For Unutilized Data, Security and Privacy Concerns Face Some Blame

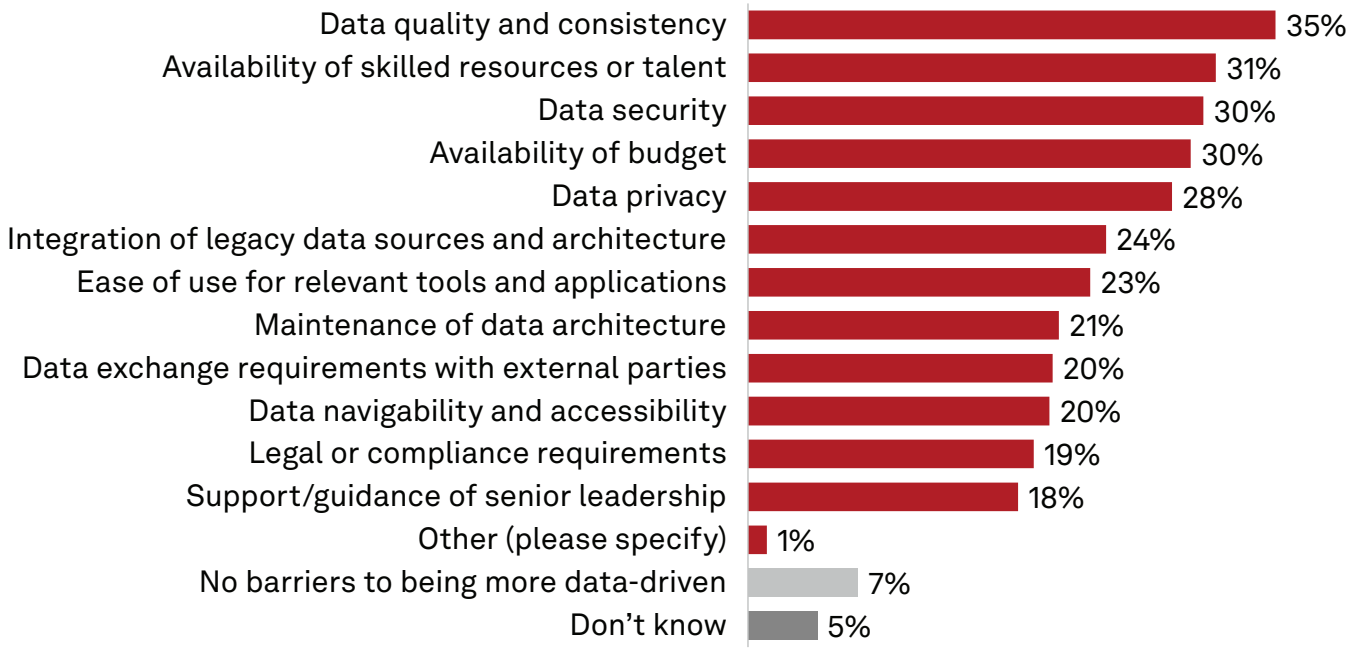
The 451 Take

Many organizations today are still struggling to gain optimal value from the data they have available. This problem is exemplified by so-called "dark data" — data that has been generated by the business but is not currently used in analytics projects to generate business insights.

Based on 451 Research's Voice of the Enterprise: Data & Analytics, Data Platforms 2021 survey, roughly 45% of enterprise data under management is reported as being dark data. The actual amount of unutilized data within the average enterprise is likely even higher, due to data sources that are unreported, not actively managed or restricted from certain uses. Furthermore, the data that is being actively used may have unacknowledged problems in terms of quality and consistency.

