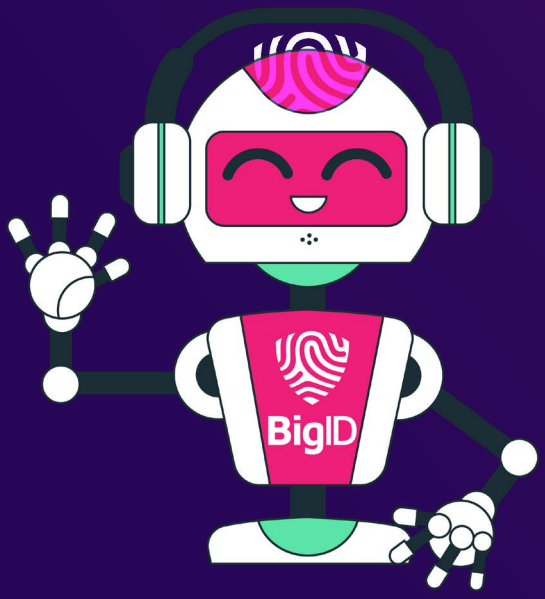
Survey Report

The 2024 GLOBAL REPORT ON GENERATIVE AI:
Breakthroughs & Barriers

Insights & Trends from Industry Leaders on the Adoption, Challenges, and Impact of Generative AI in Organizations



BigID

SAP® Endorsed App
Premium Certified

Table Of Contents

Overview & Objectives

Nearly 50% **of organizations report adverse business outcomes related to AI usage, with data breaches being the most prevalent.**

Generative Artificial Intelligence (AI) is undergoing rapid adoption within the workplace, transforming business by improving productivity, optimizing processes, and facilitating data-driven decision-making. As AI becomes a vital asset across industries, understanding how to effectively control, audit, and manage data shared with AI applications is becoming increasingly crucial. This is essential for ensuring compliance with evolving privacy and protection regulations and maintaining the security and ethical use of AI.

BigID, an SAP Endorsed Apps partner, commissioned YouGov to research present and future trends in the adoption of generative AI through a comprehensive survey. The survey, conducted by YouGov in November 2023, carried out 327 interviews from IT decision-makers and influencers from organizations around the world of various sizes, industries, and locations.

The study delved into the effects, use cases, and challenges associated with this technology, specifically focusing on critical aspects such as security, privacy, governance, and compliance. In addition, the study offered a comprehensive perspective on the current state and future trajectory of generative AI within the business landscape. This report examines these nuances, providing valuable insights into how organizations navigate the challenges and opportunities that generative AI presents.

Executive Summary

- **Most organizations are swiftly embracing generative AI**, indicating a shift towards more technology-driven and innovative business models, underscoring AI's potential to enhance business processes and efficiency.
- **Major concerns persist around the security and privacy aspects of generative AI,** with issues such as data breaches, legal complexities, and compliance highlighting the need for robust security controls and privacy safeguards.
- **Organizations face significant hurdles in implementing generative AI**, including data security, cross-functional collaboration, and transparency in AI decisions.

Section 1
Current & Future AI Adoption

Current & Future AI Adoption

Momentum: Charting the Rise of Generative AI

The survey highlights an overwhelming trend toward generative AI adoption, with 83% of organizations either already utilizing or intending to adopt this technology in the near future. The significant interest is not just about harnessing AI's transformative capabilities but also about effectively managing and controlling the data used by AI applications.

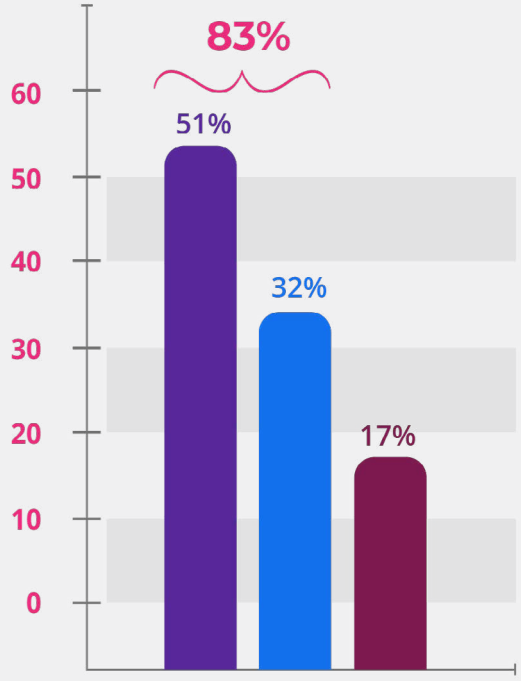
The results highlighted a notable uptick in the adoption of Artificial Intelligence (AI), with a specific emphasis on generative AI. Currently, 51% of surveyed organizations actively use or implement generative AI, illustrating its growing importance within the workplace. Additionally, 32% of organizations, while not currently leveraging AI, plan to adopt it within the next year, recognizing its potential benefits. However, this adoption also brings challenges, particularly in data governance and security, underscoring the need for controls and measures around the data shared with AI applications and the ability to audit data use based on privacy, sensitivity, regulation, and access.

However, 17% of organizations haven't planned to adopt generative AI, citing data management and security concerns. This variability in adoption rates reflects the dynamic nature of the AI-business relationship. Navigating this path necessitates organizations to prioritize comprehensive strategies for data usage, security, and governance, ensuring AI is both innovative and compliant.

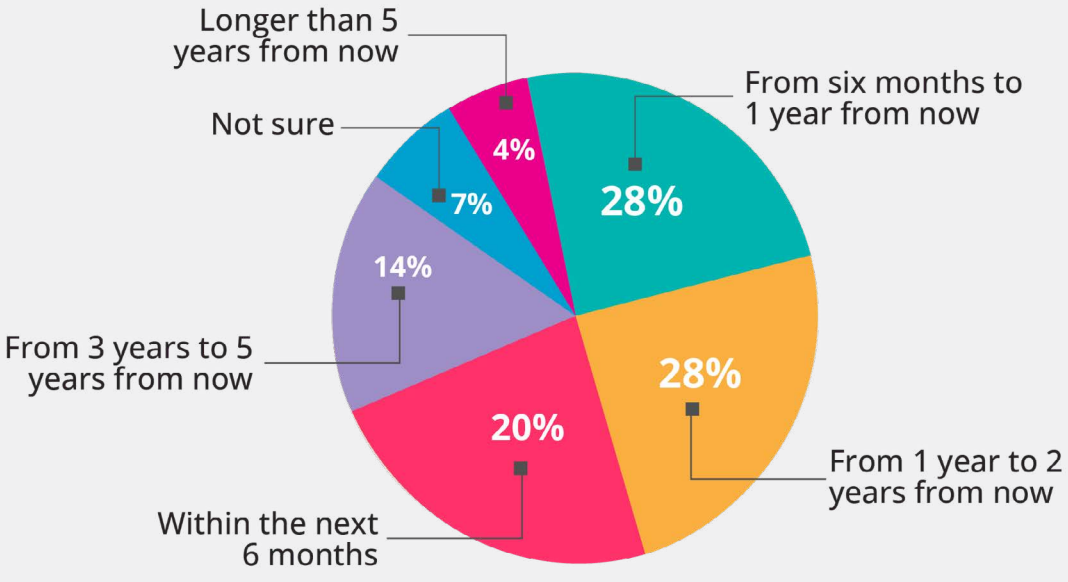
83% of organizations are actively embracing or preparing for generative AI.

Q Is your organization currently using, or in the process of implementing, generative AI?

