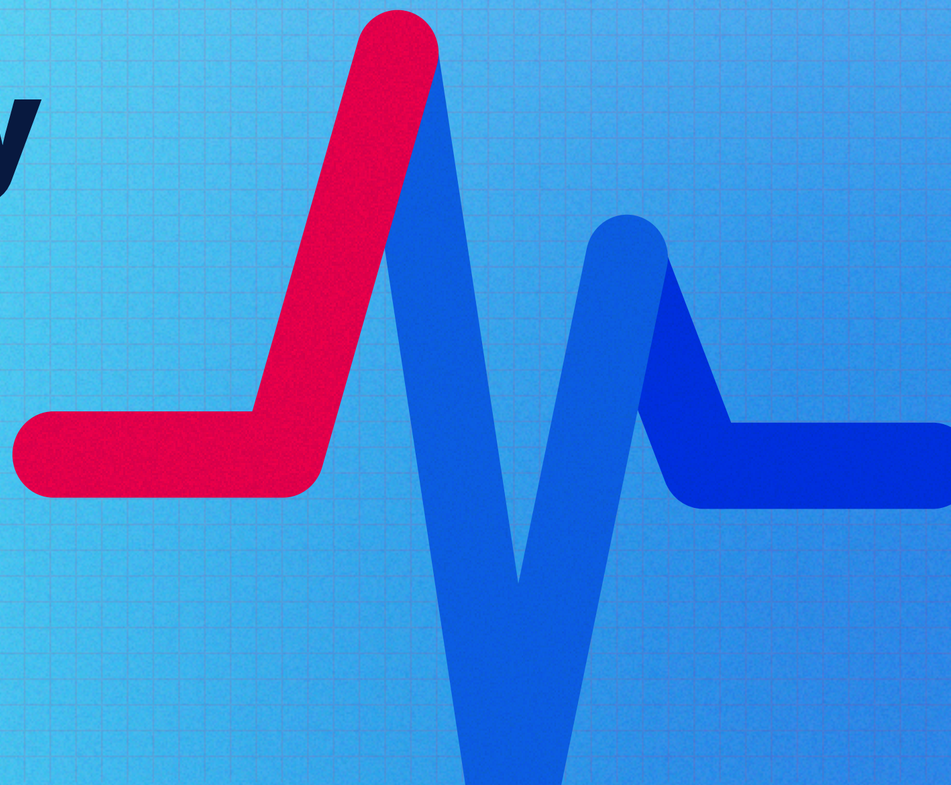
RECORDPOINT

RIMPA
GLOBAL

Pulse of the Industry Report 2023



Contents

About this report

The Pulse of the Industry Report 2023 is based on a survey conducted in May 2023 by RecordPoint in partnership with RIMPA, providing an industry–wide health check on RIMPA members and the organizations they support.

Last year, the industry focused on a move to remote and hybrid workplaces prompted by the COVID-19 pandemic. The current conversation is quite different, with data privacy increasingly the industry's central issue. Significant data breaches involving information governance and data management failures have impacted millions, particularly in Australia. Meanwhile, the ongoing review of Australia's Privacy Act will allow data custodians to play a part in increasing compliance and improving risk management.

The sector has an enormous opportunity to position itself at the core of the response to these challenges. For this reason, we have dedicated a section of this year's edition of the report to assessing respondents' privacy capabilities.

Key goals of the survey were to:

- Establish a comparison with last year to determine the relative change in maturity for RIMPA organizations' information management programs.
- Understand how members and their organizations manage the change in a time of ongoing data breaches and privacy challenges.

The survey consisted of 42 questions grouped into four areas:

1. About you and your organization
2. Technology and data
3. Grade your organization
4. Data privacy

Survey analysis was completed by i3 Ltd, which specializes in strategic information management with data analytics and visualizations provided by Analysis Paralysis Ltd.

Exec summary

Kris Brown

VP of Product

As the second edition in the annual series, the 2023 Pulse of the Industry Report acts as a measure of progress for the industry and a source of critical new insights based on new criteria.

The report can help you inform strategic and operational work program priorities by offering an essential benchmark across several key areas.

At a high level, this year's survey results show a lack of progress for the industry. In nearly all the key areas we benchmark, measures have mostly remained the same.

Given the last year featured several high-profile data breaches and cybersecurity incidents splashed across the front page, such a lack of progress is worrying.

We hope you use the survey findings as a catalyst for change.

Kris Brown

RecordPoint, VP of Product

Key takeaways

1

An information management strategy is critical

40% of respondents do not have an information management strategy (41% in 2022). This year's survey, similar to 2022, reveals organizations lack strategic plans for having a well-developed information management strategy.

Strategic planning is essential to address challenges and optimize resource allocation. Budget constraints emphasize the importance of strategic planning to ensure necessary capabilities and address issues effectively.

As Steve Jobs reflects, strategy is figuring out what not to do. This point is essential when we have limited resources, that we concentrate these resources on things that progress organizational goals.

The absence of an information management strategy risks a lack of clear understanding and mandate for the information management function.

2

Address the discipline disconnect

Survey results reveal a low frequency of interaction with important teams, such as data privacy, data security, and the Executive team.

Such a result suggests different disciplines within the organization (such as Privacy, ICT, Human Resources, Legal, etc.) may not understand each other's areas and work. Working collaboratively with staff from privacy, security, and ICT can help develop an organization-wide holistic view of privacy and security risks, issues, and opportunities.

A side benefit is developing a shared understanding of different business areas. This common understanding can lead to new insights and opportunities based on collaborative and shared approaches and extra support for resourcing and budget bids.

3

Leverage traditional IM tools at scale with AI and ML

Without adequate information management tools and expertise, the costs of managing data increase along with the risks. These risks, if realized, can have highly damaging outcomes ranging from reputational damage to serious harm. Unstructured data represents a substantial percentage of organizational information, with 60% of respondents reporting unstructured data represents between 50 and 100% of the total data in their organizations.

Information management tools knowledge have never been more relevant.

