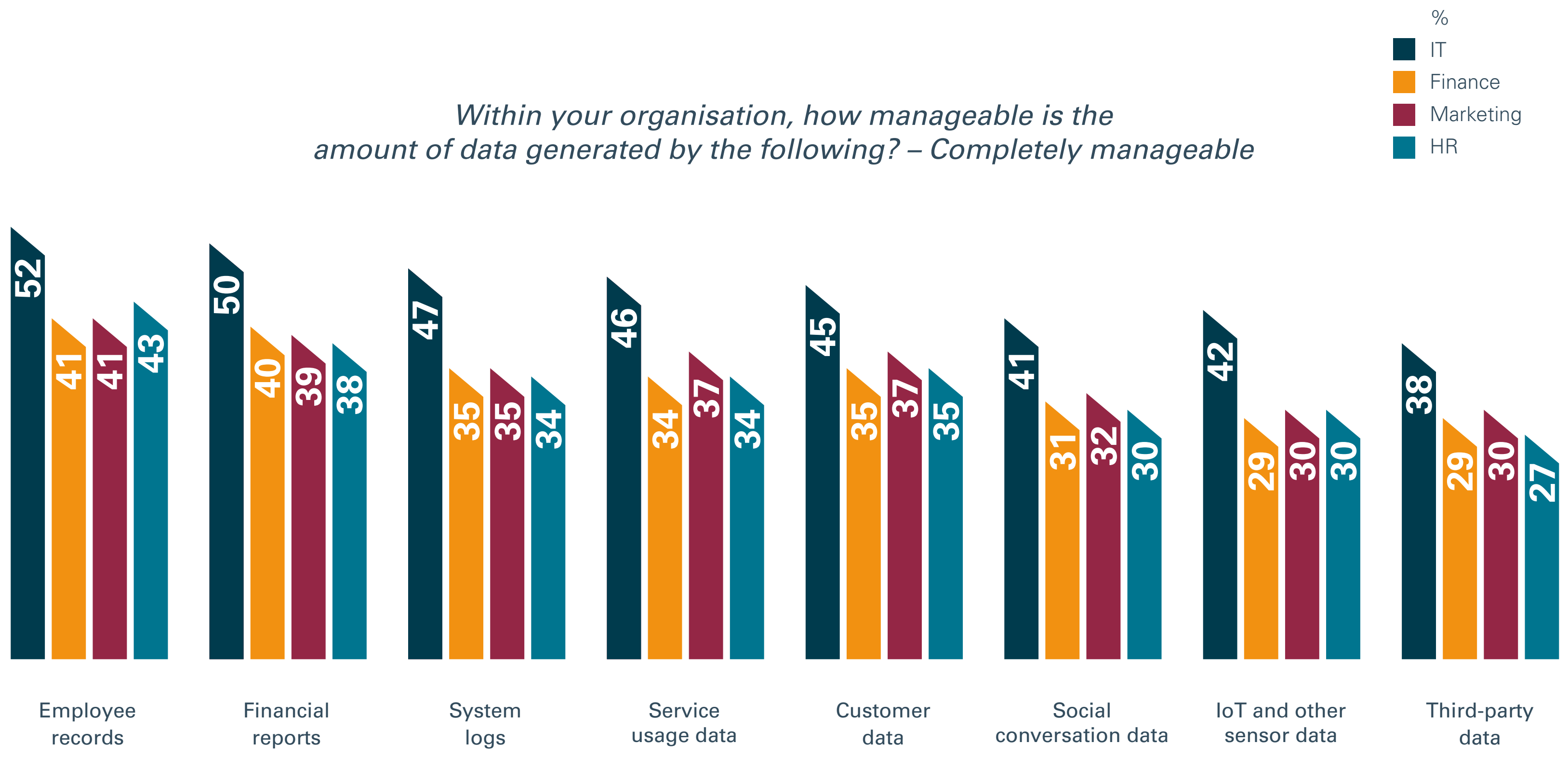
In the past, data was typically informed historical reporting, with internal needs and compliance taking priority. Today, finance leaders require far more external data for security, predictive thinking, and to innovate for the future. Compliance and risk management are still key, but the field of data 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 business models: both B2B to B2C. This creates a tidal wave of new data; customer data, people data, sales data and product data – just to name a few. Organisations are now trying to catch up with storing, analysing, advising, staying compliant and gaining and keeping consumer trust. As well as trust, there is the question of accuracy for CEO, 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. CIOs need the support of technology to effectively monitor and manage the organisation's digital use, and therefore manage risk.

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.

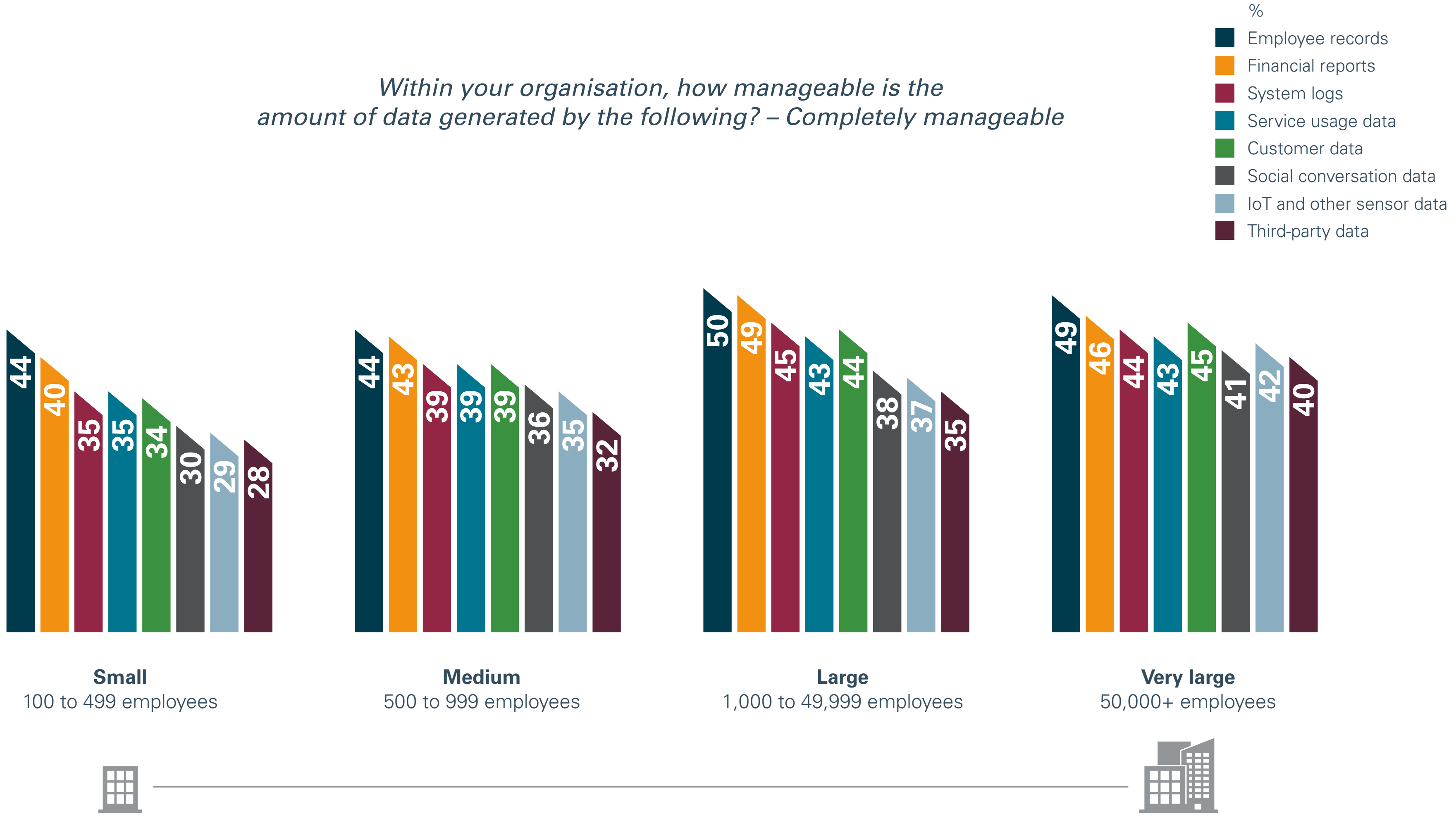


Within your organisation, how manageable is the amount of data generated by the following? – Completely manageable

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

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

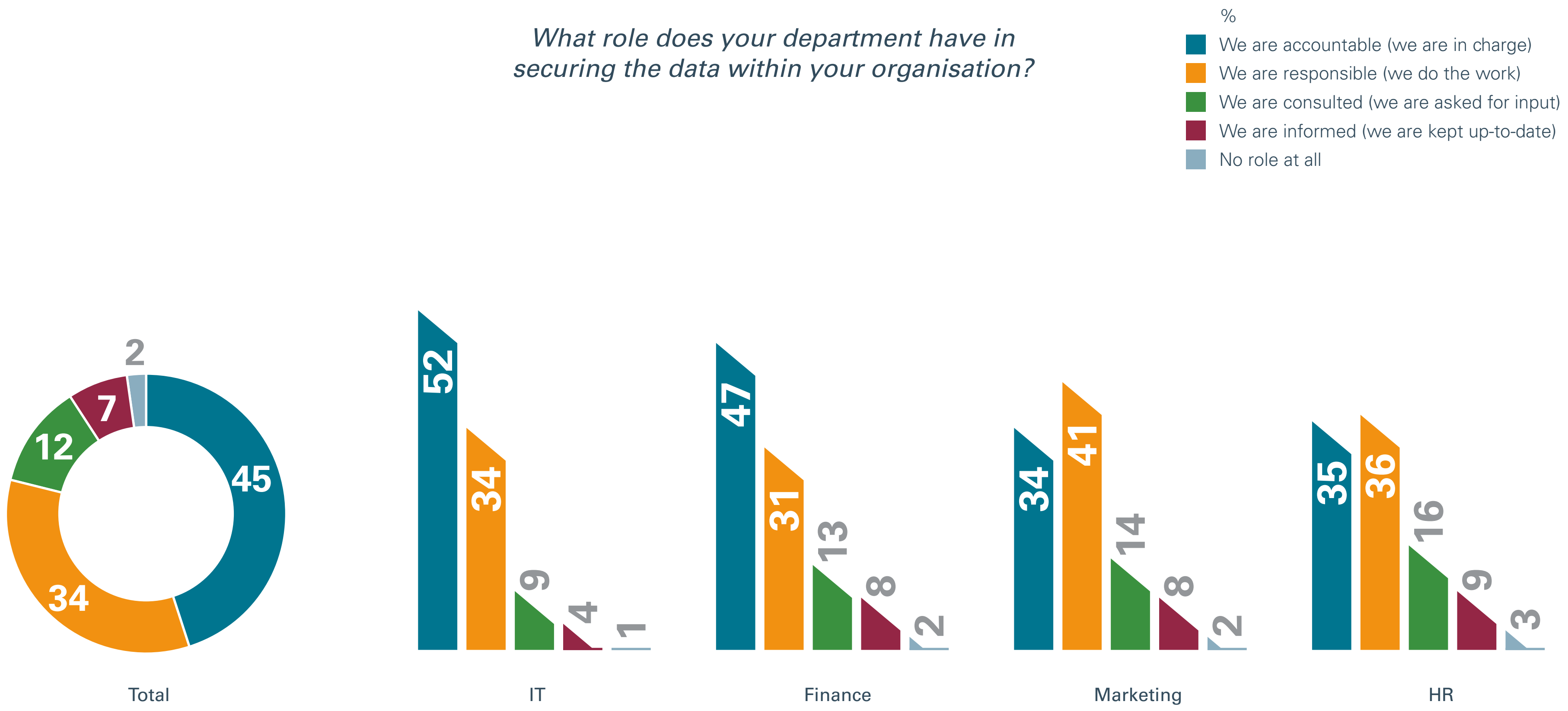
Data generated by routine tasks are considered the most commonly manageable, but capability drops with company size when data is derived from third-party needs or newer technologies.