- **51% Yes**
  currently using or in the process of implementing generative AI
- **32% Plan**
  to use in the near future but currently not using
- **17% No**
  not currently using now with no plans to in the near future

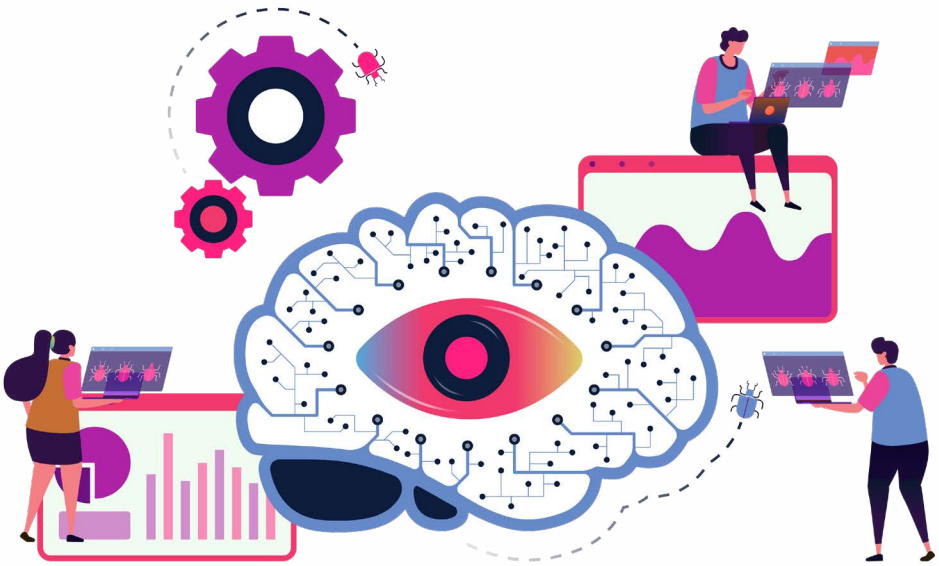


Q When do you plan to adopt generative AI at your organization?



The varied timelines for adopting generative AI, as highlighted in the survey, necessitate tailored preparation strategies. Organizations planning adoption within 1-2 years (28%) and those targeting six months to a year (28%) require immediate action. Priority should be given to strengthening data security, identified as the primary challenge in AI implementation (Section 5), through proper governance measures, controls, and frameworks. This starts with building out a strong data discovery and classification foundation, implementing the proper data access control measures, and conducting regular security audits. For the 20% aiming to adopt within six months, the focus should be on turnkey data security controls and comprehensive employee training around AI ethics and data management.

Meanwhile, the 14% considering a 3-5 year horizon and the 7% who are uncertain have the advantage of crafting more comprehensive AI governance and security strategies while weaving AI literacy into their processes. The 4% with an adoption timeline exceeding four years should leverage this extended period to vigilantly monitor the evolving AI technology and regulatory landscapes, ensuring future readiness. Regardless of the timeline, organizations must place a priority on data security when integrating AI into their operations to maximize AI's potential benefits while minimizing its evolving risks.



Section 2
Purpose of Adopting AI

Purpose of Adopting AI

The AI Effect: Advancing IT, Communications, & Customer Engagement

Organizations are leveraging AI across various domains, from optimizing IT operations to enhancing customer service. Generative AI's adaptability facilitates tailored solutions, driving efficiency and innovation. However, as AI integrates into critical functions, ensuring data integrity and security, particularly with sensitive or regulated data, is paramount. Establishing stringent policies and tools is essential for effective management and control.

Research revealed the top three areas of current applications for generative AI:

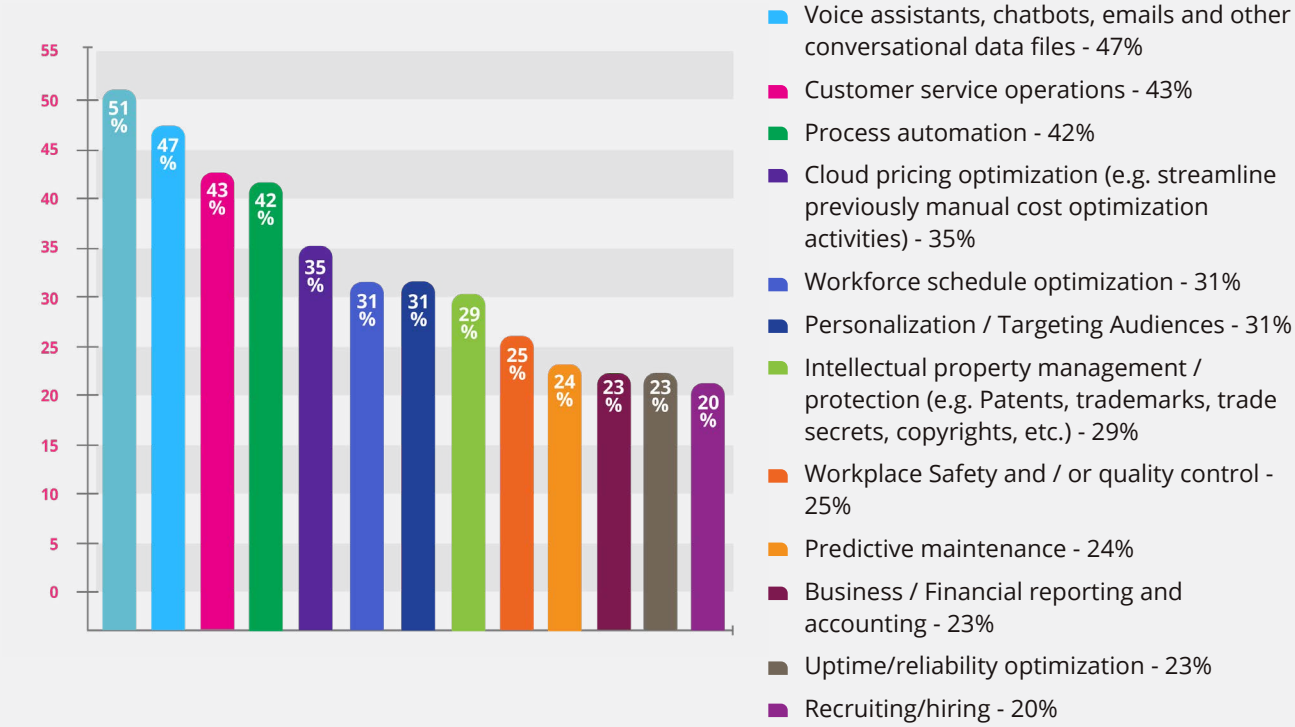
51% of organizations use AI for automating and optimizing tasks like system monitoring, data analysis, and network management. Ensuring the accuracy and security of the data in these applications is vital to prevent malfunctions or breaches.

47% employ AI in communication technologies such as voice assistants, and chatbots, and for managing conversational data in emails and other platforms. Here, the challenge is to maintain data privacy while providing efficient communication solutions.

AI is utilized by **43%** of organizations in customer service to facilitate quicker and more personalized customer interactions. AI in customer services necessitates a delicate balance between personalizing customer interactions and safeguarding consumer data, making data governance policies and consent management systems imperative.

Over half of organizations now automate IT operations with AI.

Q For what purpose(s) or use case(s) is generative AI employed or will be employed within your organization?



- IT operations management - 51%
- Voice assistants, chatbots, emails and other conversational data files - 47%
- Customer service operations - 43%
- Process automation - 42%
- Cloud pricing optimization (e.g. streamline previously manual cost optimization activities) - 35%
- Workforce schedule optimization - 31%
- Personalization / Targeting Audiences - 31%
- Intellectual property management / protection (e.g. Patents, trademarks, trade secrets, copyrights, etc.) - 29%
- Workplace Safety and / or quality control - 25%
- Predictive maintenance - 24%
- Business / Financial reporting and accounting - 23%
- Uptime/reliability optimization - 23%
- Recruiting/hiring - 20%

To ensure the ethical and effective use of AI, organizations must prioritize data security, privacy, and governance. This involves a robust grasp of the technical aspects of AI implementation and a comprehensive understanding of the entire data lifecycle — from collection and processing to storage and eventual deletion or archiving. Responsible AI use necessitates the seamless integration of data management strategies within AI applications, aligning them with broader business objectives and regulatory requirements.