Traditional information management skills offer solutions like understanding retention and disposal requirements linked to information architecture. Coupling these skills with the right tools, such as AI and machine learning, is a powerful value proposition.

4

Ensure you have the correct governance settings

This year's survey, similar to last year, highlights many concerning gaps in information governance. **Symptoms of poor governance settings include a lack of knowledge concerning critical organizational risks.** For example, a plurality of respondents (35%) did not know what percentage of their organization's documents contained sensitive information.

To establish adequate governance settings, you must understand information risks and the controls required to address them. A key ingredient for success is ensuring a common understanding of risks and their mitigation across the different disciplines (privacy, information management, ICT, etc.).

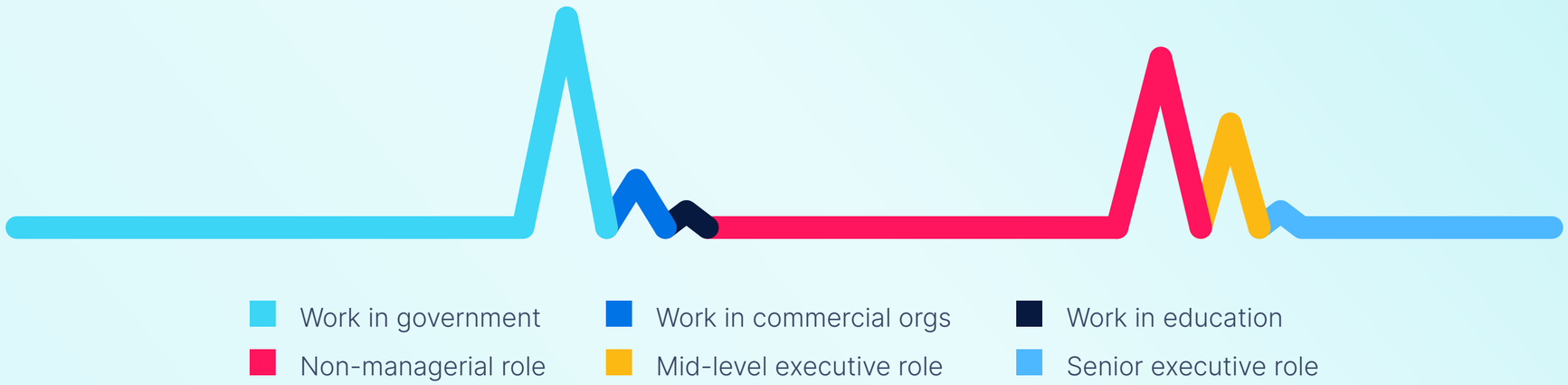
You and your org

Unsurprisingly given RIMPA's membership base, most respondents (86%) were based in Australia, with 6% based in New Zealand, though a variety of other countries were also represented, including the United States, Canada, Botswana, Nigeria, and the United Kingdom.

Most respondents (74%) worked in government, with 18% in commercial organizations, and the remaining 8% in education. Just over half of respondents (57%) were in a non-managerial staff position, with 36% of respondents at the mid-level executive level. Only 8% were senior executives, managing their department.

Most respondents (85%), represented the records and information management function. While legal and data and analytics represented only a small percentage of survey respondents (0.78 and 1.16% respectively), there is an opportunity to join forces with these areas. Joining forces can help drive good privacy and information management outcomes more effectively.

Respondents by industry



Small teams, scarce resources

Resourcing for records and information management varies with the majority of respondents having between 1–2 staff (32%) with the next largest group at 24% having between 3–5.

Digging deeper into the results shows resourcing is somewhat inconsistent and does not necessarily correlate to organizational size. However larger organizations are more likely to have more records and information management staff, with a plurality of 5001+ employee organizations having 21 or more records managers.

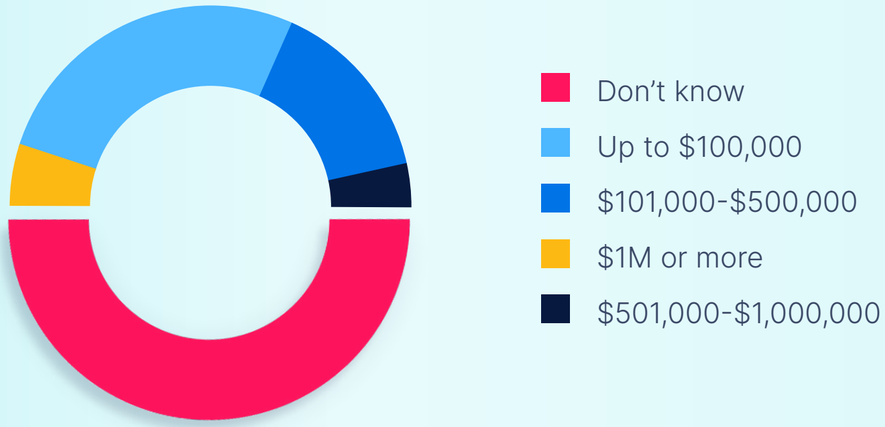
This demonstrates that the resourcing needs for records and information staff isn't predicated on organizational size alone. For example, the type of industry and the associated complexity of the regulatory environment would also influence the resourcing requirements for records and information management staff.

65% of respondents said their records and information management team had not grown in the last year.

This a concerning result given the increasing complexities of managing information across multiple silos coupled with the growing volume of information.

Utilizing scarce resources more strategically requires increased emphasis on working smarter, whether it is utilizing AI in terms of functionality such as trainable classifiers to recognize personal identifiable information (PII) data or partnering with like-minded colleagues in other disciplines.

IRM budget

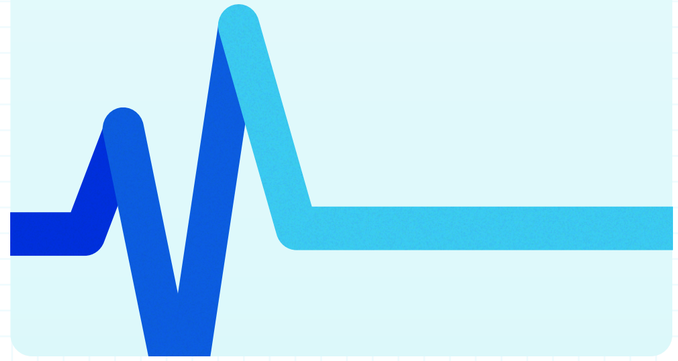


A strategy shortfall

Like last year, 40% of respondents lack an information management strategy, a very concerning finding.