%	Small (100 to 499 employees)	Medium (500 to 999 employees)	Large (1,000 to 49,999 employees)	Very large (50,000+ employees)
Employee records	44	44	50	49
Financial reports	40	43	49	46
System logs	35	39	45	44
Service usage data	35	39	43	43
Customer data	34	39	44	45
Social conversation data	30	36	38	41
IoT and other sensor data	29	35	37	42
Third-party data	28	32	35	40

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 – marketing and HR – are taking less accountability.

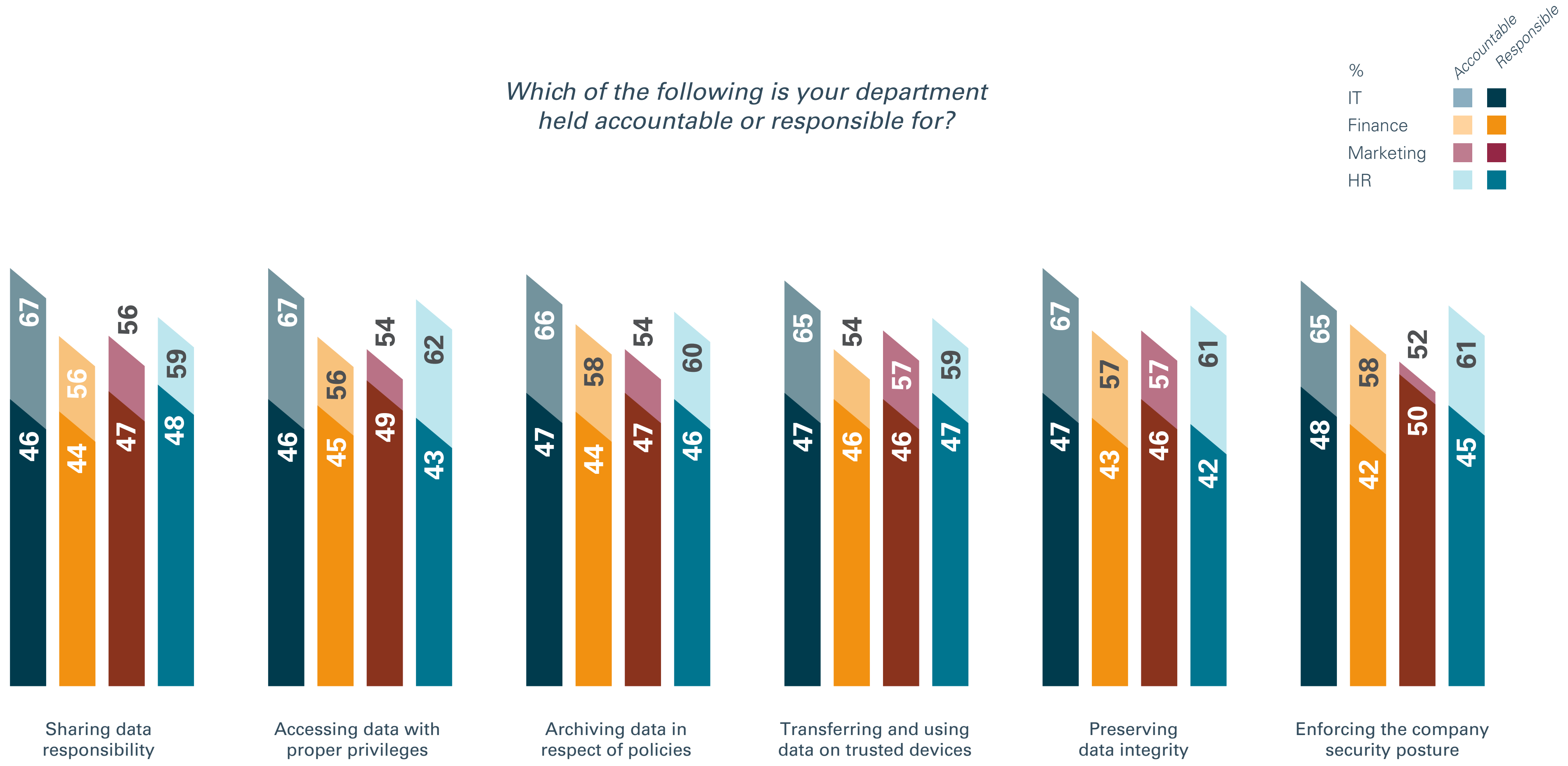


Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

When prompted to consider taking specific actions, respondents in every department believe they are accountable – **especially IT**.

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



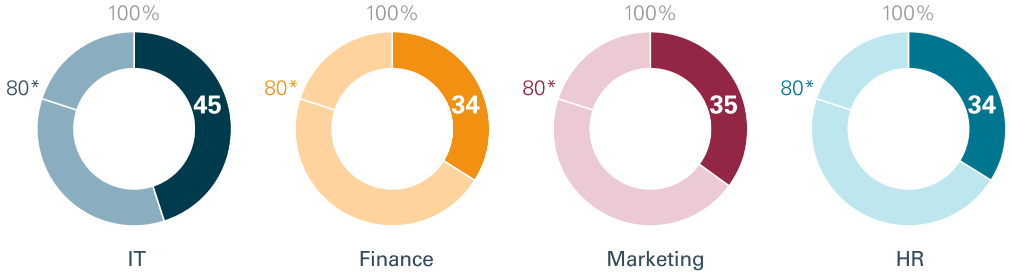
Base: Global population, 24 markets, nr. 5,539

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 45% of IT leaders, and less than 50% across all business leaders and all forms of data, believe their data to be completely manageable.

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



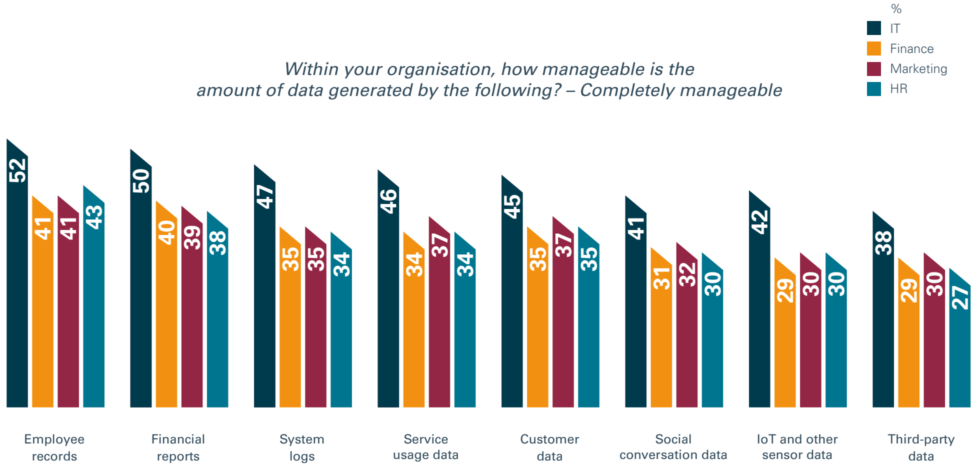
The source of the issue?

Our research finds that only 38% to 52% of IT leaders across various sources believe that data is highly manageable. While IT comes ahead of other departments, it is concerning that this response from IT is still low. After all, data collection, management, and security has fallen into their wheelhouse for many years.

This means, at best, half of the value that insights and analysis data could offer goes untapped. No line of business, including IT, 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 by the following? – Completely manageable



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.

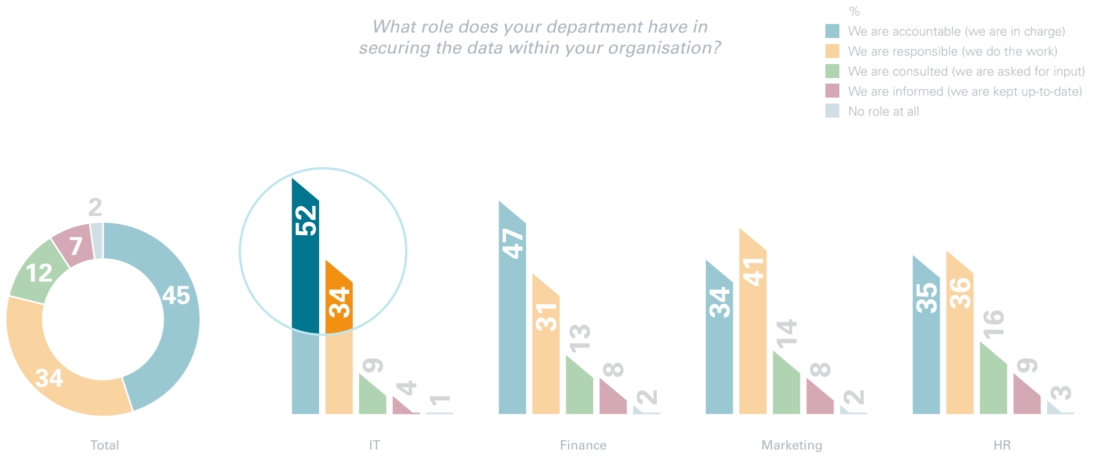
However, with the advent of the cloud, the importance of data to business success, combined with new regulations, means more accountability needs to be accepted across all lines of business.

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 as well.

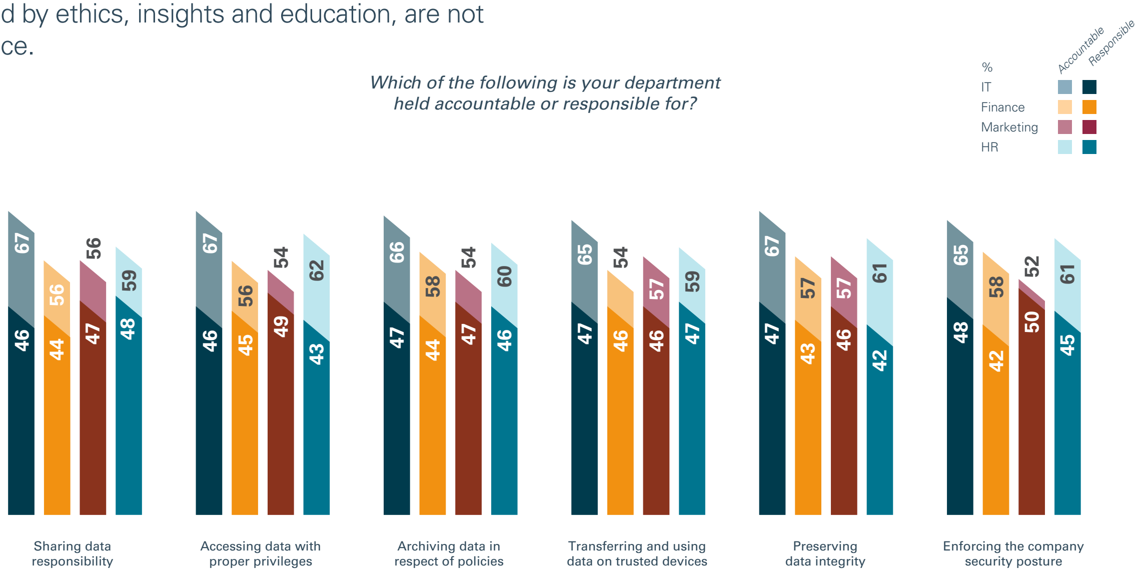
The data shows that marketing and HR do not understand how their roles are changing and that accountability, as well as responsibility, must shift. The old mindset has been ‘we use the data, but IT owns it.’ This is no longer the case; and yet organisations are struggling to keep up.