Section 3
Barriers to AI Adoption

Barriers to AI Adoption

Overcoming Obstacles: Navigating the Challenges Hindering AI Use Within the Workplace

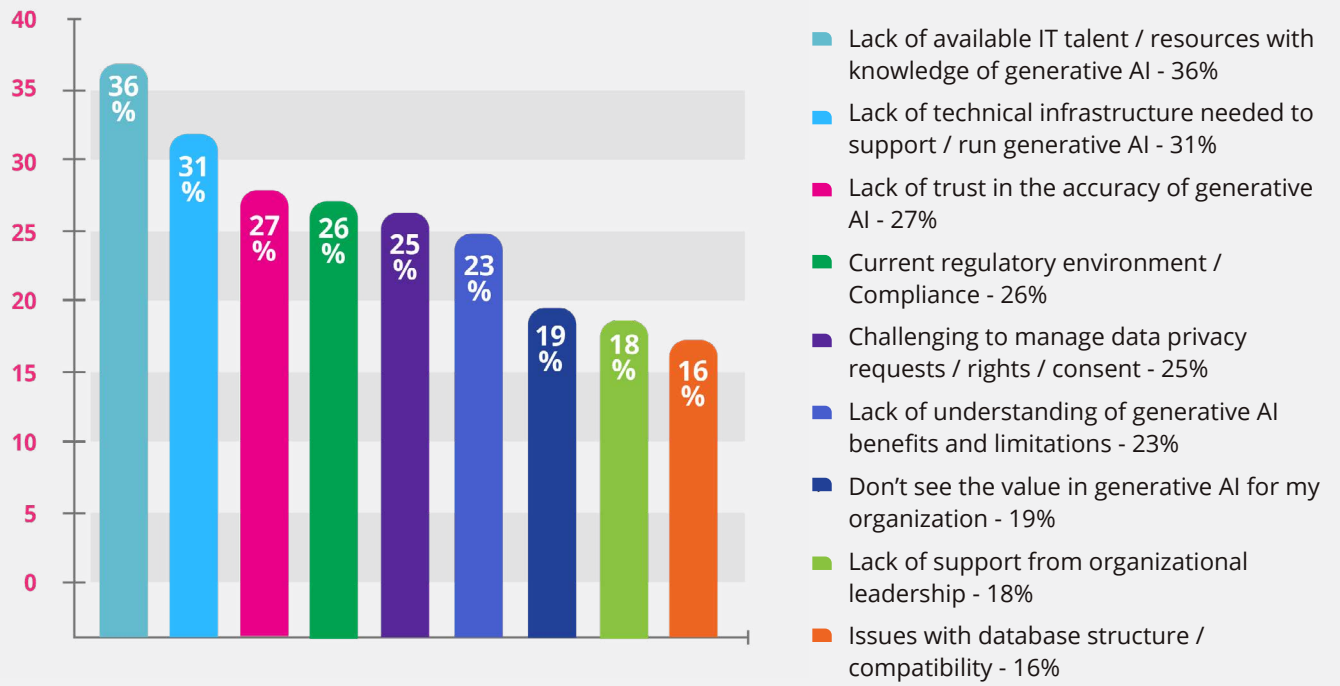
While interest in AI adoption is significant, organizations encounter various barriers that impede its widespread implementation. These barriers encompass regulatory challenges, a shortage of essential infrastructure and skilled talent, and concerns about the accuracy of AI applications.

A notable 67% of organizations yet to embrace AI cite a crucial gap: the need for proficient talent and advanced technical infrastructure. This issue is not a minor impediment but a substantial roadblock to digital transformation. Accuracy concerns in generative AI are often rooted in incomplete data visibility and control. Issues arise from inadequate data visibility, context, and insights - generative AI relies heavily on high-fidelity data and metadata understanding for accurate outputs.

Equally important is the challenge of comprehensive data governance. Maintaining the integrity and appropriateness of data used in AI applications can be hampered, leading to potential inaccuracies. Furthermore, the lack of governance of training data can lead to issues beyond just performance, including security, privacy, and risk complications.

One in four organizations consider the lack of trust in accuracy as a barrier to generative AI adoption.

Q For what reasons is your organization not currently using AI?



Emphasizing the importance of data visibility and control is pivotal in establishing the essential technical foundation for AI adoption. Utilizing tools that offer thorough data discovery, comprehensive classification, effective categorization, and precise flagging, tagging, and labeling is key to ensuring organizational success. A profound and contextual grasp of the data environment empowers generative AI applications to deliver superior and more accurate results.

Establishing adequate visibility and control throughout the data environment is paramount for achieving enhanced security and governance outcomes. It involves implementing robust policies and tools for effective data management, incorporating techniques to control, audit, and monitor data shared with AI applications. These measures are essential to guarantee data accuracy and compliance with privacy and security regulations. As AI technology advances, an organization's proficiency in managing its data effectively will be a critical factor influencing its success in leveraging AI.

Section 4
Key Decision-Making Criteria for Adopting AI

Key Decision-Making Criteria for Adopting AI

Factors of Influence: Security, Privacy, & Transparency

Security concerns play a significant role in shaping the decisions of organizations contemplating the integration of generative AI. The looming threat of data breaches and ransomware attacks serves as a formidable deterrent, emphasizing an increased awareness of vulnerabilities in the latest AI applications. This underscores the imperative of implementing robust security measures to effectively mitigate these risks and foster a secure environment for AI adoption.

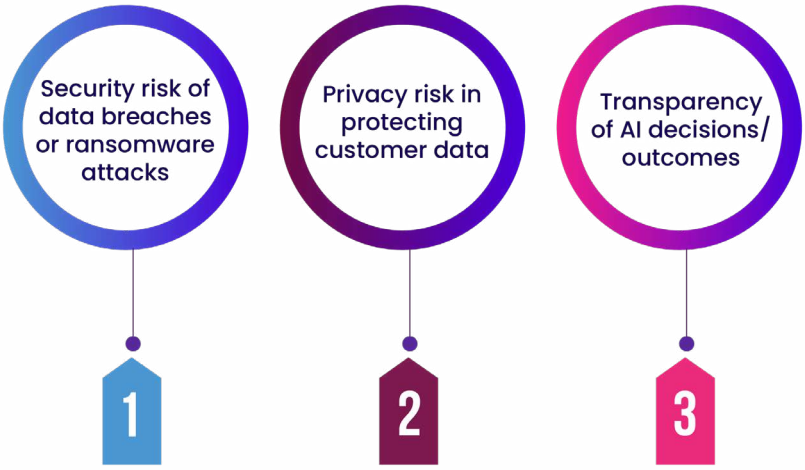
Protecting customer data privacy also plays a pivotal role in decision-making. As AI applications handle large volumes of data, ensuring the confidentiality of sensitive customer information becomes paramount. The focus on privacy reflects an increasing trend towards stringent data privacy and the need to align AI practices with data protection regulations.

Transparency in AI decisions and outcomes stands out as another crucial factor. Organizations are now prioritizing AI solutions with transparent and accountable operations, steering clear of the opaque nature exhibited by some AI applications. This shift toward transparent AI practices signifies a rising preference for responsible and understandable AI implementations.