Meanwhile, half of the respondents do not know their annual budget. These findings suggest that records managers lack control and direction and may impact their organization's activities less. These findings also represent an opportunity to help gain better visibility of funding streams for records management initiatives.

An information management strategy prioritizes a work program and informs annual budgeting requirements. It can also help identify areas for savings; for example, retaining information longer than required leads to unnecessary storage and retrieval costs and may increase risks of privacy breaches.



Legacy systems add complexity

While most (87%) use Microsoft 365, legacy content management and collaboration platforms are still widely used. 45% (40% in 2022) of respondents have plans to consolidate IM and CM platforms in the next 12 months, reflecting that consolidating information remains a key challenge.

45% of respondents have plans to consolidate IM and CM platforms in the next 12 months.

Legacy data systems can be a significant contributor to the consolidation challenge. They are also more likely to be less efficient and more vulnerable to security breaches. Legacy systems present a particular challenge in that they are often not easy to integrate with newer technologies or platforms, making it challenging to create a cohesive environment. Using older systems may lead to isolated data silos, hindering collaboration and accurate decision-making.

Top CMS systems

This represents 79% of the systems used by respondents.

Data growth continues apace

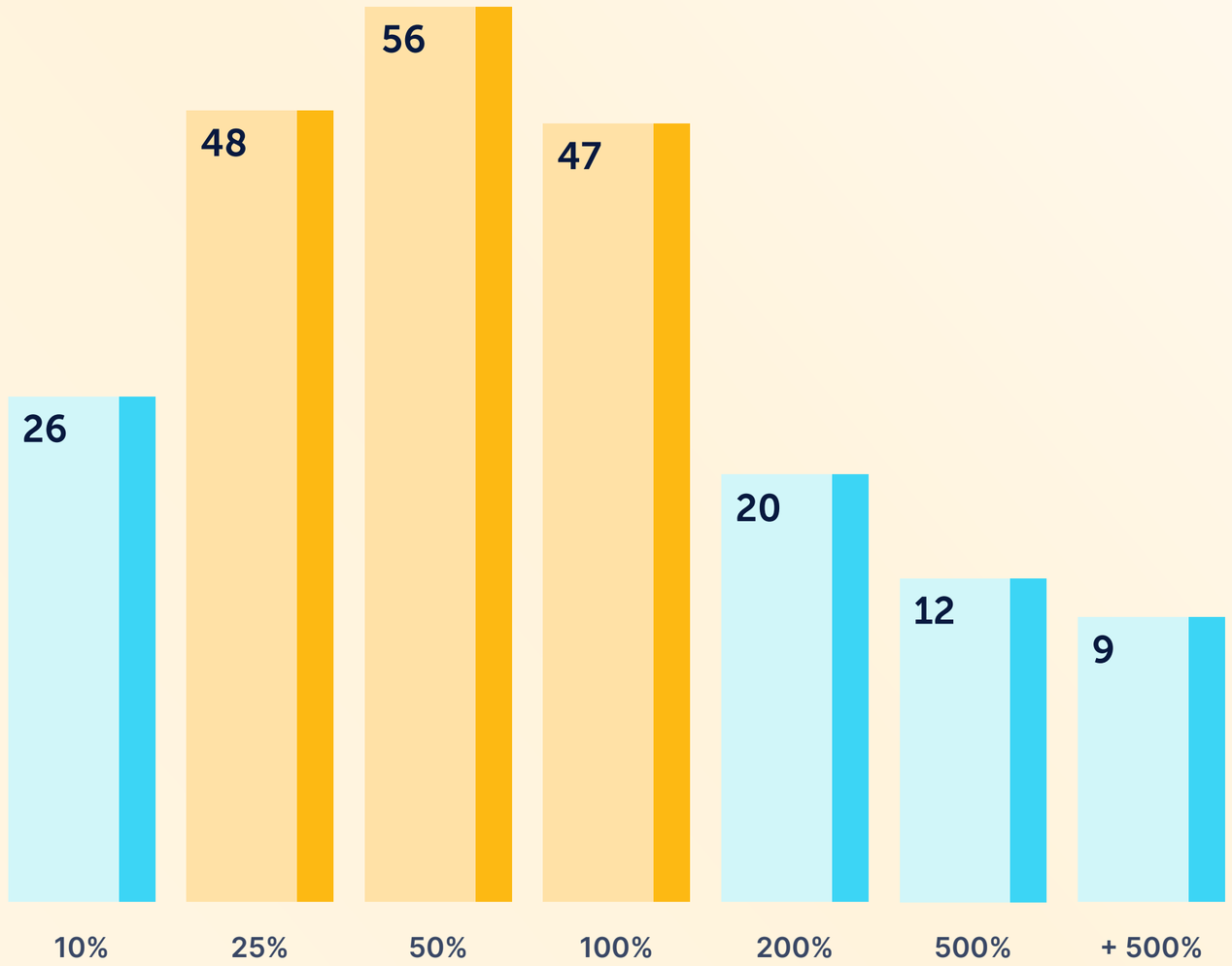
As noted in the 2022 survey, exponential data growth is still a key trend. Coupled with the fact that 76% of respondents expect their budget to be the same or decrease slightly or significantly, this raises substantial challenges in terms of organizational capabilities and capacity required to manage exponential data growth effectively.

48% of respondents expect their organization's data to grow between 50% and 100% in the next two years. This exponential data growth rate poses substantial challenges with key ones, including data management and organization, and data security and privacy risks. Information management professionals can offer their expertise to address the challenge of exponential data growth using their skills in archiving and retention policies to help manage the data lifecycle more effectively.