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



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.

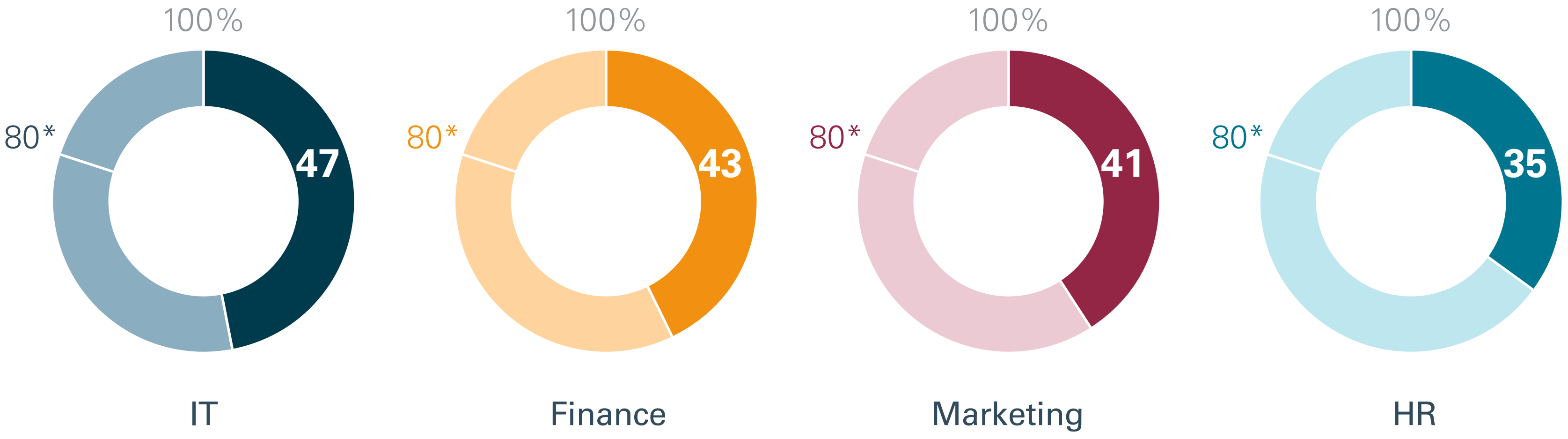
Which of the following is your department held accountable or responsible for?



Less than 50% of IT 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

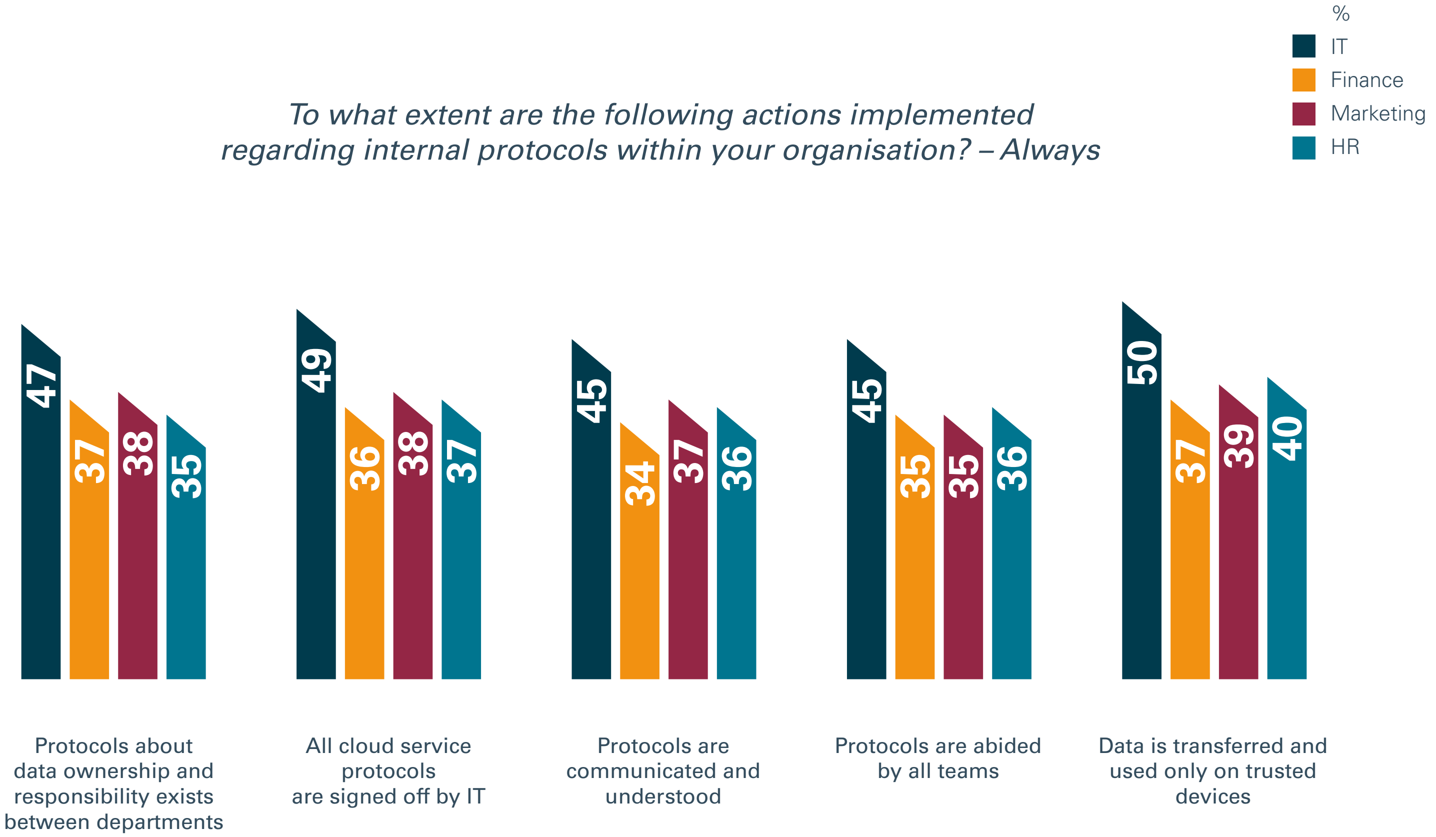
** Reasonable expectation estimated at 80% or higher*



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

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 other departments are 10% points or more behind.**

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

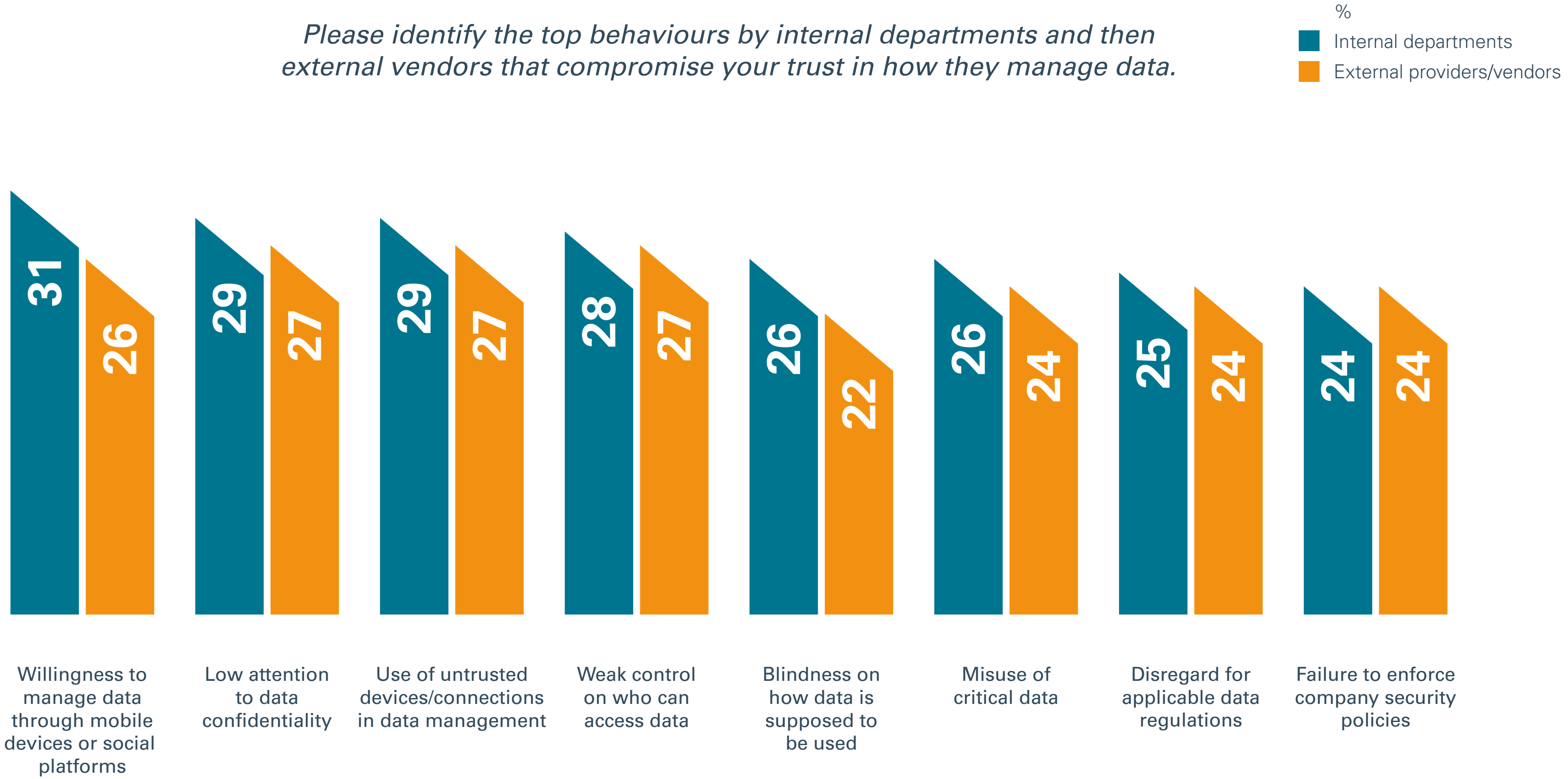


Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

So what keeps us awake at night? The use of both mobile/social platforms and untrusted devices, as well as low attention to data confidentiality, 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: IT population, 24 markets, nr. 2,806

Security confidence

As is the case with the ability to manage data, the bar should be set high in this respect.

However, only 47% of IT 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.