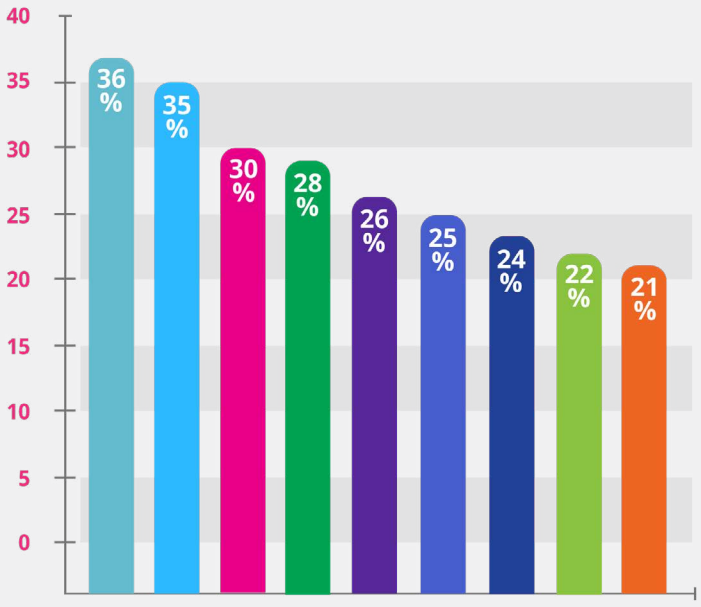
Together, these concerns shape a cautious yet strategic approach toward AI adoption. Organizations are keenly aware of balancing innovation with risk management and ethical considerations. The emphasis on security, privacy, and transparency in decision-making highlights the complex landscape of generative AI integration, where effective data management and governance play a crucial role in navigating these challenges.

Cybersecurity threats, such as data breaches or ransomware, emerge as the **biggest influence** in deciding to adopt generative AI.

The top three influences when deciding to adopt generative AI:



Q How influential are each of the following in your organization's decision-making processes related to generative AI?



- 36% - Security risks, such as data breaches or ransomware attacks
- 35% - Privacy risks in protecting customer data
- 30% - Transparency of AI decisions / outcomes
- 28% - Existing AI laws and regulations
- 26% - Ethical implications like surveillance practices or data bias
- 25% - Cross-functional collaboration (e.g. IT, Security, Legal, Business)
- 24% - Data governance policies & procedures for managing data
- 22% - Explainability of AI models across departments
- 21% - Inclusion / Management of unstructured data (e.g. emails and chats, etc.)

Section 5
Challenges When Implementing AI

Challenges When Implementing AI

AI Integration Hurdles: Securing Data and Fostering Cross-Functional Synergy

As organizations integrate AI into their operations, they encounter various challenges, with data security emerging as the top concern. Half of organizations that are currently using AI highlight data security as their biggest challenge.

Addressing data security in AI involves more than safeguarding stored information; it extends to ensuring the integrity and confidentiality of data throughout AI applications. This challenge demands deploying advanced solutions to identify and protect sensitive data, manage access controls, and continuously monitor for vulnerabilities. By focusing on these aspects, organizations can establish a solid foundation for AI initiatives, ensuring data security while maximizing AI's potential.

Alongside data security, fostering efficient collaboration between IT, Security, Legal, and Business departments emerges as a critical aspect, with 47% of AI users. Such collaboration is vital to harness AI's broad organizational impact effectively. Additionally, for 45% of adopters, ensuring the transparency of AI decisions and outcomes is a significant concern, underlining the need for transparent and accountable AI processes.

There are distinct priorities for businesses on the cusp of adopting generative AI. Surprisingly, cross-functional collaboration, a significant concern for current users, ranks least for future adopters at only 26%. This discrepancy suggests a potential underestimation of the complexities of seamlessly integrating AI across various business functions.

Successfully navigating these challenges requires organizations to implement comprehensive data security and governance strategies. However, this starts with having a strong data discovery and classification foundation to allow organizations to establish a complete and unified data inventory, for data leveraged for AI training. This allows multiple lines of business - including IT, security, legal, and business departments - to revolve around a single source of truth about the data environment, which inevitably fosters better collaboration and action to mitigate unwanted exposure from AI. Combined, with the right data access controls and continual data security posture assessments, organizations can ensure the responsible and effective use of AI applications.

Organizations identify Data Security as the biggest challenge challenge when implementing AI (50%), followed by cross-functional collaboration (47%).

Q Which of the following areas are / were most challenging to your organization when adopting / integrating generative AI?

Underestimating of Certain Challenges

There's a possibility that organizations planning to adopt AI are underestimating challenges such as data security, transparency of AI decisions, and cross-functional collaboration. These areas often reveal their complexity only during practical implementation, which the planning organizations might not yet appreciate.

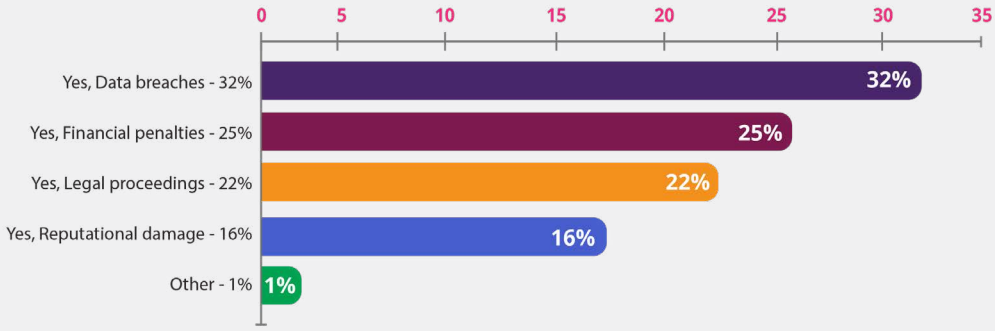
Section 6
Adversity When Using Generative AI

Adversity When Using Generative AI

The AI Paradox: Raid Adoption Brings Innovation & Adversity

Nearly 50% of organizations report adverse business outcomes related to AI usage, with data breaches being the most prevalent.

Q Thinking of the past 12 months, have you experienced any adverse outcomes related to generative AI



The rapid integration of generative AI into business operations while addressing the need for innovation also presents significant challenges. The sobering reality is that nearly half of companies (49%) have encountered adverse outcomes following the adoption of generative AI. Data breaches, impacting 32% of organizations, are the most prominent threat, demanding robust security measures in the AI-powered business landscape.

Additionally, 25% face financial penalties and 22% have legal issues, further painting a picture of non-compliance and ethical shortcomings. Plus, 16% of organizations suffer from reputational damage, a stark reminder of the long-term consequences of AI challenges.

These findings highlight the complexities and potential pitfalls of integrating generative AI. Companies reporting data breaches must implement more robust security measures, including encrypting data, regularly updating security protocols, and monitoring for unauthorized access. While implementing stronger security measures is essential, it's not about whether a data breach will happen but about when it happens; organizations must have a well-defined data breach response plan. Detecting and investigating data breaches to understand the full scope and impact will help determine the immediate steps for mitigating and remediation.

Those reporting financial and legal penalties further stress the importance of maintaining compliance and adhering to ethical standards during and after AI deployment—the potential for reputational harm points to the importance of cautious and well-considered AI integration strategy. Organizations must incorporate forward-thinking data risk management and security postures to mitigate these risks. It's also important to note that collaborations across the organization are vital to any AI adoption. By embracing these strategies, organizations can address the inherent risks of generative AI, ensuring the secure and compliant use of AI across their operations.

Mitigating AI-Related Challenges

In response to the survey's findings on AI-related challenges, particularly around data breaches, organizations can enhance their AI risk mitigation strategies by prioritizing comprehensive data visibility and control - which includes proper data classification, categorization, flagging, tagging, and labeling. These practices not only ensure data suitability for AI but also shield it from unauthorized access and misuse. A robust data security strategy built on this foundation is crucial. Understanding and controlling your data is the bedrock of secure AI applications.