Responding to this challenge will require tools that address the challenges of data discoverability and governance regardless of the data's location. Ongoing pressures to consolidate data will continue. Effective information management will become even more critical, especially ensuring data is not unnecessarily duplicated.

How quickly has your organization's data grown in the last 2 years?

Shown by number of respondents.



Records teams need tooling to handle their unstructured data

Most respondents (36%) rated their organization's management of unstructured data as average, with 35% rating it as needing improvement. This result aligns with 2022 findings, where most respondents (39%) rated their organizations as needing improvement in unstructured data management.

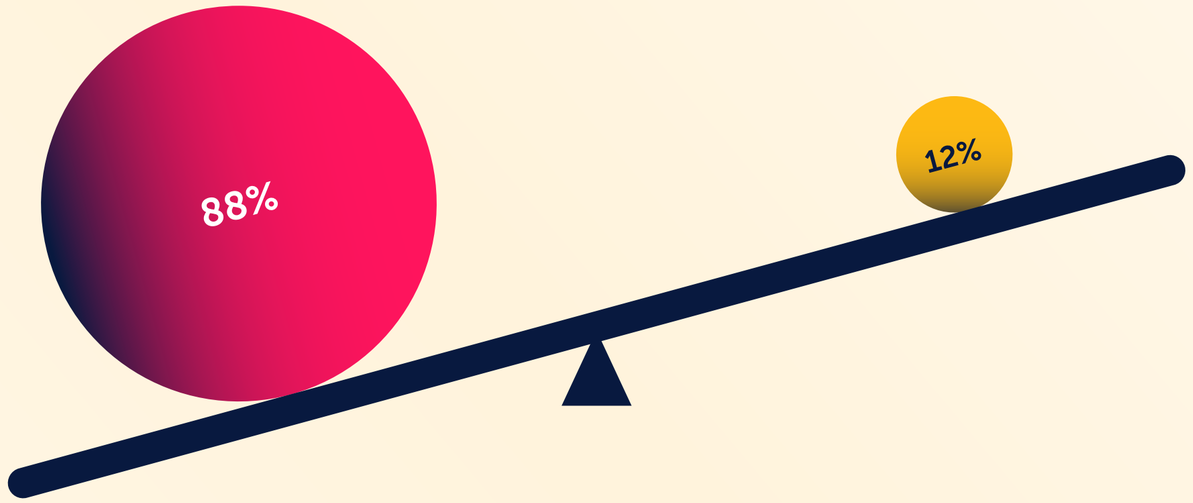
Given that 60% of respondents reported unstructured data represents between 50% and 100% of total data in their organizations, an identical finding to last year's survey, there is a significant opportunity to improve the management of unstructured data with several associated benefits.

Has AI and ML maturity gone backwards?

In 2022, 29% of respondents rated their organization's maturity in artificial intelligence or machine learning as very immature, with no plans or capability in this area. In 2023, this has increased to 38%. Only 12% of respondents rated their organization's maturity as somewhat mature, mature, or very mature.

The data reflects that many organizations were still in the early stages of AI and ML adoption in 2022. Progress in maturity was made by some organizations by 2023, though it was relatively limited. Most organizations fell within the "very immature" and "somewhat mature" categories, demonstrating that there is still room for growth and advancement in implementing and utilizing AI and ML technologies across various industries.

As the capability and prominence of these tools have increased dramatically in the last year with the advent of generative AI tools, it would be somewhat understandable if respondents felt their AI/ML maturity now had a greater distance to go. On that score, only 12% of respondents said they used generative AI tools as part of their business, with most not using them (64%). This result reveals an opportunity to utilize these tools and learn how they work and their limitations.



A concerning lack of improvement in critical areas

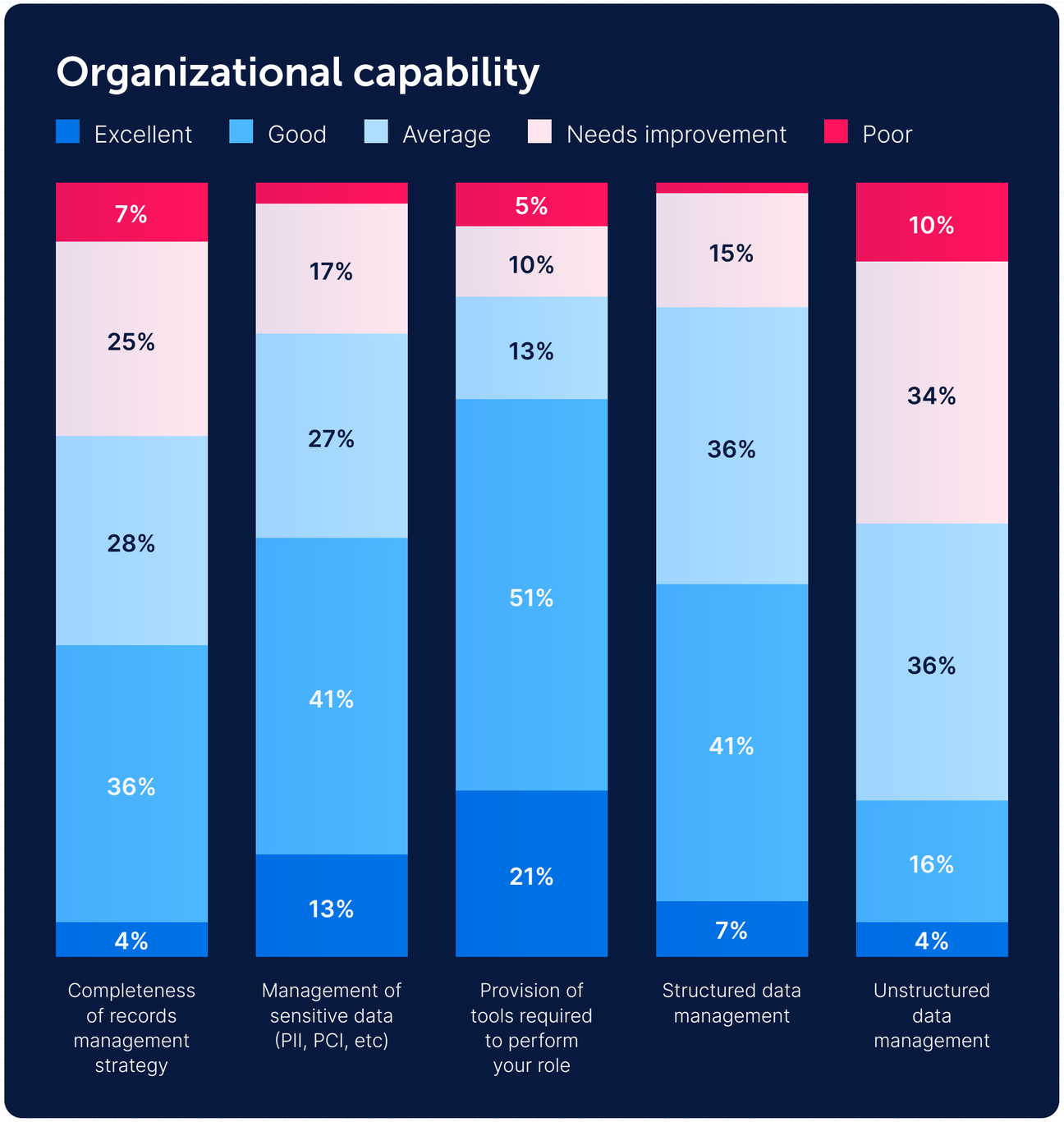
Across the board in this section, most responses were average or below, identical to 2022 results. Many key metrics saw no percentage change in the last year. On two key measures, the industry was at the same point as it was in 2022:

40% of respondents reported that their information strategy is poor or needs improvement in its alignment with business strategy, which is identical to last year's result.

While 53% reported their strategy was only average or needs improvement.

This reflects the same result as 2022. The fact that neither of these metrics has moved in the last year is enormously concerning for those wanting to see a solid records and information management industry.

The completeness of a records management strategy is critical for organizations, especially regarding compliance, data governance, and decision-making.



Sensitive data management is a problem

Managing sensitive data is of crucial concern for organizations. The results underscore the urgency of this matter, with 27% of organizations rating their management of sensitive data as average and an alarming 22% rating it as needing improvement or poor.

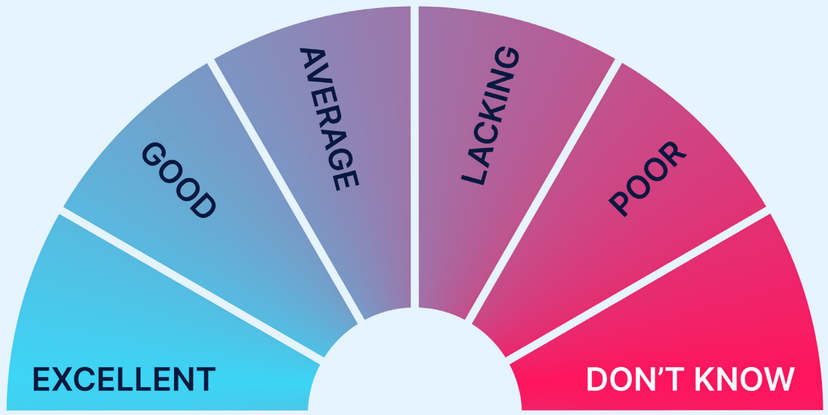
The implications of these statistics are deeply troubling, especially considering the escalating frequency of data breaches. Such breaches expose organizations to reputational damage and pose a severe threat to the affected individuals whose personal information is compromised. This situation underscores the pressing need for robust measures to safeguard sensitive data.

Consumer expectations further compound this issue. In today's digital landscape, individuals anticipate that their personal information will be protected from unauthorized access. This expectation is foundational for building trust and cultivating long-term relationships with customers. Failing to meet these expectations not only risks loss of faith but can also lead to a loss of business.

Addressing this challenge requires a multi-faceted approach. Automation emerges as a pivotal tool in strengthening the management of sensitive data, enabling consistent adherence to security protocols at scale.

However, the effectiveness of automation hinges on the organization's commitment to making data security an organizational imperative.

How does your organization rate?



A significant proportion of respondents (35%) don't know what percentage of their organization's documents contain sensitive information.

This lack of awareness is concerning, as many organizations may not clearly understand the extent of sensitive data in their document repositories.

39% of respondents reported their organizations having 21–50% of their documents containing sensitive information, suggesting a considerable portion of organizations acknowledge having a substantial amount of sensitive data in their document repositories.

Most respondents (62%) based this estimate on an educated guess. Educated guesses indicate that respondents might have some understanding or insights about their organization's data but not from a concrete, data-driven inventory.

33% of respondents made uneducated guesses, indicating that many organizations responded without any data or informed understanding of their document content, which is concerning.

Only 6% of respondents based their responses on a current inventory. A tiny percentage of organizations have conducted a comprehensive assessment or analysis of their document repositories to determine the proportion of sensitive information.

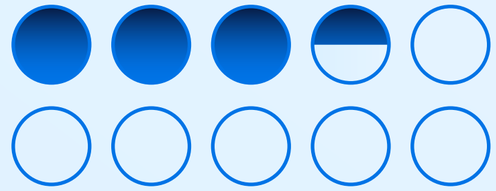
Worryingly, 54% of respondents could not identify the tool used to provide the current inventory. This lack of awareness about the inventory source raises concerns about the transparency and reliability of the data used to make decisions about sensitive information handling.

Overall, the insights highlight the urgent need for organizations to improve their awareness and understanding of sensitive information within their document repositories. These results represent significant risks for the organizations concerned.

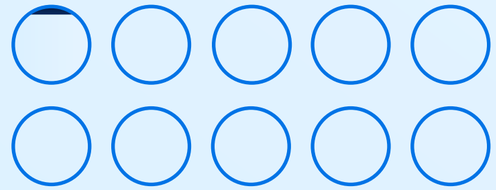
Organizations must prioritize data governance, invest in appropriate tools and practices, and ensure transparency and accuracy in handling sensitive information.