It's a team game

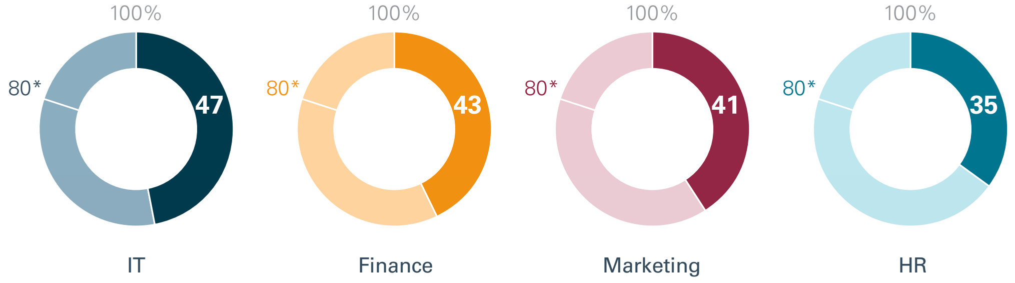
Why aren't respondents feeling more confident in the security of their data? We suggest this relates, at least in part, to internal protocols – or the lack thereof – implemented within the organisation. Less than half of respondents believe that critical actions are being fully implemented within their 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 45% of IT leaders believing that security protocols are abided by all the time. Given these findings, it is no surprise that IT leaders are not highly confident in the security of their data.

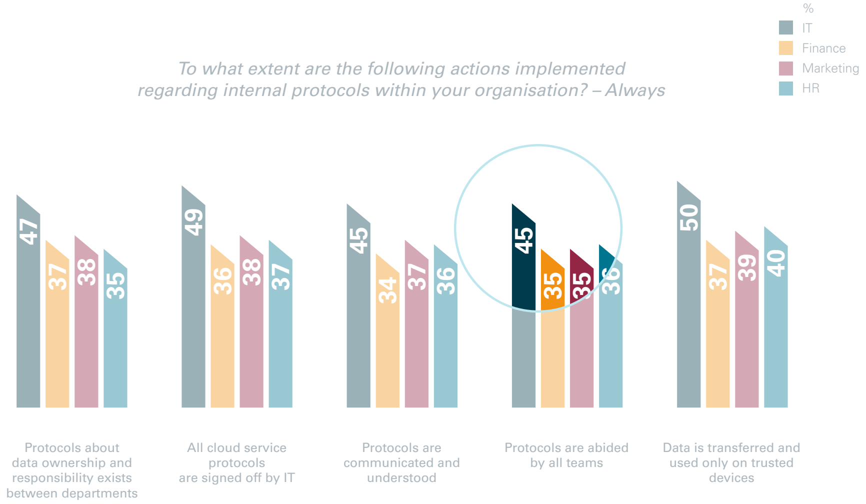
19% of total decision makers state that protocols are abided by sometimes, rarely, or never. Such findings prove that organisations are currently open to threat due to the identified practices of their own people.

However – this isn't just about which departments are taking action on their own. The solution lies in organisations creating common protocols supported by cross-functional team 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



ORACLE Cloud

Try Oracle Cloud today

Data management – Analysis (cont.)

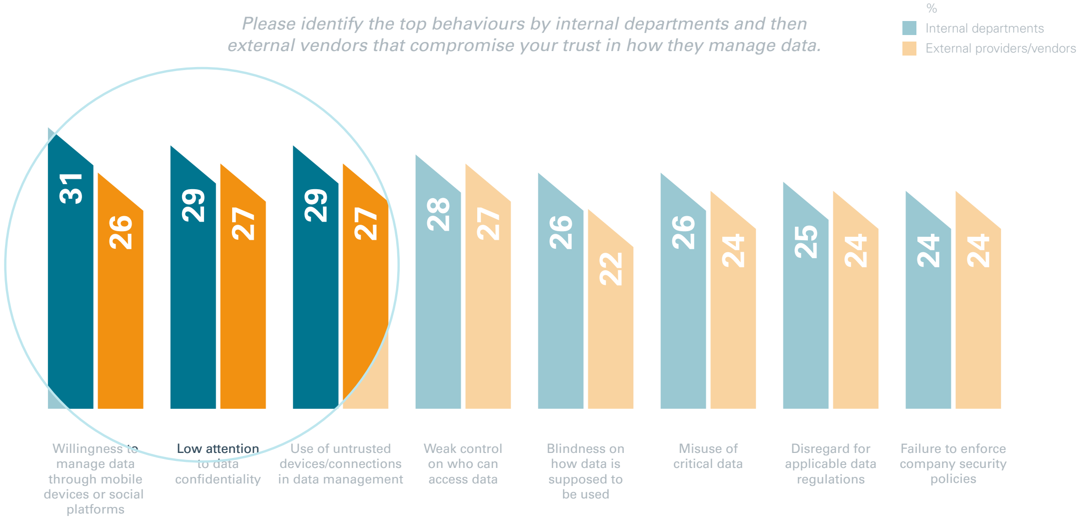
The pain points

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’ (31%), ‘Low attention to data confidentiality’ (29%), and ‘Use of untrusted devices and connections’ (29%).

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 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.



- **Responsible use and management of data are key elements of a digital economy:** CIOs need the support of technology to effectively monitor and manage the organisation's digital use, and therefore manage risk. If we want them to take full accountability and responsibility for data security, we need to free up their time so they 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.

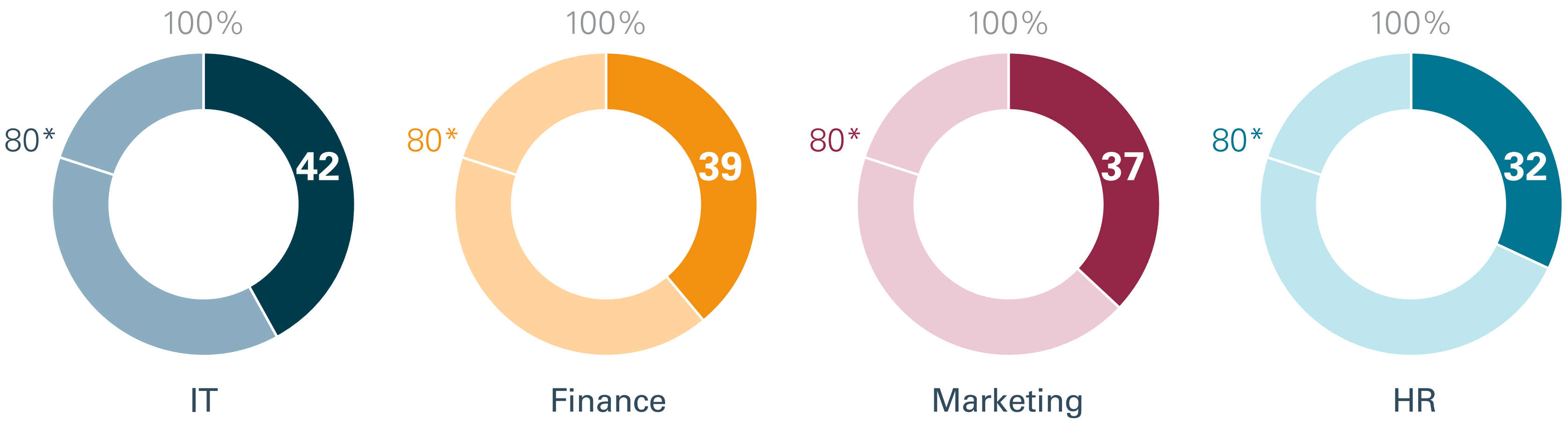
- **Good data management practice requires basic protocols to reduce uncertainty and make it manageable, and 'managed.'** Admittedly, data strategies are somewhat new; protocols therefore need to catch up with the new reality and be enforced within all lines of business. The concept is that a common 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 42% of IT 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

The real issue with data is one of quality not quantity. So although 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.

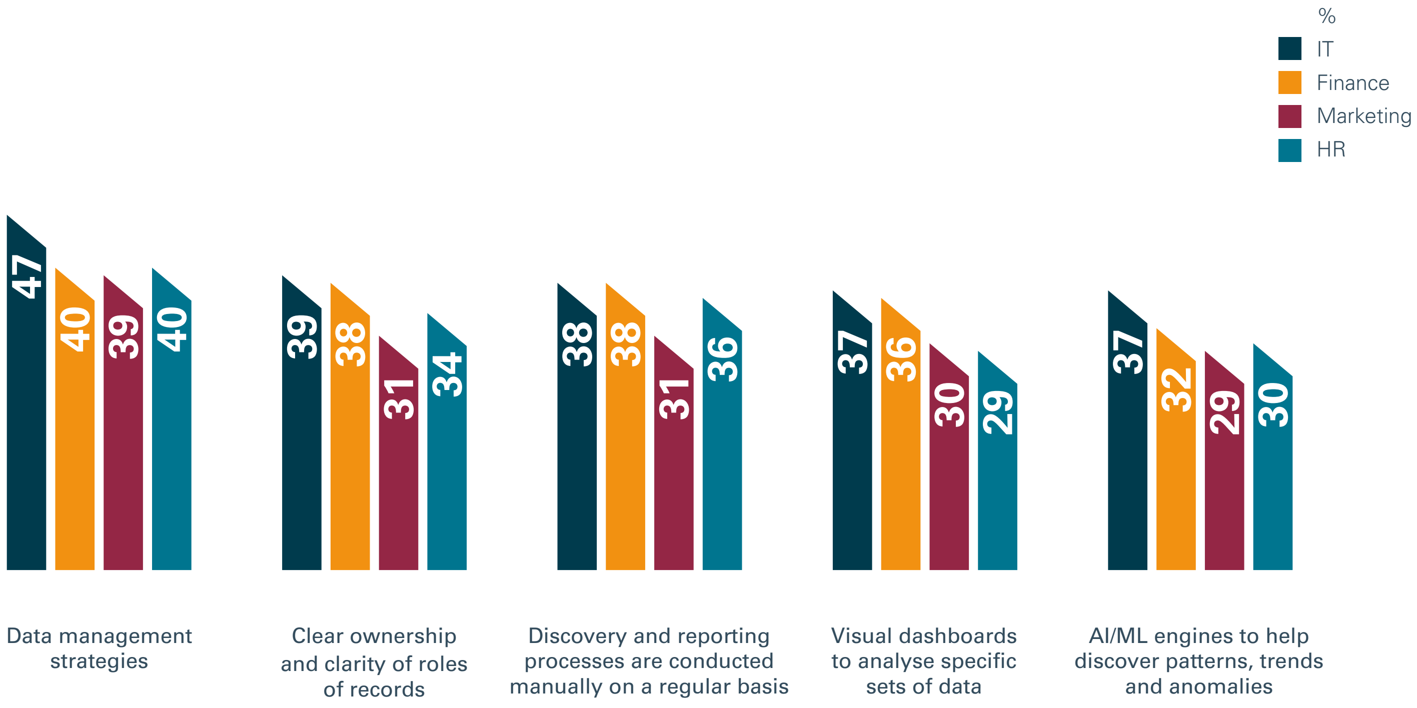
The key questions that the C-suite team are asking: Are organisations able to generate maximum insight from the deluge of financial data? Is this trustworthy? Is this 'data' or 'insight'?

To ensure the survival of their business and secure growth, companies have considerably shifted their models: as a priority that focus was translated into products, commercial propositions and customers', experiences – 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 tasks. At the moment many functions are focused on historical reporting only, with little or no forward-looking modelling taking place. There is a lack of measurement of the value created. It can put in place the technology platforms to enable business to see and measure their progress and value.

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.