But it's not just about control – it's about proactive risk management. With complex data comes the risk of exposing sensitive information. Advanced tools and techniques can help automatically detect and address threats before they escalate, minimizing the risk of breaches. This makes risk management integral to building resilient and secure AI applications.

However, security alone isn't enough. AI operates in a dynamic landscape with evolving ethical considerations and compliance regulations. Regularly updating data management practices to align with current standards ensures responsible AI deployments. By balancing AI's potential with legal and ethical obligations, we build trust and reliability in these technologies.

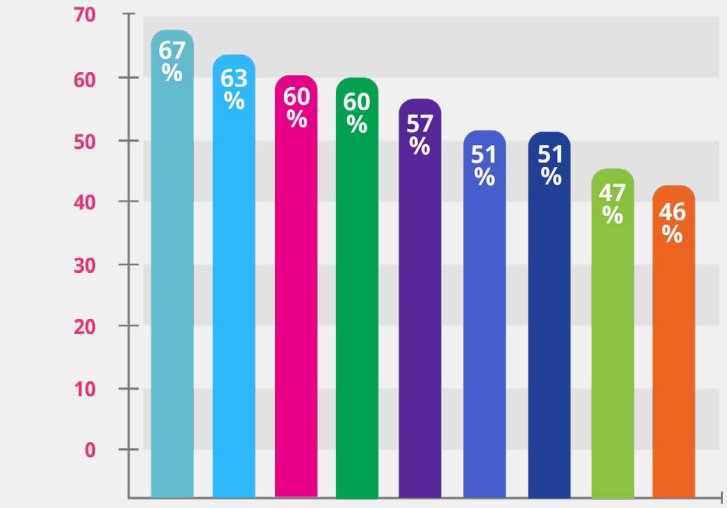
Section 7
AI Concerns

AI Concerns

Balancing Innovation with Responsibility: Key Concerns When Deploying AI

More than two-thirds of organizations rank security risks, like data breaches, as their top AI concerns.

Q From the list below, indicate the Top 5 topics of concern to your organization with regards to generative AI. #1 = Most Concerning, #2 = Second Most Concerning, etc. up to five characteristics

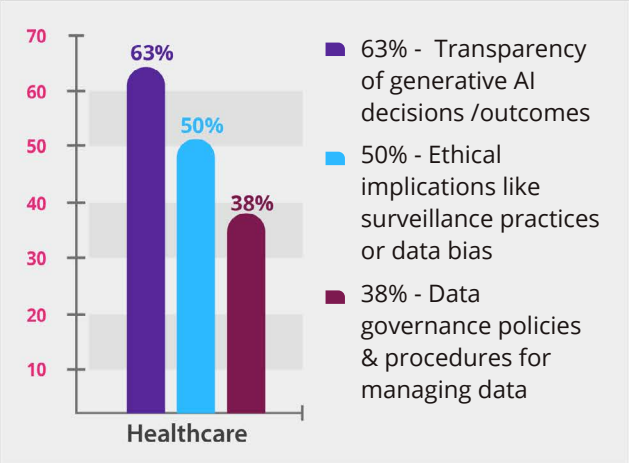


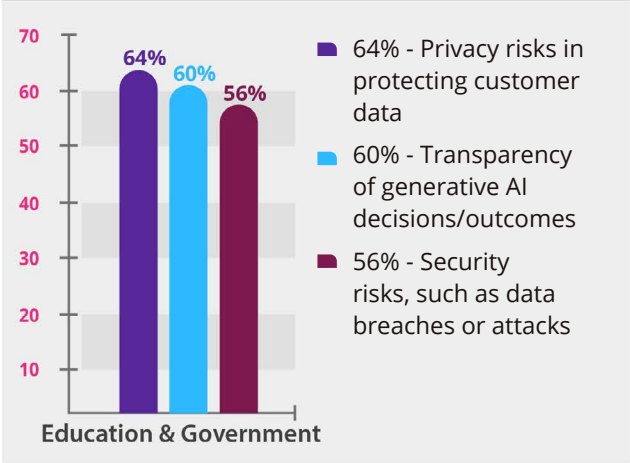
- Security risks, such as data breaches or attacks - 67%
- Privacy risks in protecting customer data - 63%
- Transparency of generative AI decisions / outcomes - 60%
- Data governance policies & procedures for managing data - 60%
- Ethical Implications like surveillance practices or data bias - 57%
- Explainability of generative AI models across departments - 51%
- Familiarity with existing AI laws and regulations - 51%
- Cross-functional collaboration (e.g. IT, Security, Legal, Business) - 47%
- Inclusion / Management of unstructured data (e.g. emails and chats, etc.) - 46%

Adapting to Industry-Specific AI Concerns

In sectors like healthcare, where the emphasis is on transparency in AI decision-making, organizations face unique challenges in maintaining data accuracy and ethical standards. Likewise, education and government sectors prioritize security and privacy risks, necessitating stringent data protection and risk management practices.

In these sectors, organizations must adopt comprehensive strategies to control and audit the data shared with AI applications. This includes establishing AI data usage policies and ensuring adherence to these policies. It is essential to be vigilant about what data is shared based on privacy, sensitivity, regulation, and access. Regular audits and inspections of shared data, policy enforcement, and breach alerts can significantly enhance AI governance and data security.





Mitigating Data Risks in AI Across Diverse Industries

In sectors like healthcare, education, and government, where sensitive information abounds, the integration of robust Data Security Posture Management (DSPM) solutions is indispensable when incorporating generative AI. DSPM empowers organizations to proactively monitor, assess, detect, investigate, and remediate potential data risks and vulnerabilities associated with AI applications. By leveraging DSPM, organizations can consistently uphold stringent data security measures, showcasing their proficiency in safeguarding their most valuable and sensitive information. Effective DSPM involves a thorough understanding of the data environment, encompassing its location, sensitivity, accessibility, flow, and associated exposure risks. Regular data security and risk posture assessments are crucial for proactively identifying and mitigating vulnerabilities. Integrating governance policies and ethical considerations ensures that AI applications meet regulatory standards and maintain stakeholder trust.

As AI technology continues to evolve and permeate various sectors, adopting a comprehensive DSPM strategy becomes imperative. These methodologies contribute to regulatory compliance, instill confidence in AI applications, and ensure they remain secure, transparent, and ethically aligned with industry-specific standards.

Section 8
Protecting Sensitive Data When Using AI

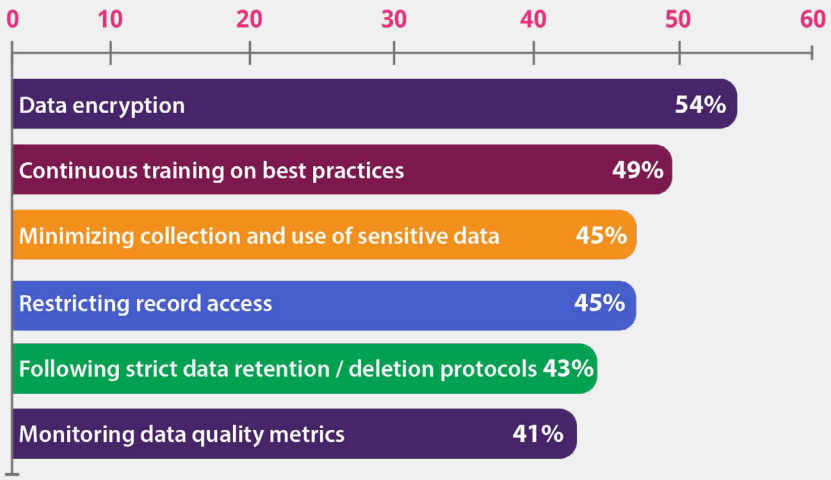
Protecting Sensitive Data When Using AI

Ensuring Data Privacy: How Organizations are Protecting Sensitive Information for AI Use

Safeguarding sensitive information has emerged as a paramount concern in an age where AI plays an ever-expanding role in processing immense volumes of data. The report underscores the diverse strategies employed by organizations to ensure data privacy. These include data encryption, ongoing employee training, and the limitation of access to sensitive data. It's essential to note that the efficacy of these measures relies on meticulous implementation and frequent updates, critical for addressing the dynamic landscape of cyber threats and the evolving nature of AI applications.