Again, traditional information management tools like information asset registers, which capture high-risk and high-value information, would assist here. Coupled with Enterprise Data Models, these tools give a strategic view of core data and information across the organization.

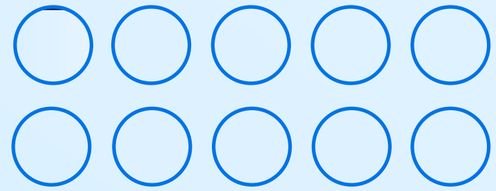
Organizations don't know the sensitive data they possess



35% of respondents don't know what percentage of their organization's documents contain sensitive information.



10% of respondents guessed 50% of data contains PII or PCI.



6% of respondents conducted an analysis of their systems to detect PII and PCI.

Organizations need to build their privacy teams

The fact that 56% of organizations have a privacy officer or department reflects a growing awareness of the importance of data privacy and the need to comply with data protection regulations. A designated privacy role demonstrates an organization's commitment to managing and protecting sensitive data.

The proportion of respondents whose organization does not have this role or department was sizeable, at 33%.

Many organizations may not have established a formal structure to address privacy concerns or handle compliance with data protection regulations.

These organizations without a privacy officer or department might be facing resource constraints or may not have recognized the full scope and importance of privacy management. These organizations could be more vulnerable to privacy risks and regulatory non-compliance.

Of the respondents with a privacy officer or department, 62% indicated this team had under two people. Smaller privacy teams or a single privacy officer could face challenges in managing an organization's comprehensive privacy needs, especially if the organization handles a large volume of sensitive data. Such teams must be adequately supported and resourced.

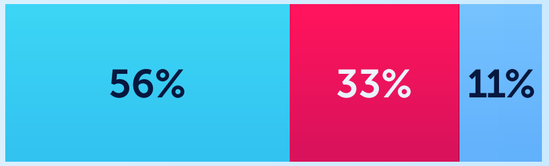
26% had between two and 10, indicating that some organizations have recognized the need for a larger team to handle the complexities of privacy management, especially in larger or more data-intensive organizations.

The privacy landscape is evolving. As data protection regulations continue to mature, organizations must reevaluate their privacy officer/department sizes and ensure they have the expertise to handle emerging privacy challenges effectively.

These insights highlight progress and potential improvement areas in organizations' privacy management. Establishing a dedicated privacy officer or department is a positive step. However, as a matter of urgency, organizations should also ensure that their privacy teams have the resources and capabilities to address the complexity and ever-changing landscape of modern privacy and data protection requirements.

Taking a closer look at privacy teams

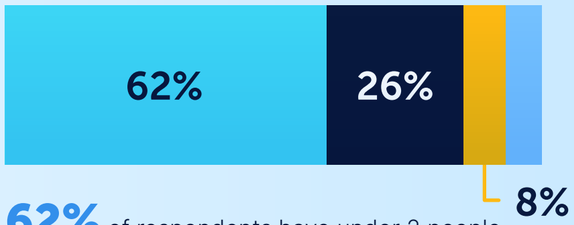
Do you have a Data Privacy Officer?



56% of respondents answered 'yes', compared to **33%** of respondents answering 'no'.

Worryingly, **11%** of respondents didn't know if their organization had a Data Privacy Officer.

Data privacy: Team size



62% of respondents have under 2 people, compared to **26%** of respondents with 2–5 people in their data privacy team.

Very few organizations have privacy teams with over 6 people; **8%** have 6–10 people with more than 10 people in the minority at **4%**.

Privacy is still seen as an IT problem

Most respondents reported that their IT position holds the primary responsibility for data privacy in their organization (28%), with the second largest proportion of responses being the Data Privacy Officer (23%) followed by Legal (17%). Records Management came in 4th place at 14%.

Only 13% of respondents reported that the Executive level is primarily responsible for data privacy. This finding is unexpected as data privacy is often considered a critical aspect of business strategy and should ideally have strong support and involvement from top executives. Could a lack of an information management strategy be to blame?

The delegation challenge

Most organizations delegate data privacy tasks to their IT departments, which could involve implementing security measures, access controls, and safeguarding data.

Organizations must build an understanding of roles and responsibilities for data security and privacy and ensure these are documented and understood. This understanding will create a more holistic approach to understanding and managing privacy risks. Robust data privacy is a combination of understanding key risks, treating those risks in terms of mitigations and controls, and—above all—testing the controls to be effective.

It is somewhat surprising that the Executive and Risk functions have less involvement in data privacy matters, given the increasing importance of data protection and its potential impact on an organization's reputation and compliance. This is also in contrast to the results of a survey across the Americas by Ernst and Young, which had executives and board directors putting cybersecurity and data privacy in the top five priorities for 2023.

These results also reveal an opportunity to take a more multi-disciplinary approach to data privacy using the different skills across records management, privacy, legal, risk, Executive, and IT. All these disciplines will bring a slightly different perspective to augment data privacy initiatives, as opposed to taking a siloed approach.

But records and information managers are impacting privacy

Most organizations (69%) had undertaken activities related to cybersecurity controls. The 2nd and 3rd activities were Data Access Control (57%) and Data Classification (54%).

These results indicate that organizations are taking significant steps to improve their data privacy posture by focusing on cybersecurity controls, data access control, and data classification. By prioritizing these activities, organizations aim to strengthen their data protection efforts and mitigate the risk of data breaches and unauthorized access to sensitive information.

While these three activities are prevalent, other data privacy-related actions should also be undertaken by organizations, depending on their specific needs and regulatory requirements. These should include regular employee data privacy training, privacy impact assessments, incident response planning, compliance with data protection regulations, and conducting regular privacy audits to ensure ongoing adherence to data privacy best practices. We should never assume controls are adequate without regular testing.

A concerning lack of certainty

The findings reveal that despite high awareness about information assurance among respondents, 29% have personally experienced the impact of a data breach in 2022/2023. Even with understanding, privacy breaches can still affect individuals.