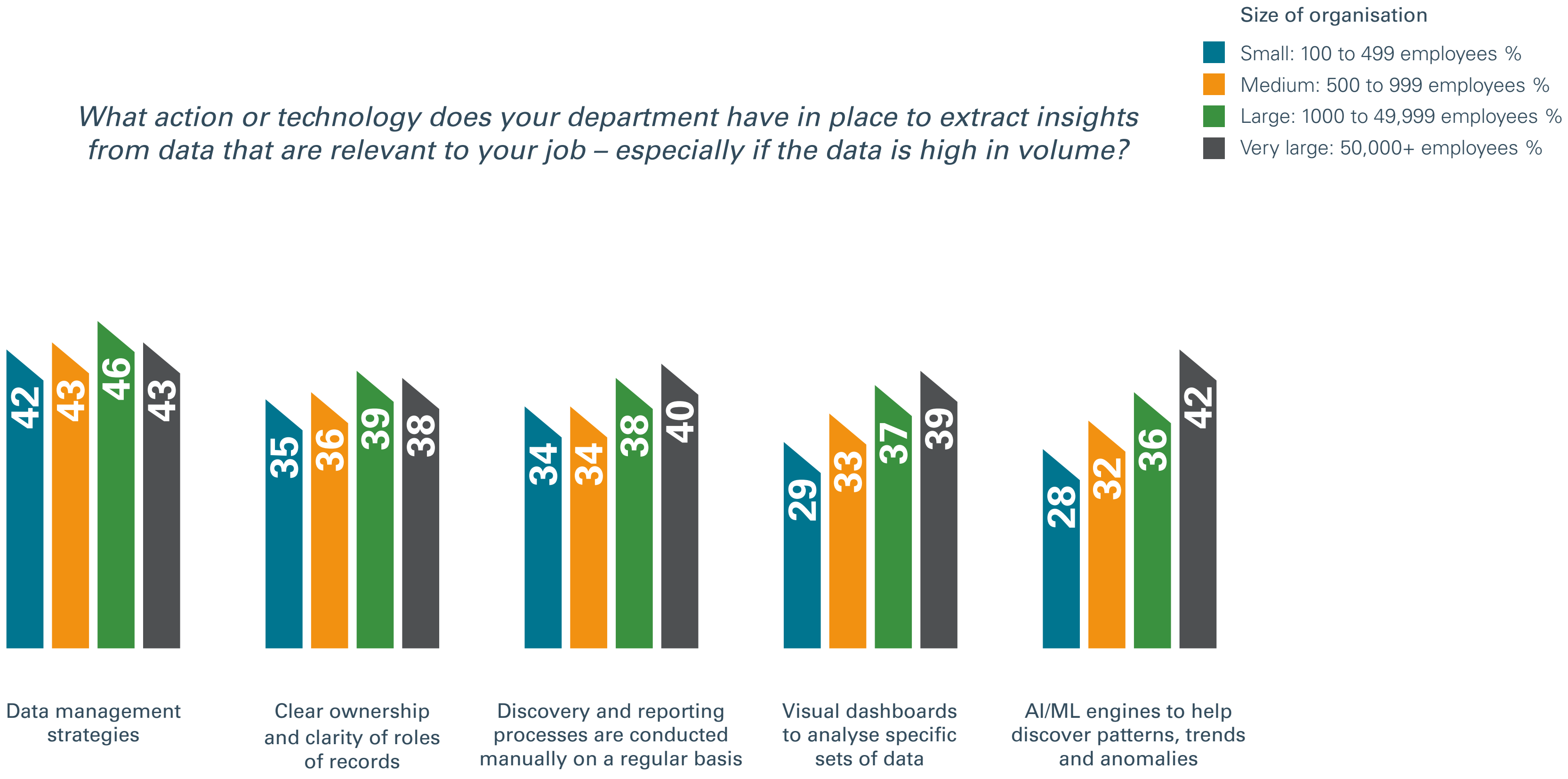
What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?



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

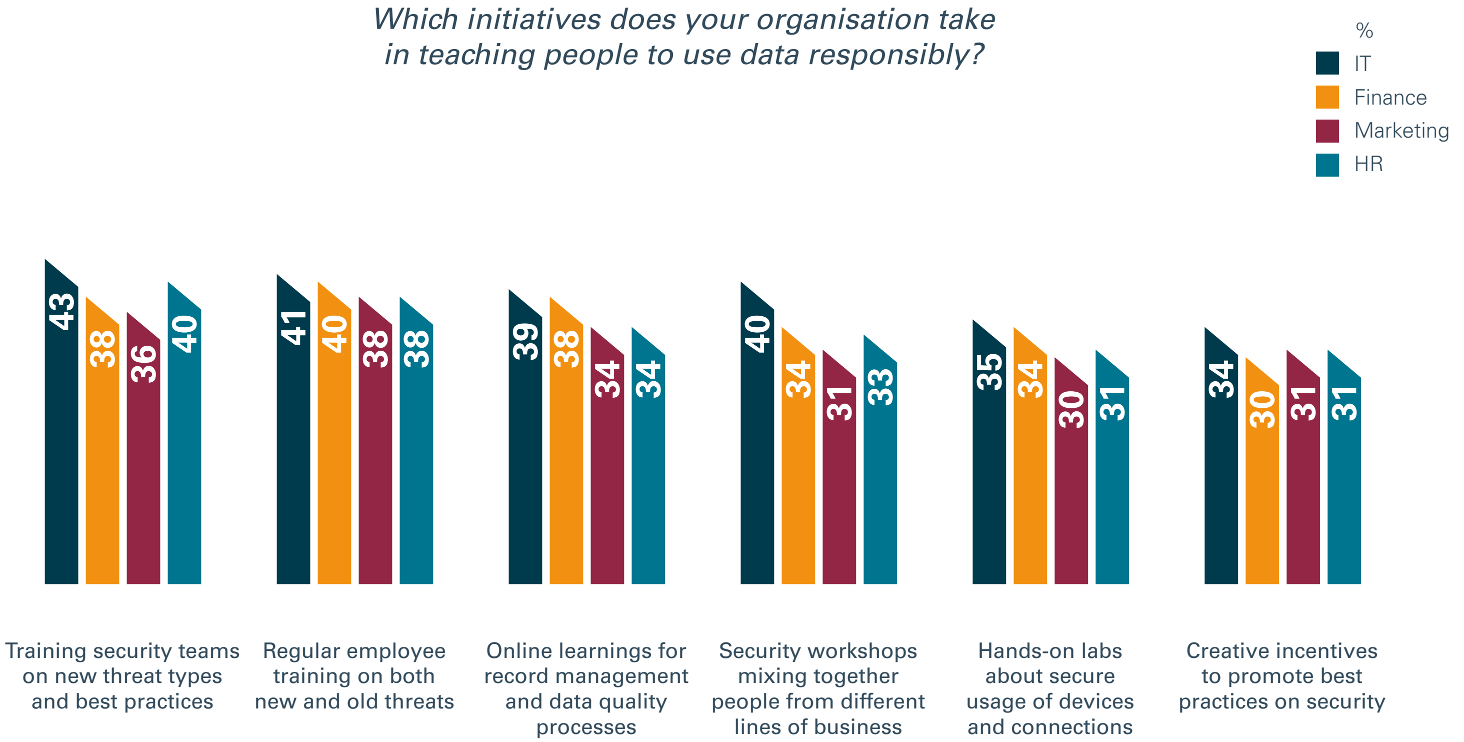
Organisations of all sizes are putting strategies in place to improve data management, **but taking key actions lessens with company size**.

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?



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**.



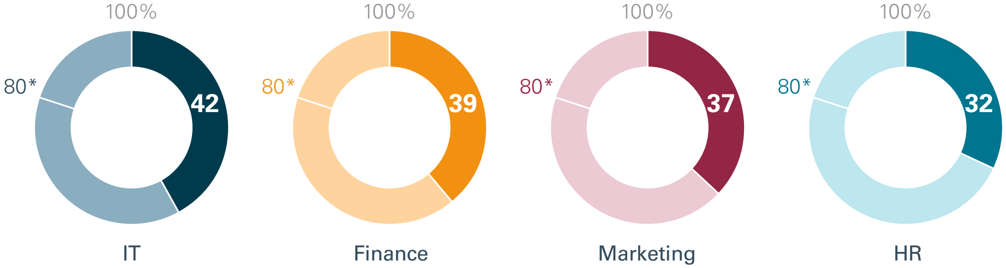
%	IT	Finance	Marketing	HR
Training security teams on new threat types and best practices	43	38	36	40
Regular employee training on both new and old threats	41	40	38	38
Online learnings for record management and data quality processes	39	38	34	34
Security workshops mixing together people from different 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

Seeing the value

Only 42% of IT leaders are highly confident in their organisation's ability to manage data to generate meaningful 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



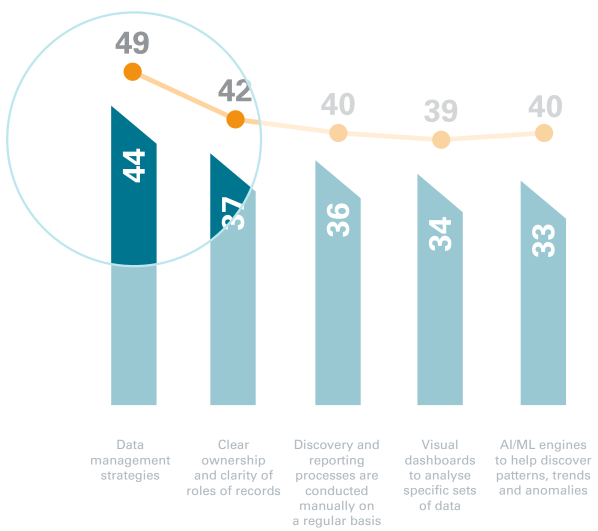
Accountability also leads to stronger data strategies

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.

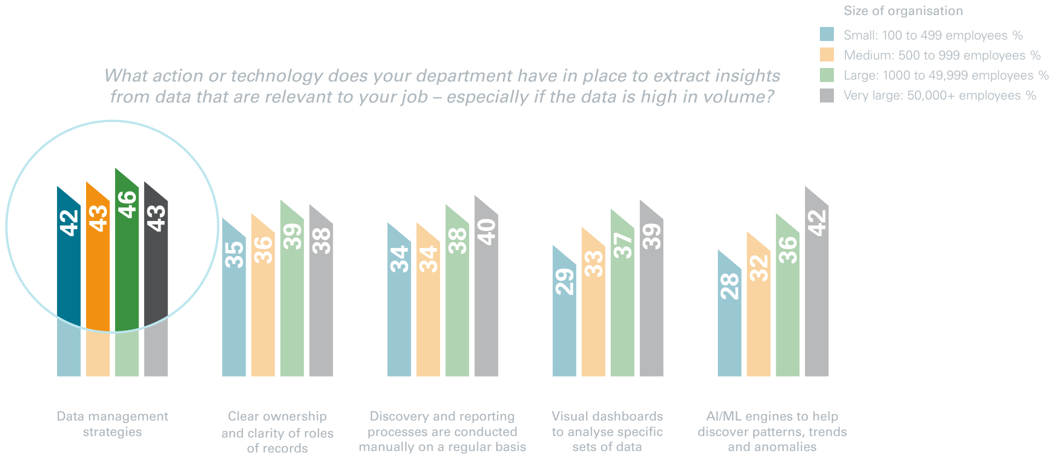
What action or technology does your department have in place to extract insights from data that are relevant to your job – especially if the data is high in volume?



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.

However, these insights are only valuable if the organisation can trust in its accuracy; only then can these insights support decision making. Predictive decision making, a key differentiator with ML/AI, can aid in more accurate projections with built-in machine learning capabilities, thus contributing to trust.