Only 43% of organizations adhere to strict data retention and deletion controls when using AI.

Q How is your organization safeguarding user confidentiality when handling unstructured data?



Closer Look into Key Methods and Potential Gaps

- **Data Encryption:**
  Essential for thwarting unauthorized access, requiring frequent updates to combat evolving cyber threats.
- **Continuous Employee Training:**
  Key to minimizing human error, requiring ongoing updates to cover new security threats and best practices.
- **Data Retention & Minimization:**
  Consistently removing redundant, obsolete, and non-essential sensitive data enhances security. Regular deletion aligns with evolving business needs and threat landscapes.
- **Access Control:**
  Vital for evaluating, managing, governing, and remediating access to sensitive data, necessitating regular reassessment for efficacy without impeding AI functionalities.
- **Data Quality Monitoring:**
  Crucial for ensuring data integrity, foundational for security, and optimal AI performance. Regular monitoring upholds quality standards effectively.

By prioritizing these strategies and conducting regular reviews and updates, organizations can enhance the protection of sensitive data within AI applications, effectively addressing both existing and emerging security challenges. For a more in-depth understanding of securing and governing AI, please consult sections 5 and 6, where essential best practices are meticulously detailed.

Effective data protection in AI involves more than implementing standard security measures. Organizations need to adopt a comprehensive approach to data lifecycle management, focusing on retention and deletion.

Managing the lifecycle of data includes:

- Understanding what data is collected.
- Assessing its relevance and risks.
- Applying appropriate retention and deletion policies.

To overcome these challenges, organizations should leverage advanced data discovery and classification solutions. These tools play a crucial role in seamlessly applying retention, remediation, and deletion policies, adeptly handling legal exceptions, and ensuring alignment with internal policies and external regulations. It is imperative to establish secure data deletion processes that adhere to privacy regulations, encompassing the implementation of approval workflows and the meticulous maintenance of audit trails. Adopting this proactive stance towards data lifecycle management is pivotal for mitigating privacy risks and fostering ethical and responsible data utilization within the dynamic landscape of generative AI.

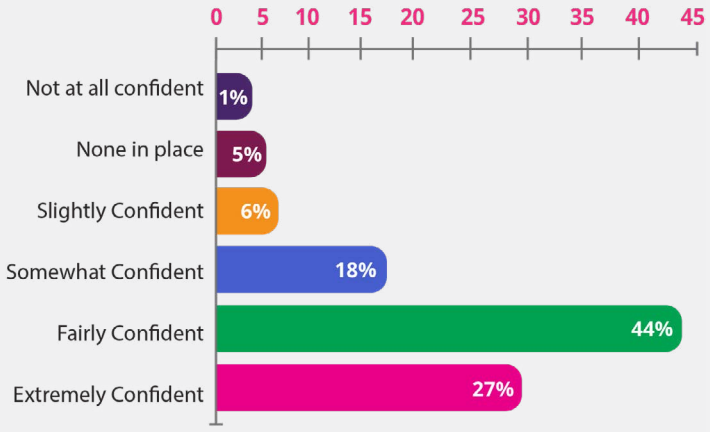
Section 9
Securing AI

Securing AI

Fortifying Defenses: Addressing the Security Confidence Issues When Incorporating AI

73% of organizations are not fully confident in their data security measures regarding generative AI.

Q How confident are you in your organization's data security measures regarding generative AI, if currently in place?



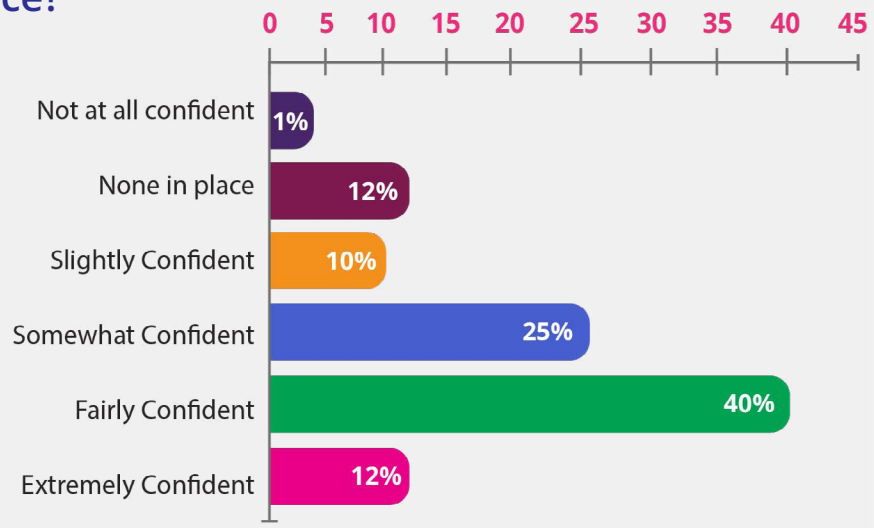
The survey reveals a significant concern among organizations regarding the effectiveness of their existing security measures in mitigating issues associated with generative AI. This lack of confidence underscores the critical importance for organizations to assess and fortify their security strategy. It's not merely a matter of having security measures in place; rather, they must be robust enough to adeptly address the challenges inherent in generative AI technologies.

Collaborating closely with the Chief Information Security Officer (CISO) and the broader security team, the following essential measures should be implemented to enhance the security of your data, minimizing the risk of unauthorized exposure, access, and utilization in the context of AI applications:

- **Identify AI Training Model Data:**
  Discover sensitive, personal, and regulated information in AI training sets, including secrets and passwords, customer data, financial data, IP, confidentiality, and more.
- **Enforce Data Security Policies:**
  Enforce policies around sensitive data to monitor data location and movement with respect to AI, and trigger the right security controls.
- **Implement Access Control:**
  Implement strict access control measures to ensure only authorized individuals and AI applications can access and modify sensitive data - both internally and externally.
- **Data Transfers & Sharing:**
  Follow secure file transfer protocols when transferring sensitive data between systems or to third parties; secure protocols should be used to maintain data security.
- **Data Encryption:**
  Secure sensitive data transmitted over networks, preventing interception. If data is stored in the cloud, encryption should be applied to data at rest and during transfer.
- **Monitor AI Applications:**
  Constantly monitor AI applications for unusual or malicious activities. Routine security audits help evaluate and improve AI security, providing an active defense against vulnerabilities.

When looking at organizations planning to implement generative AI, the percent increases to 88% of organizations are not fully confident in their data security measures regarding generative AI.

Q How confident are you in your organization's data security measures regarding generative AI, if currently in place?