Why are many organizations so far behind in extracting business value from their data? It's not due to a true lack of data. Growth of data remains exponential in most cases, making consistent data management difficult. But there are other pain points and concerns that limit the generation of insights from this data. Top challenges here often relate to data quality, data security, data privacy and integration of data architecture. Analytics initiatives, specifically, also face issues around data quality, security and privacy. Based on 451 Research's Voice of the Enterprise: Data & Analytics, Data-Driven Practices 2022 survey, these technical pain points all rank among the top overall challenges that organizations face in becoming more data-driven.

Most Significant Barriers Faced in Becoming More Data-Driven



Q. What are the most significant barriers your organization faces in attempting to be more data-driven? Please select all that apply.
Base: All respondents (n=477)
Source: 451 Research's Voice of the Enterprise: Data & Analytics, Data-Driven Practices 2022

Many organizations are trying to establish the concept of a "data culture" to help accelerate outcomes based on business insight gained from data. Building a data culture means making data more easily accessible to workers in everyday roles, while simultaneously ensuring appropriate controls for security and privacy. Some of the steps that businesses have taken to do this include establishing self-service visualization/analytics programs, as well as programs for secure exchange of data with external parties. Nearly 70% of respondents to the Data-Driven Practices 2022 survey say their organizations have a program for secure exchange of data with external parties such as partners or suppliers. Yet these programs are often hampered due to international data transfer restrictions, and sometimes lack true control over datasets once they leave the hands of the originating organization.

The motivations for appropriate data security and privacy extend beyond regulatory and legal requirements. Data privacy is increasingly becoming a customer experience issue, with customer trust affecting the bottom line. According to 451 Research's Voice of the Connected User Landscape, Connected Customer, Trust & Privacy 2022 survey, 78% of U.S. consumers are concerned about the privacy of their data online. Furthermore, consumers place the burden of responsibility for data privacy on businesses. In the same survey, 39% of individuals that are not willing to pay a modest hypothetical monthly fee to secure their data online cite their top reason as being, "It is the responsibility of the business or entity collecting and using my data to keep it private and secure."

Business Impact

Enterprise data often goes unutilized in analytics due to issues around data quality, security and privacy. A high proportion of enterprise data is dark data or restricted data that goes unutilized in analytics and data science programs. Common technical barriers include data quality/consistency, data security, data privacy and architectural integration with existing IT investments. Tapping the value of data means addressing these problems, so that insights can be both trusted and secure, and adding interoperable solutions to existing technology stacks rather than "ripping and replacing."

Building enterprise data culture means making data more accessible to workers, while ensuring privacy and security. Enterprise data culture needs to balance data accessibility with data security and privacy, yet these objectives are not necessarily at odds. Consistent technical controls for privacy and security can actually liberate the use of datasets to groups of enterprise end users that may have been entirely blocked from access before. Individual workers do not necessarily need to see the granular details of data to benefit from analytics-derived insights.

Data privacy and security are a must not only for compliance, but also for customer trust and engagement. Consumers are becoming much more sensitive to perceived violations of data privacy and security. They change their behavior accordingly when they believe their data is threatened — often in ways that affect a business's bottom line. Modern customer experience practices should be intertwined with data privacy and security practices, giving consumers the confidence they need to engage digitally.

Looking Ahead

Any enterprise that fails to recognize consistent data privacy and security as foundational elements of modern analytics initiatives is destined for a difficult journey. No longer constrained to regulatory requirements, data privacy and security are permeating consumer consciousness. Cultivating customer trust around the use and stewardship of personal data is necessary to build high-value, lasting relationships.

The data control mechanisms necessary for ensuring data privacy and security are the same underlying mechanisms that help the enterprise tackle persistent issues such as data quality. These problems are not isolated, and should be addressed together. For too long data security and privacy have been treated as add-on features rather than something inherent to successful analytics efforts. For a data privacy function such as pseudonymization to succeed as a means of using more data, the business needs full control of datasets. Fully addressing data privacy and security does not necessarily mean that an organization needs to "rip and replace" IT architecture. Interoperability is becoming much more common, and any organization looking to purchase new technology should first take inventory of existing IT investments.