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?

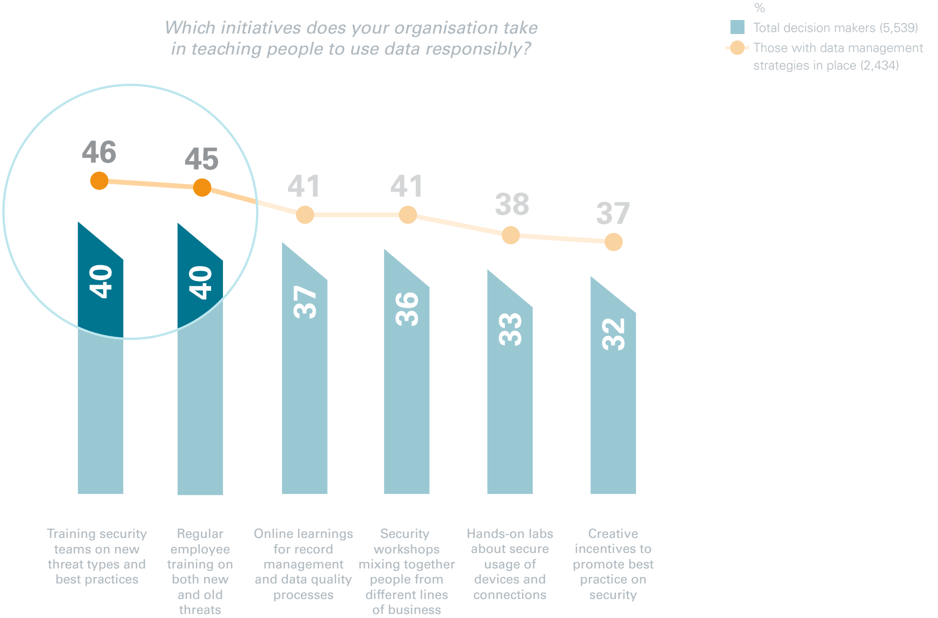
Education for all

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.

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. CIOs need to support HR 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 CIOs 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 across the entire organisation:** Therefore, an important consideration is measuring IT performance with well-aligned metrics and data that all business leaders can understand. Conversely IT needs to use data and metrics that are meaningful to business leaders.

- **Data is the thread that ties all the lines of business and IT functions together:** 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 becomes more essential than ever. The increasing interest and focus across the board are twofold: ethical data usage and data-driven business models.

- **Traditional monitoring and problem-solving approaches are inadequate.** In the massively scaled and complex infrastructure that supports large digital businesses, the only viable solution is to apply analytics to the growing volumes of data to find hidden insights that help keep IT infrastructure and applications humming. Taking ownership of these opportunities starts with taking accountability. Those that accept accountability for data management are more likely to have put a data management strategy in place. From here, best practice and greater compliance to internal protocols can start to take effect and stronger insights can be drawn.

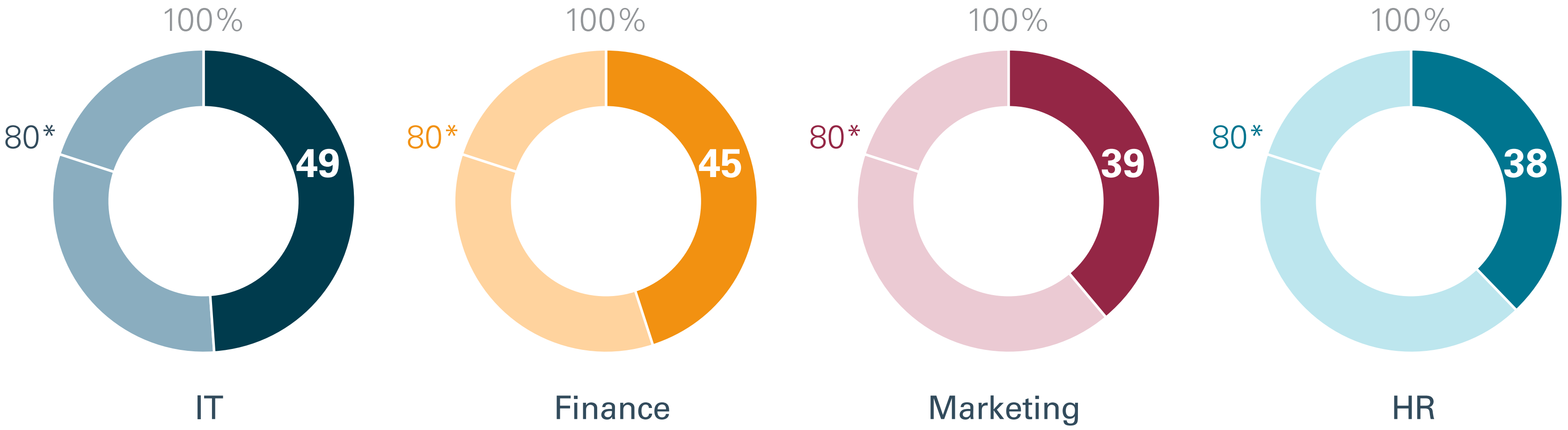
Ethics

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; although IT respondents were the highest at 49%, **this still leaves over half of IT leaders who were not highly confident**.

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

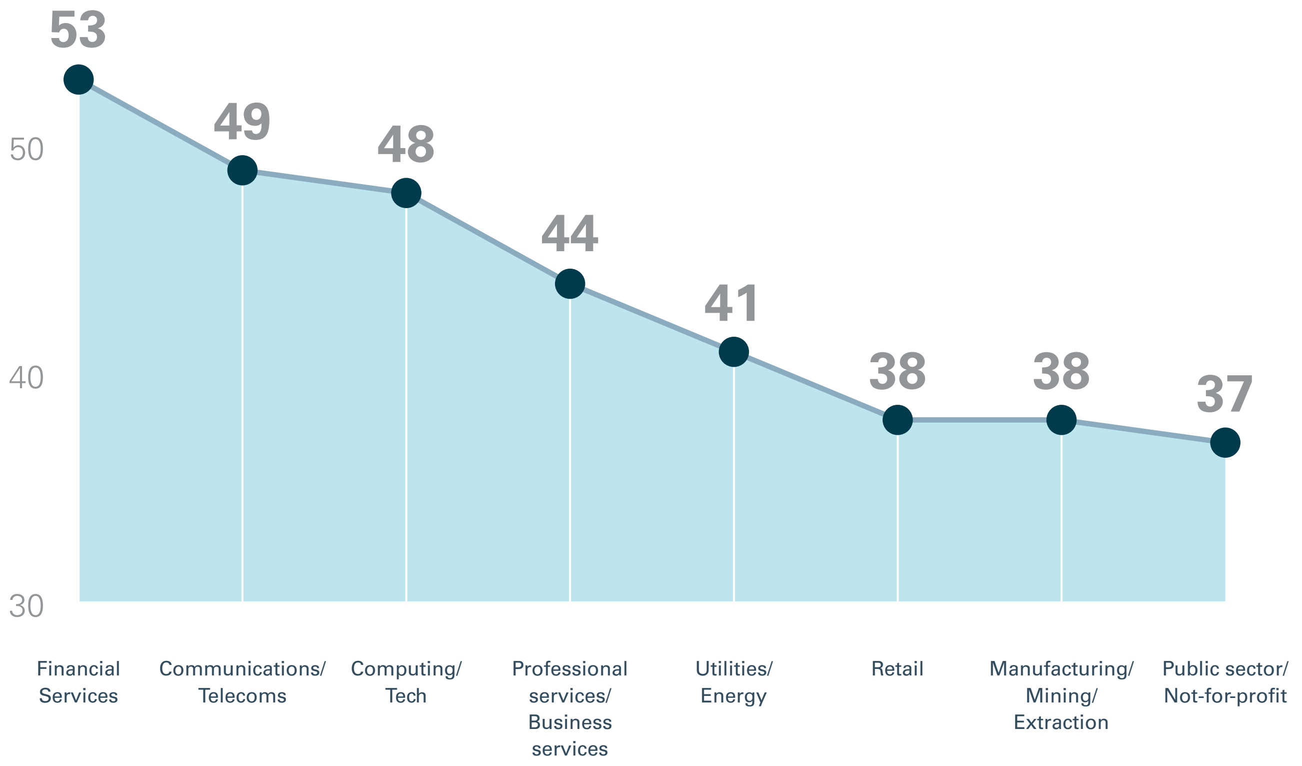
An ethical mindset is a pre-requisite in today's digital and social economies. As organisations seek to generate maximum value from the deluge of customer, market and sales data, CIOs have a key role to play. They must work hand in hand with the commercial teams to ensure that the data they process is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

A key consideration for finance leaders is how to ensure that data is being used ethically whilst delivering the experiential programmes that customers are prioritising. Ethical usage of customers and data is strongly tied to that 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 uneasy if you demonstrate that you know too much about them. Keeping that balance right is crucial.

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

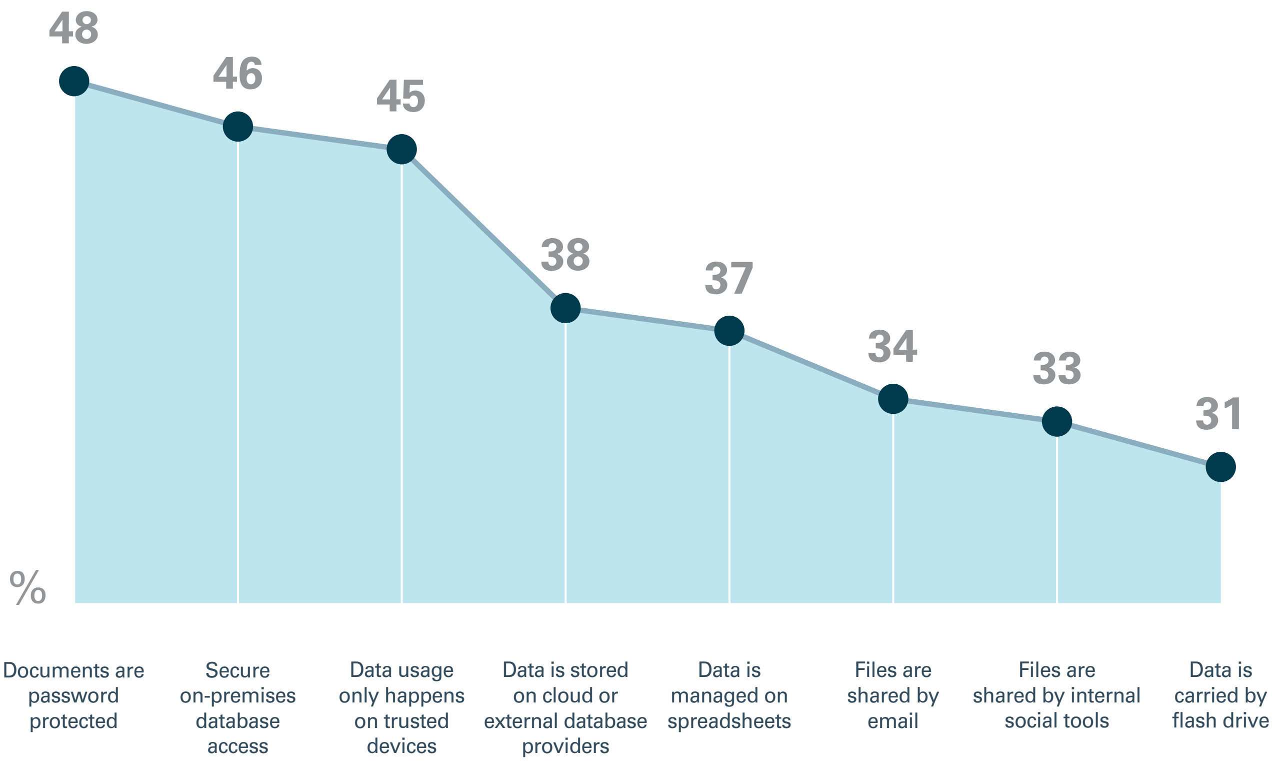


Base: Global population, 24 markets, nr. 5,539

Try Oracle Cloud today

Good practice has improved and critical data 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

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.