Section 10
Governing AI

Governing AI

Strengthening Foundations: Enhancing Data Governance for AI Readiness

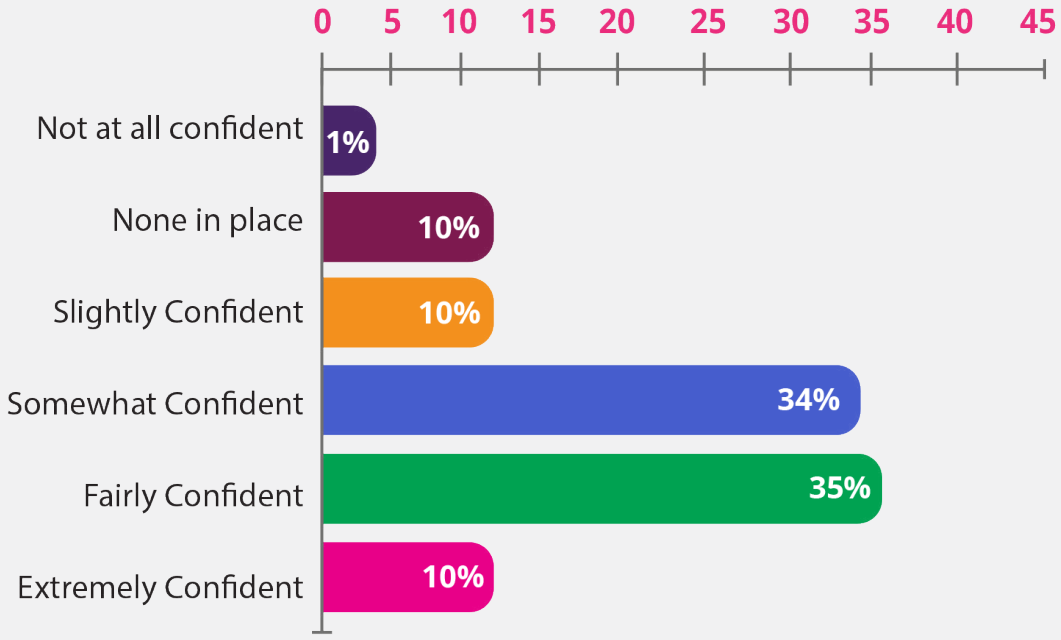
The survey results expose a notable disparity in the confidence levels that organizations harbor regarding their data governance policies, especially concerning generative AI. This discrepancy highlights the pressing need for a comprehensive reassessment and reinforcement of data governance frameworks.

Effective data governance is pivotal for overseeing AI applications to ensure their reliability, ethical conduct, and compliance with regulations. Managing data throughout its lifecycle, from initial collection to final deletion, is crucial. Updating governance policies to specifically address AI's challenges, with a focus on data quality, lineage, and algorithm transparency, is essential.

Organizations must stay current with data protection laws to ensure their AI applications are compliant. Regular data quality audits, meticulously documenting data sources and AI models, and implementing robust data security controls are crucial. Involving stakeholders from various departments in policy development and ongoing training for staff on their roles in data governance is critical. Continuously reviewing and adapting these policies to align with evolving AI technologies and business needs helps organizations use AI responsibly and effectively.

90% of organizations preparing for AI report a lack of full confidence in existing data governance approaches.

Q How confident are you in your organization's data governance policies regarding generative AI, if there is a governance policy in place?



Section 11
Meeting AI Regulations & Compliance

Meeting AI Regulations & Compliance

Navigating Regulatory Complexity and Uncertainties

Given that 72% of organizations harbor concerns about aligning with upcoming AI regulations and compliance, skillfully navigating the intricate legal landscape of generative AI becomes a top priority. Central to this endeavor are thoughtful considerations of data privacy, security, risk management, and ethical usage. Organizations must acquire a comprehensive understanding and ensure adherence to relevant laws, which can vary by region and industry – examples include GDPR in Europe and COPPA or HIPAA in the United States.

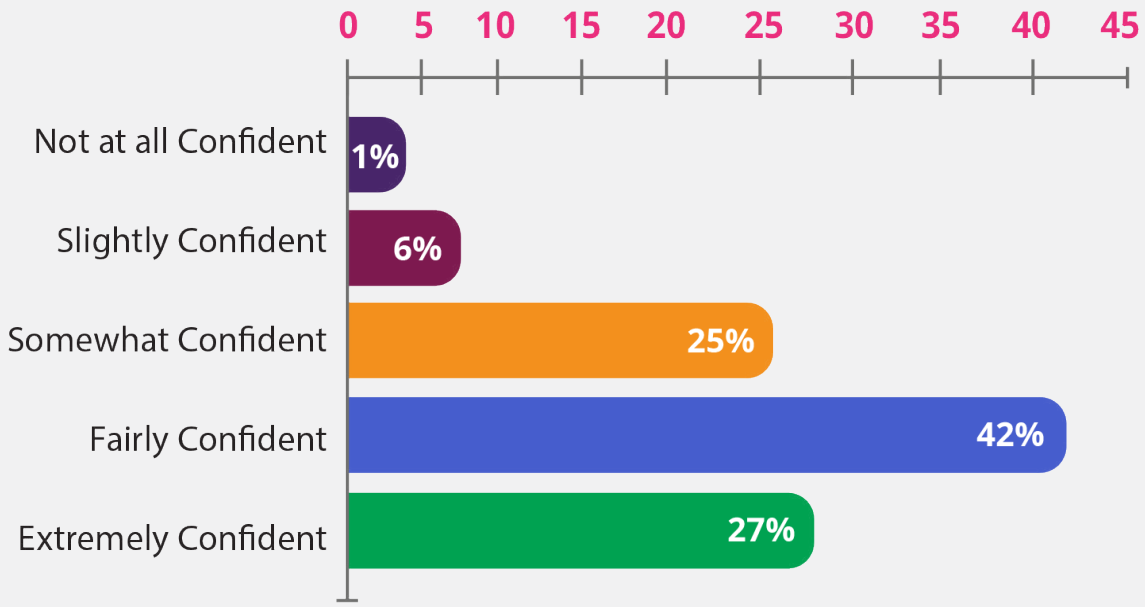
Establishing a robust AI data governance framework is fundamental. This framework should clearly outline data collection, processing, and sharing while embedding ethical development and usage. This framework necessitates clear policies, oversight mechanisms, risk management strategies, and assessing and updating AI applications for ethical standards and legal requirements. Transparency in AI decision-making processes is also vital, particularly for compliance with regulations such as GDPR's Article 22.

Conducting Privacy Impact Assessments (PIAs) becomes imperative, particularly for AI applications involving personal data. These assessments evaluate privacy risks and initiate safeguards to protect individual privacy. Data security measures, including encryption, access control, and secure data transfers, are paramount for maintaining data confidentiality and integrity. In the event of data breaches, a comprehensive response plan is necessary for efficient notification and mitigation efforts. This plan should involve collaboration across various organizational teams, ensuring a holistic approach to privacy risk management.

Anticipating future AI regulations and compliance, particularly in the realm of Generative AI, is an evolving and continuous undertaking that necessitates a comprehensive and well-rounded approach. This involves a deep understanding of legal requirements, the establishment of a robust governance framework, emphasizing ethical considerations, and an unwavering commitment to transparency and data protection.

72% of organizations lack full confidence in meeting future AI regulations and data compliance requirements.

Q How confident are you in your organization's ability to meet any future generative AI regulations and compliance with respect to your data?



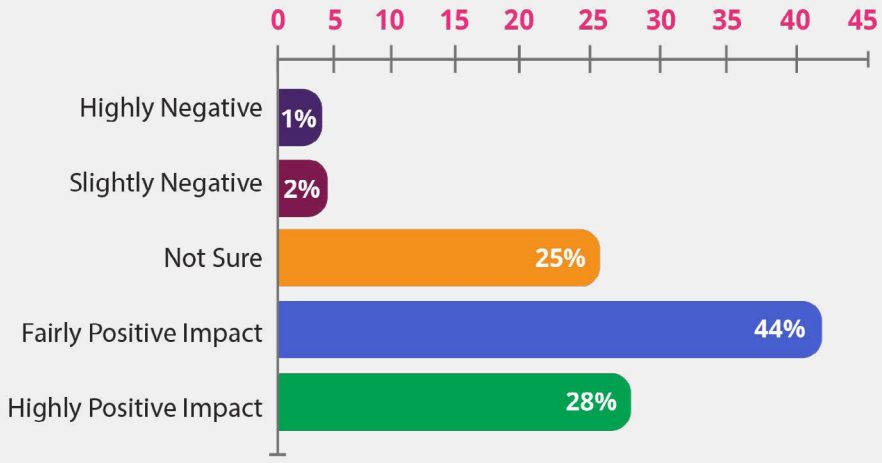
Section 12
Current Sentiment on the Future of AI

Current Sentiment on the Future of AI

Charting Tomorrow: Unleashing AI for a Brighter Future

Generative AI's Bright Future: 72% of organizations foresee generative AI having a positive impact over the next five years.