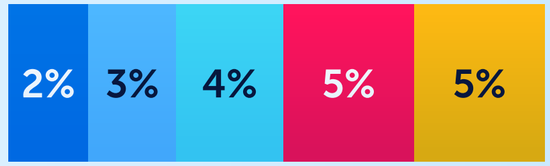
Of concern is 26% of respondents are uncertain whether a privacy breach has impacted their organizations, suggesting inadequate monitoring or incident response protocols and underscoring the criticality of heightened awareness and increased investment in cybersecurity.

More collaboration will lead to better outcomes

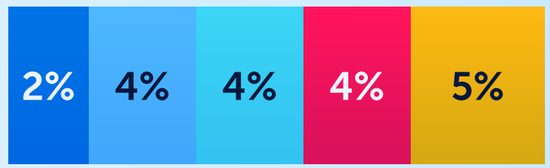
Interactions with data privacy, data security, executive/board, and legal teams are not as frequent as may be expected. Greater collaboration can reduce gaps in data privacy planning and organization decision-making processes.

How often do RIM teams interact with:

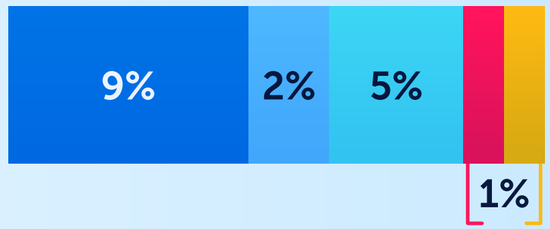
Data privacy teams



Data security teams



IT teams



Recommendations

1

Sell your value in the context of privacy

56% of respondents noted they have a privacy officer/ team, but 28% reported that responsibility for managing privacy falls on the IT team, as many organizations still see privacy as an IT problem.

However, records and information management professionals impact privacy and cybersecurity by accurately classifying sensitive information so it can be retained only as long as legally required. Data breaches are increasingly a fact of life; organizations that manage and reduce their data will minimize risk.

This fact needs to be understood by the wider business. Records and information management professionals are data custodians, and their activities can positively impact the privacy posture of an organization. When establishing an information management strategy, this should be an essential pillar.

2

Become a leader when it comes to technology adoption

We are at an inflection point in terms of technology adoption. By embracing automation, you can focus on critical priorities like establishing an information strategy linked to your budget and understanding sensitive data. Such an approach will help solve your organization's data challenges and reduce risk.

Based on the results of this survey, many organizations struggle to classify and understand their data. ML and AI (not necessarily generative AI) can make an impact and allow for a strong privacy posture.

Meanwhile, your colleagues are likely experimenting with generative AI, such as LLMs, possibly in an unsafe way that involves using a free model and providing confidential company data and customer PII.

You are running out of time to take control and govern how your organization uses these products to reduce the risk of your organization losing control of sensitive data or making decisions based on biased or hallucinated information.

Records managers missed the last wave of technological change. It doesn't have to be that way with these new tools.

3

Demand more from your organization

The industry has not evolved from its position last year in many key metrics. It has regressed in some areas, such as its understanding of AI and ML technologies. Forty percent of respondents lacked an information strategy. Half did not know their budget. And over a third needed help managing their unstructured data. Across the board, there has been a notable lack of improvement over last year.

When we look at new measures, the results are not encouraging. Half of respondents guessed how much PII their organizations held, and nearly half of respondents rated their organization's management of sensitive data as either average (27%) or needing improvement or poor (22%).

As we discussed, the three massive, damaging data breaches that occurred last year should have been a wake-up call for all organizations to ensure they had a firm handle on all their data. Instead, it seems most kept their head in the sand.

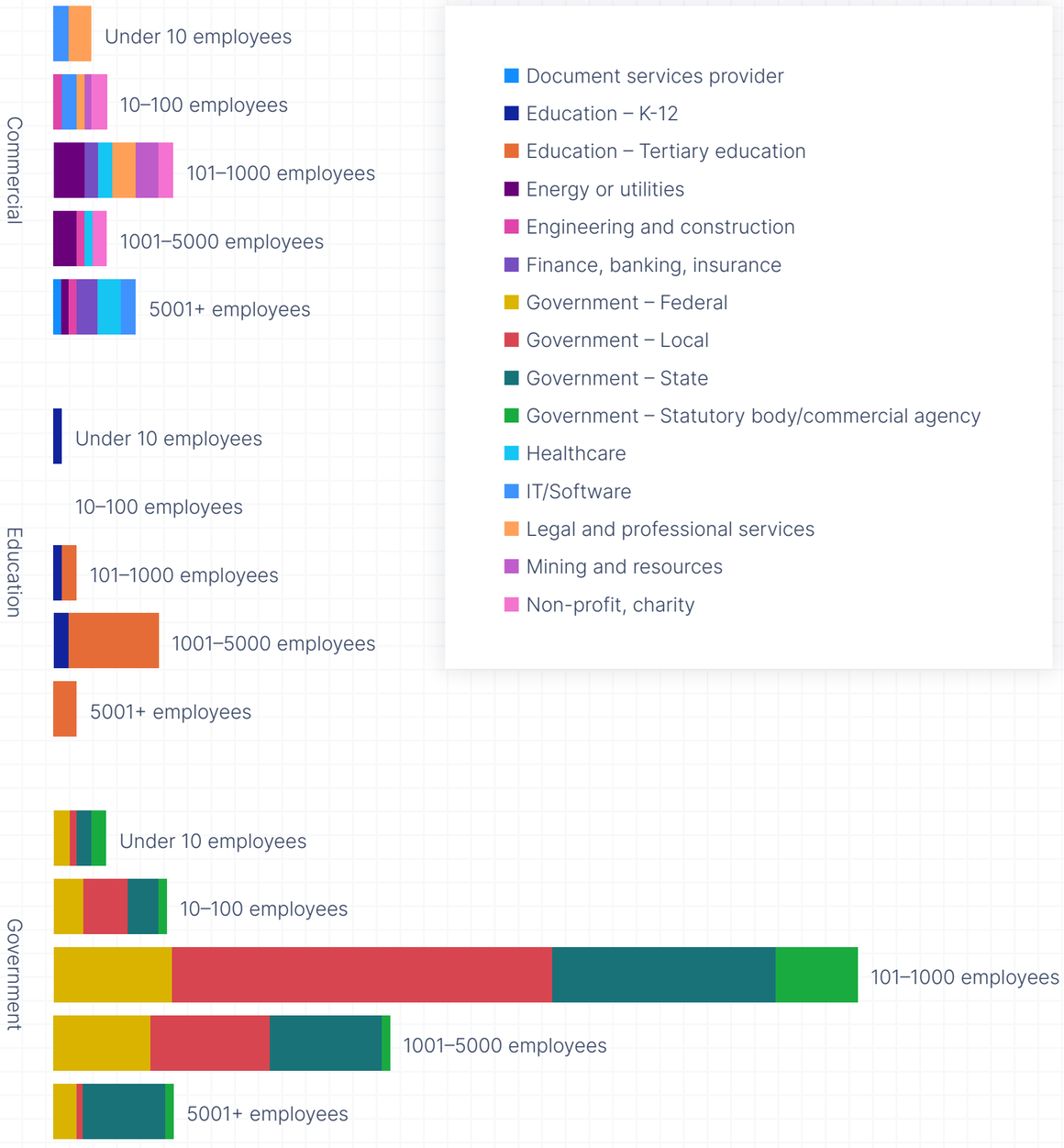
What will it take? A data breach? A fine from a regulator?