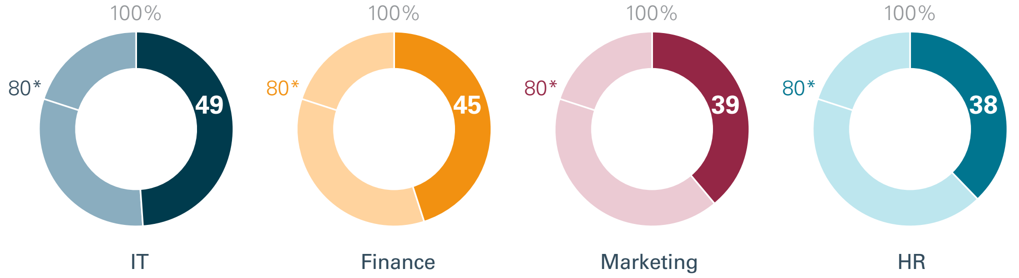
While the precise definition of 'ethical use' is complex, we had expected this percentage to be much higher. IT again scores highest (49%) – 10 percentage points above both marketing and HR departments.

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.

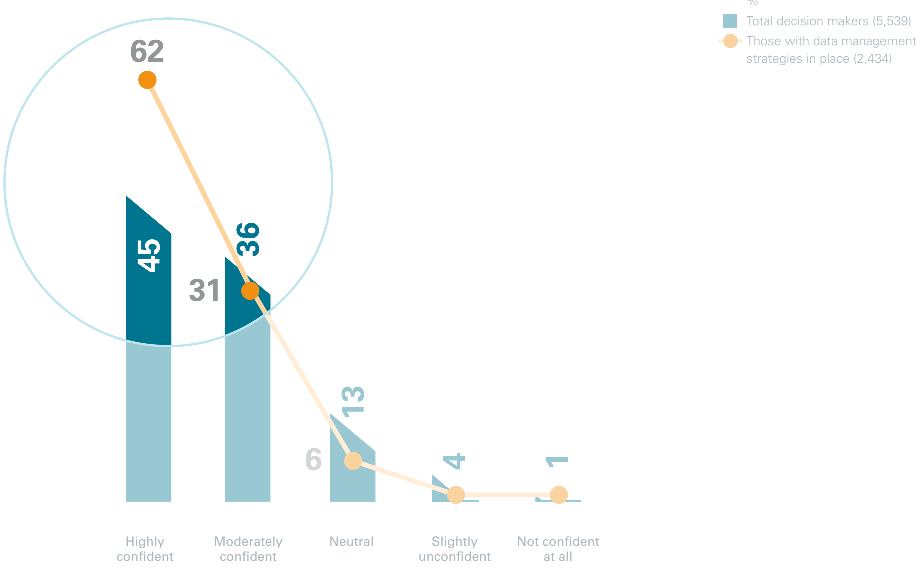
Stronger strategy improves confidence in ethics

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



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

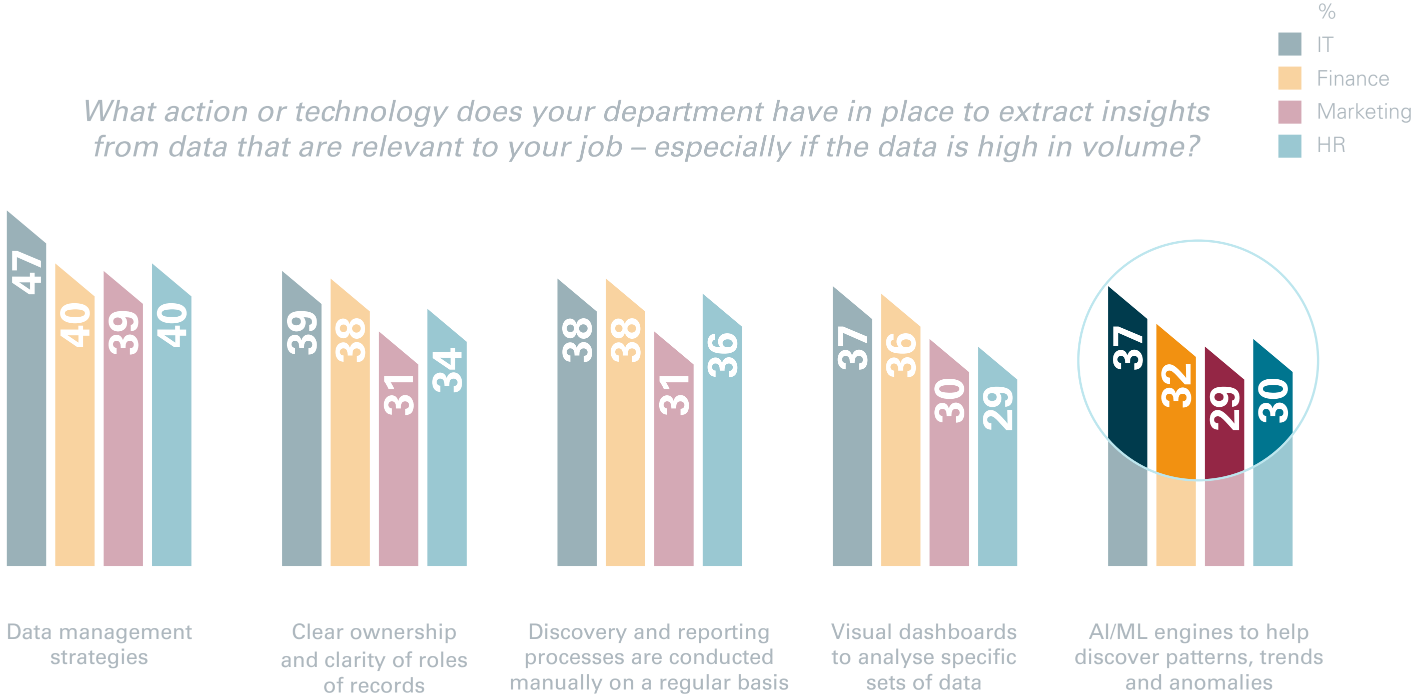


ORACLE Cloud

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 three out of ten 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.

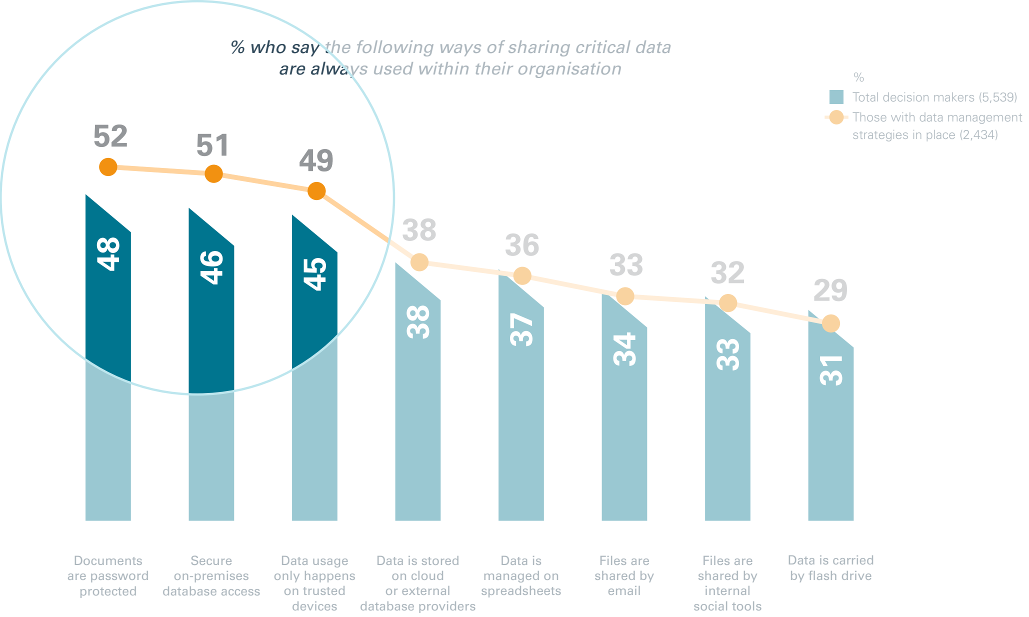
This is especially true when you bring in the many ways that organisations share data internally and externally across email, portable devices and other non-secure platforms and tools.

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 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.



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*.

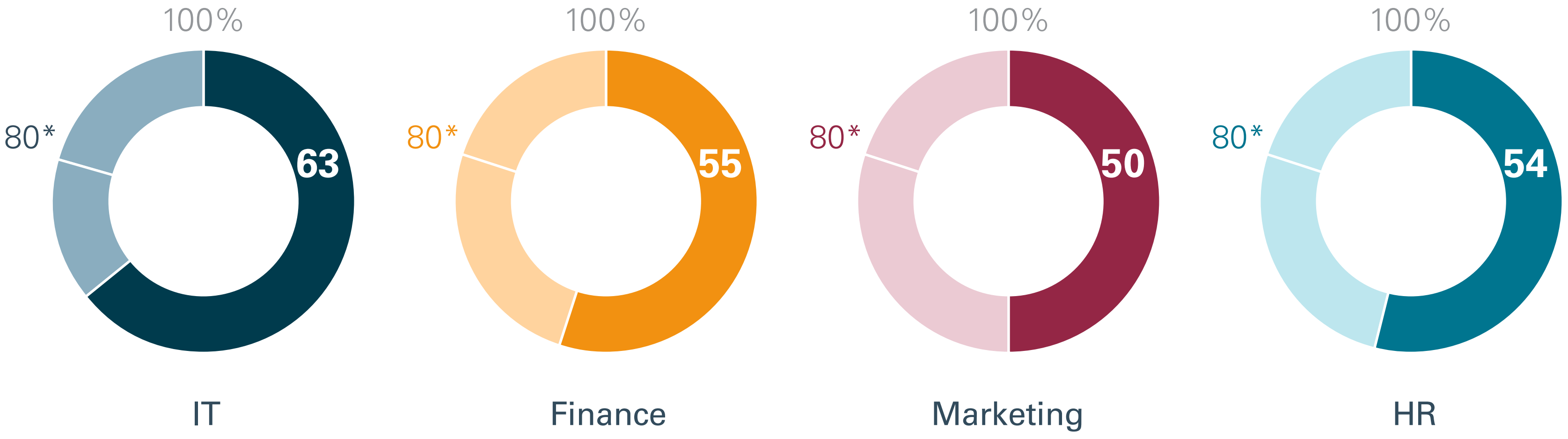
Reputation

Ensuring your organisation's reputation is supported by data

IT leaders lead the way in appreciating the importance of the 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*



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

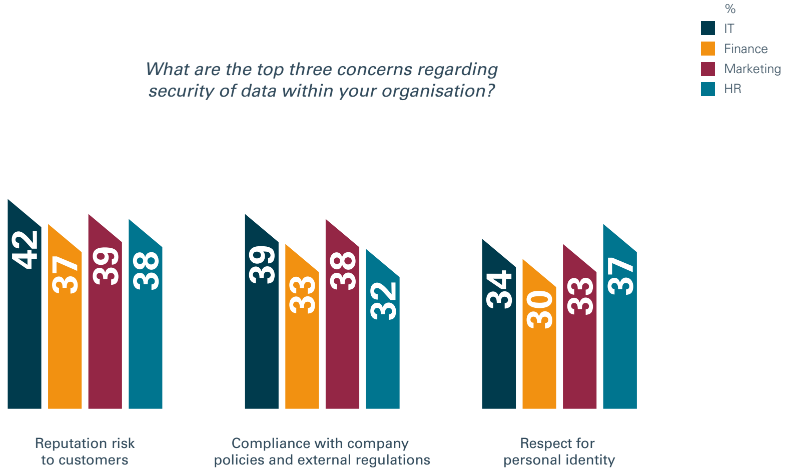
Top three concerns

Protecting company reputation is a top concern across departments. IT leaders place a little more value on reputation risk in front of the customer and compliance, but value respect for personal identity less.