Q Now thinking about the next five years, do you foresee generative AI having a positive or negative impact on your business?



Despite the challenges associated with adopting and implementing generative AI, there is a strong optimism about its future positive impact. This optimism is fueled by the technology's potential to drive significant innovations, enhance operational efficiency, and boost productivity across various sectors. From addressing complex challenges in healthcare diagnostics and environmental conservation to transforming customer service through personalized interactions, generative AI is positioned to play a transformative role in diverse industries, showcasing its capacity for innovation, problem-solving, and economic growth.

Potential Areas of Impact:

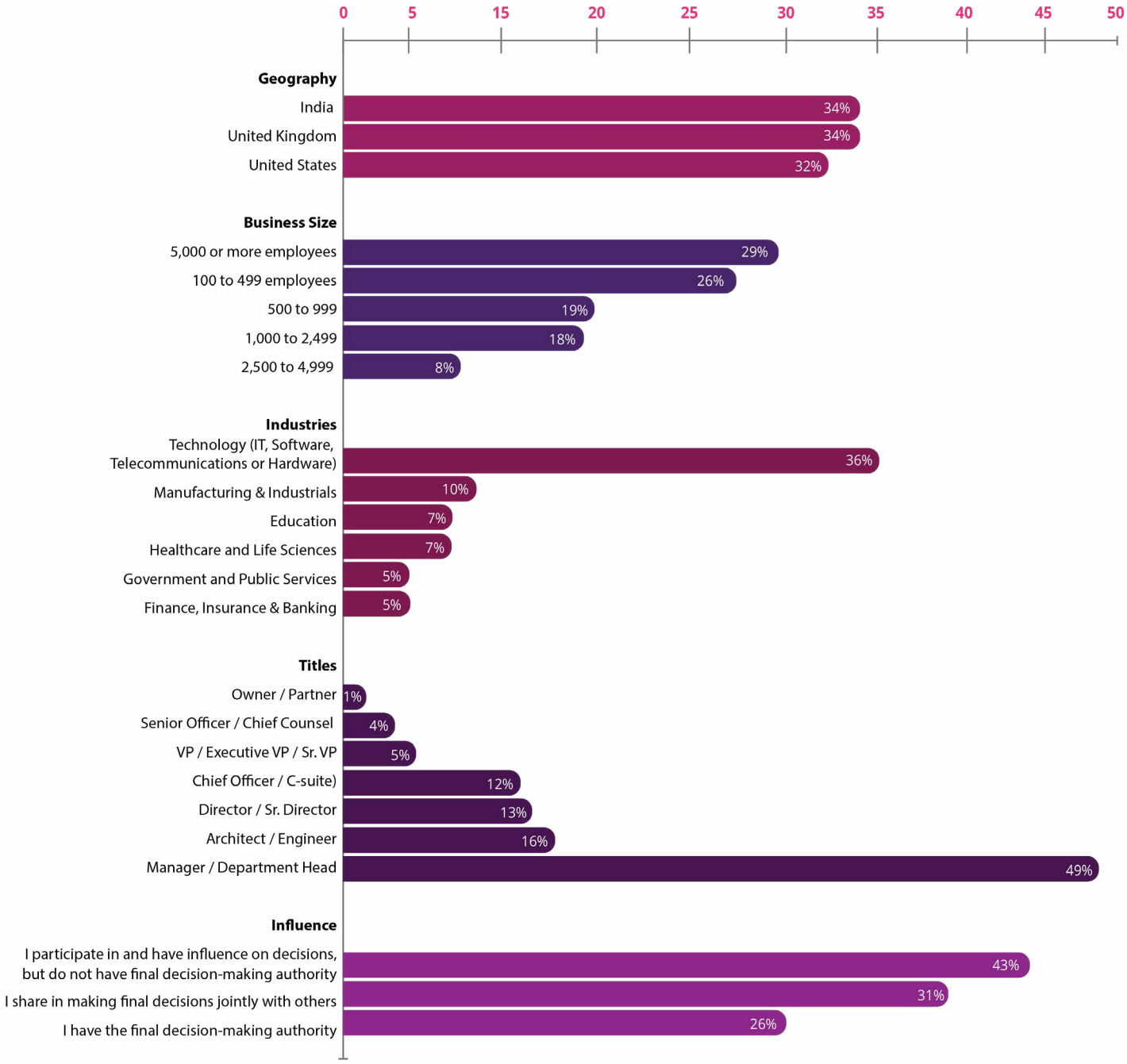
- **Healthcare:**
  AI's application in diagnostics, treatment personalization, and research could revolutionize patient care and medical outcomes.
- **Finance and Banking:**
  AI is expected to enhance financial services through improved risk assessment, fraud detection, and customer service.
- **Retail and E-Commerce:**
  AI can significantly impact how businesses interact with customers, offering personalized shopping experiences and efficient supply chain management.
- **Education:**
  Personalized learning experiences and enhanced educational tools could be realized through AI, potentially transforming the educational sector.
- **Environmental Conservation:**
  AI's role in monitoring and addressing environmental issues could be pivotal in efforts towards sustainability.

Generative AI's impact on data security, privacy, governance, and compliance is profound and multifaceted. As organizations chart their course toward a future enriched by AI, they must put a greater emphasis on how they manage and protect their data with diligence. AI's integration into various sectors increases its responsibility to protect sensitive data, uphold privacy standards, and ensure ethical compliance.

Managing AI within the workplace requires rigorous governance controls to mitigate risks associated with data breaches and privacy infringements. Additionally, the compliance landscape is evolving rapidly, with AI technologies at the forefront, requiring organizations to stay agile and informed about regulatory changes. As AI continues transforming industries, the need for strong frameworks that ensure the secure, private, and compliant use of AI becomes a priority. This approach not only safeguards organizational interests and consumer trust but also strengthens AI's positive potential for innovation and complex problem-solving.

Despite acknowledging the challenges, there is a strong belief in the transformative power of AI. This optimism is rooted in AI's capacity to fuel innovation, spur economic growth, and bring about advancements across diverse fields, promising a substantial positive impact in the years ahead.

Respondent Breakdown



About BigID

BigID enables security, compliance, privacy, & governance for all data, everywhere. BigID is enterprise-ready and built to scale: enabling a data-centric approach to comprehensive cloud data security & DSPM, accelerating compliance, automating privacy, and streamlining governance. Customers deploy BigID to proactively discover, manage, protect, and get more value from their regulated, sensitive, and personal data across their data landscape.

BigID has been recognized for innovation as a 2019 World Economic Forum Technology Pioneer; named to the Forbes Cloud 100; the Inc 5000 for 3 consecutive years; the Deloitte 500 for 3 consecutive years; Market Leader in Data Security Posture Management (DSPM); Leader in Privacy Management in the Forrester Wave; and an RSA Innovation Sandbox winner.

Find out more at https://bigid.com.

Know Your Data, Control Your Data.

Data Security • Compliance • Privacy • Governance

Reduce risk, accelerate time to insight, and get data visibility and control across all your data - everywhere.

> **Tools like BigID are the future.**
> Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.
>
> IDC
> Ryan O'Leary
> Future of Trust: Battling Data Discovery Confusion