Let's start with someone (you, perhaps) demanding they take these challenges seriously. At this point, ignorance is no longer an excuse. We have to work together to lift these numbers.

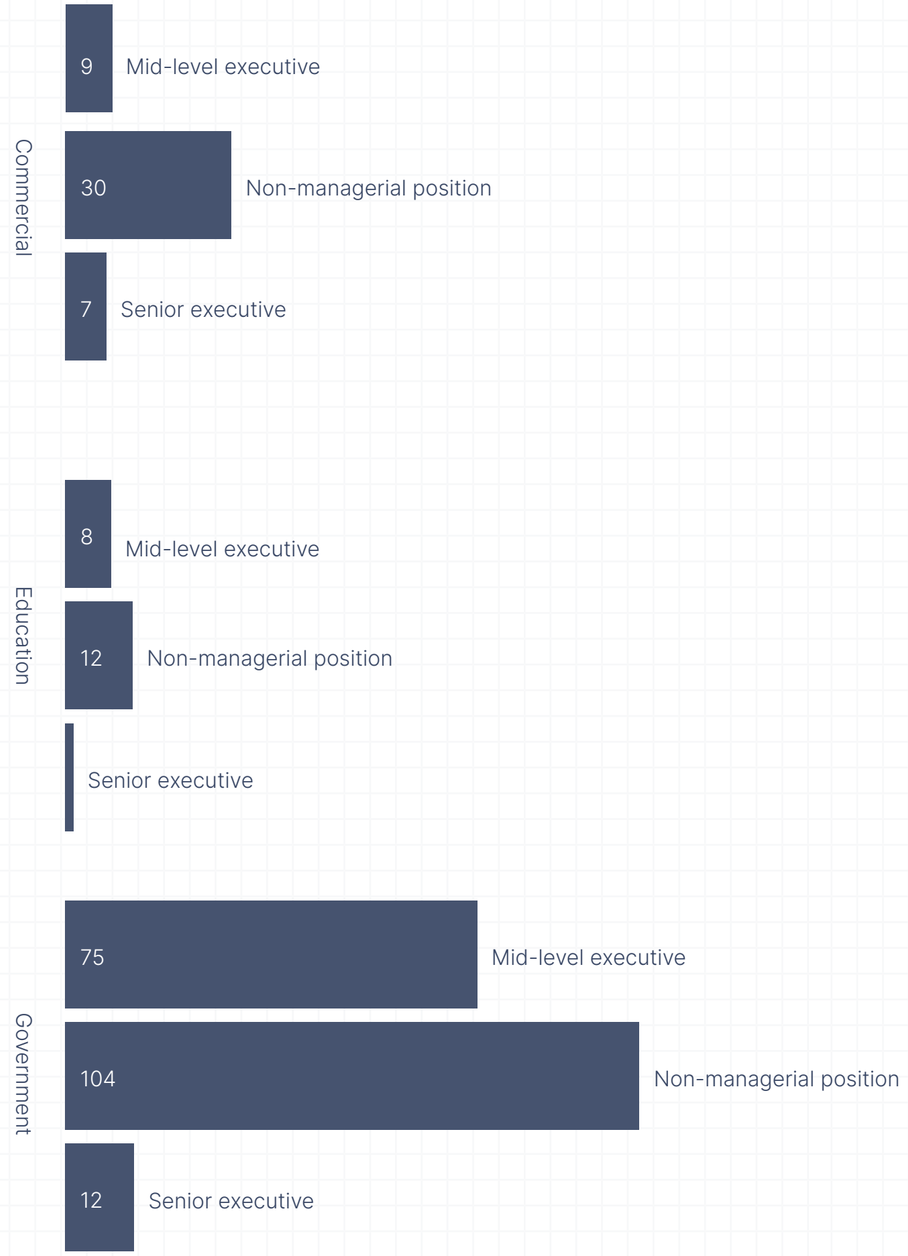
If your organization is one of those struggling, and you're unsure how to get started on changing these results, we would love to know what your challenges are and how we may be able to help overcome them.

Appendix

Respondents by organization size



Respondents by position



RECORDPOINT

RIMPA GLOBAL

Be the company your customers can trust with their data.

RecordPoint is the Data Trust Platform, giving highly-regulated organizations a competitive edge with safer, more secure, better-managed data. Businesses can trust that their data is accurate, private, and safe everywhere, all the time, for consistent confidence that's backed by RecordPoint expertise.

For more information visit www.recordpoint.com