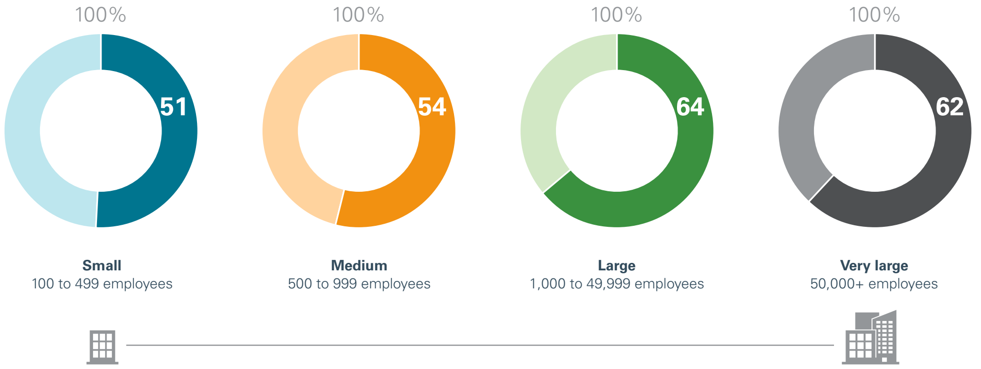
Importance by size of organisation

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?



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



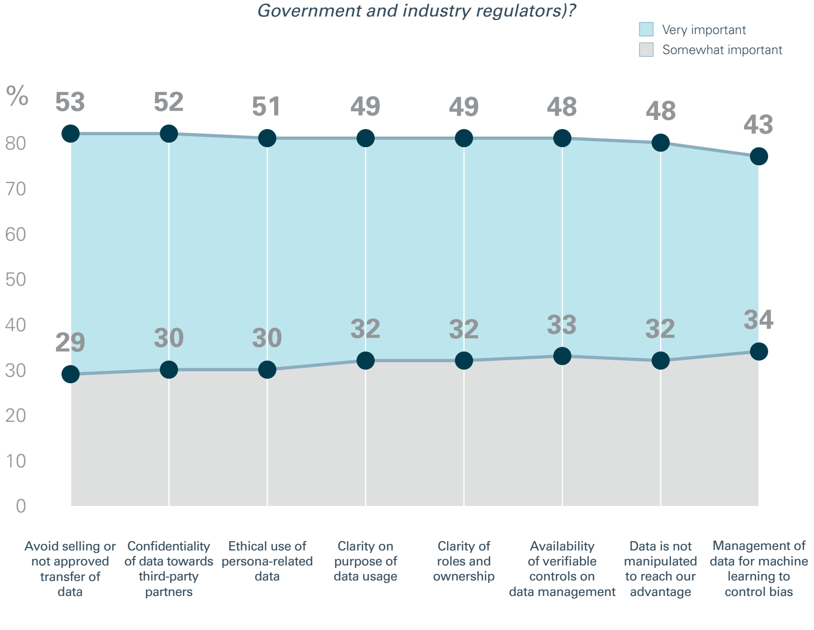
Base: Global population, 24 markets, nr. 5,539

Reputation – Trust and benefits

Trust across audiences

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

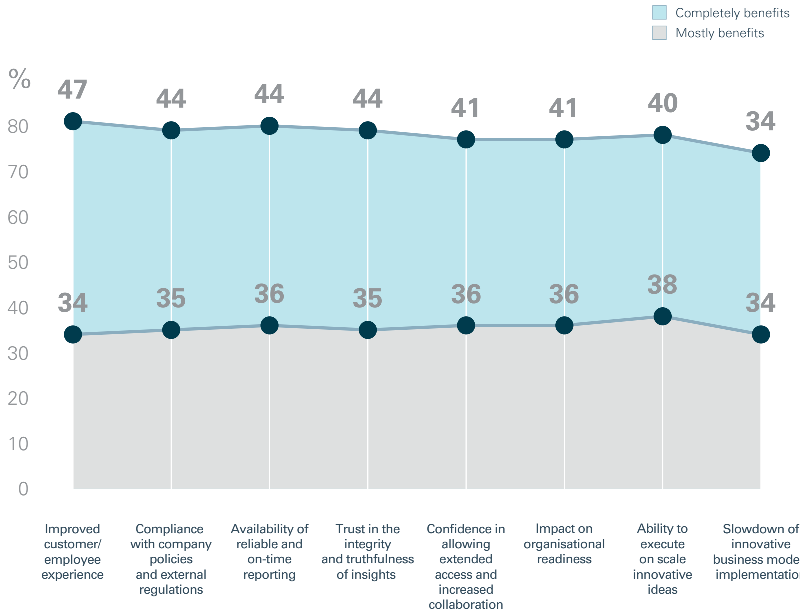
How important are the following factors in allowing your organisation to achieve trust with its audiences (customers/employees/managers/ Government and industry regulators)?



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

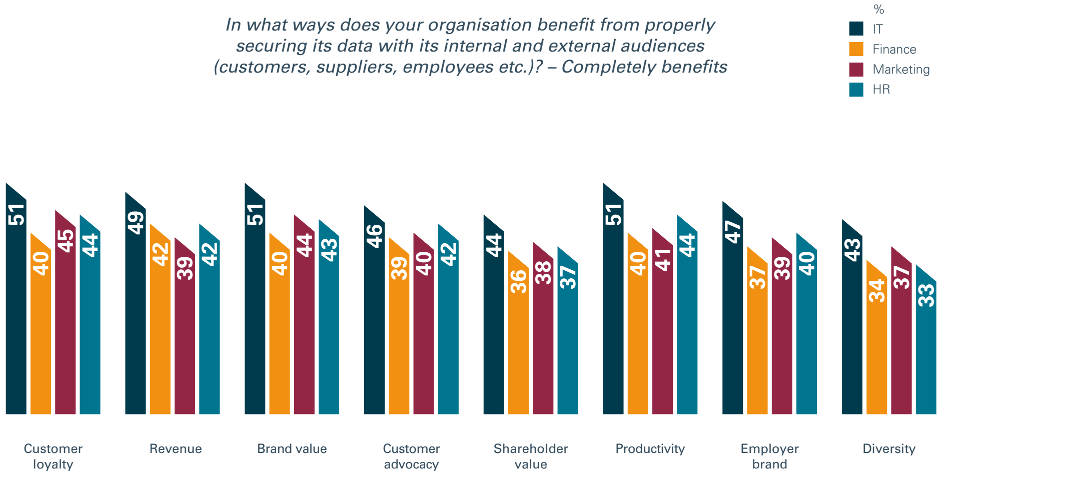


Base: Global population, 24 markets, nr. 5,539

Reputation – Internal/external audiences

Benefits by line of business

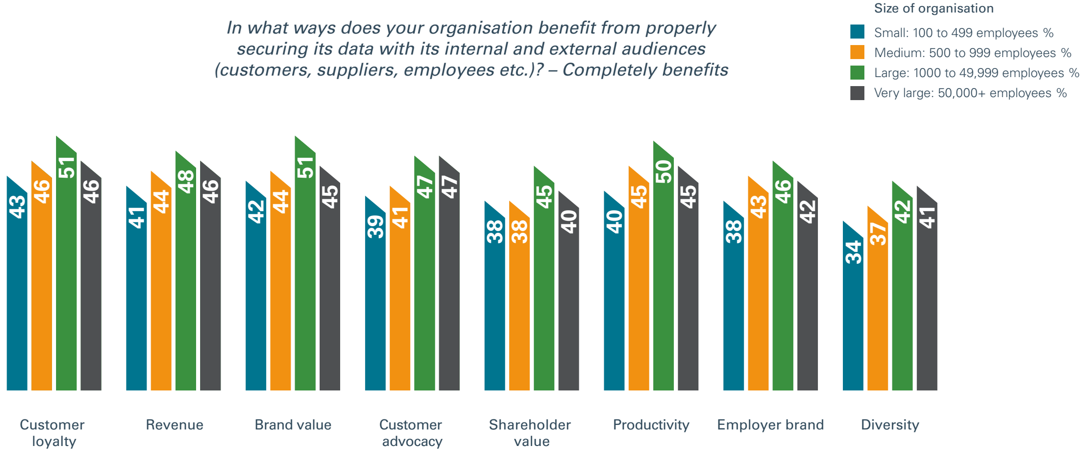
Internal and external relationships benefit across the board from properly securing data. Overall, IT perceive the greatest value, whilst finance see the least.



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

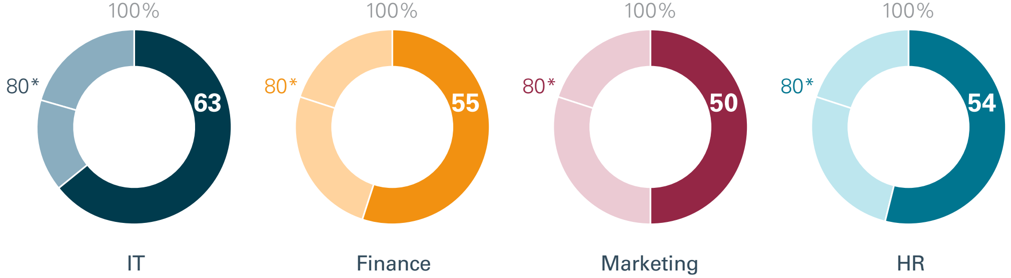
Try Oracle Cloud today

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.

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 **IT, alongside all lines of business, place first or second priority on enhancing security controls and procedures with 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

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

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

- **Data is no longer about protecting sensitive data and keeping hackers out:** IT leaders must focus on enabling organisations to leverage, collaborate on and monetise their data without being exposed to privacy breaches, giving up their intellectual property or having data misused

- **Lead the business in establishing data management strategies and protocols:** They should further ensure this is both implemented through internal education, and effectively monitored

- **Recognise that if IT's confidence levels are low** this lack of confidence will be the same in the wider business, and action therefore needs to follow

- **Encourage autonomous technologies:** The goal is to relieve the human burden of security and compliance and set confidence levels

- **Encourage data migration to big data platforms with increasing embedded cognitive capabilities:** The goal is to eliminate security silos and streamline encryption spend

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

Oracle Cloud