Developing a Data-Sharing Leadership Playbook

Presented by MIT CDOIQ in collaboration with Privacy Analytics, held on 19 July 2021

Watch this executive roundtable on-demand

Based on background research conducted and in consultation with MIT Chief Data Officer & Information Quality program (MIT CDOIQ), Privacy Analytics identified "data sharing" as an issue of significant importance to Chief Data Officers (CDOs) and similar senior-level data and analytics leaders. In this exclusive, deep-dive roundtable discussion, executive data leaders explored what's worked and what hasn't from across multiple industries, in both the private and public sectors. The discussion focused on defensive strategies to govern data and limit risk, and offensive strategies to drive business opportunities and realize new value when sharing sensitive data.

Three key takeaways emerged from this event:

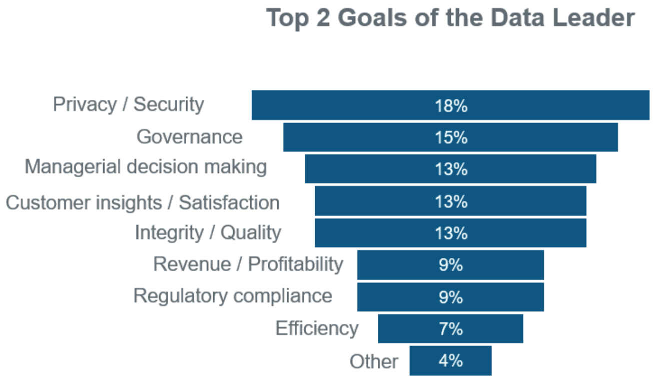
- Engage and motivate stakeholders early and throughout the data journey, with a focus on their business needs rather than technical details.
- Establish standard processes and tools that can more easily facilitate data sharing initiatives.
- Strike the right mix of offensive and defensive strategies to enable successful data sharing.

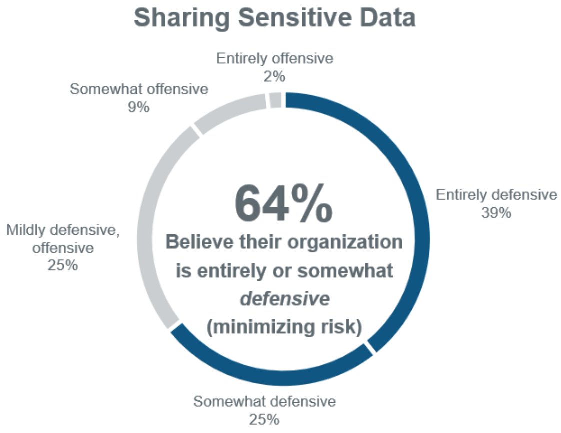
Emerging trends in sensitive data sharing

MIT CDOIQ and Privacy Analytics polled data leaders at an event held on May 19, 2021. Respondents believed their organizations were using sensitive data often/all the time, but more could be done to drive value. The poll results also showed that:

- Respondents ranked their "top job" as analytics officer & data entrepreneur (37%) followed by data governor (23%) -- essentially, offense first, defense second.
- 68% of respondents said their organizations use sensitive data often or for every innovation & service improvement; but believed their organizations could drive more value with increased sharing (92% internal, 80% external)
- Barriers to data sharing were primarily privacy, security, and legal concerns

At our 19 July 2021 event on data sharing, over 50 data leaders chose to participate in audience polls (over a 70% response rate). The introductory poll results below show participant focus areas and the perception they have of their organization's risk appetite regarding the uses of sensitive data. We described sensitive data to be any data derived from people, be it identified with their name or transformed in any way, including aggregated. The results suggest that participants' top leadership goals are privacy / security and governance. These are closely followed by managerial decision making, customer insights and satisfaction, and integrity and quality. The results also suggest that participants believe their organization is entirely or somewhat defensive (minimizing risk).


Top 2 Goals of the Data Leader

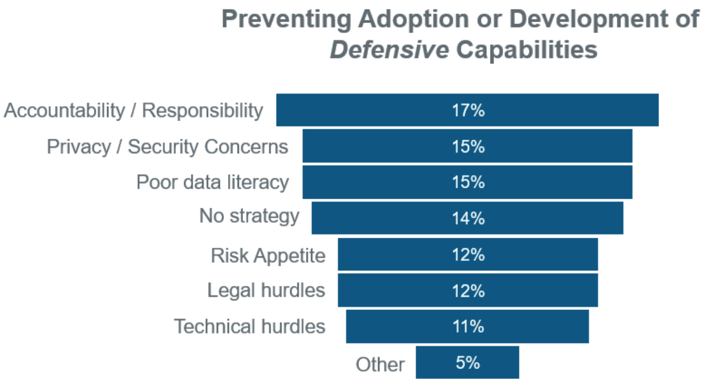

Sharing Sensitive Data

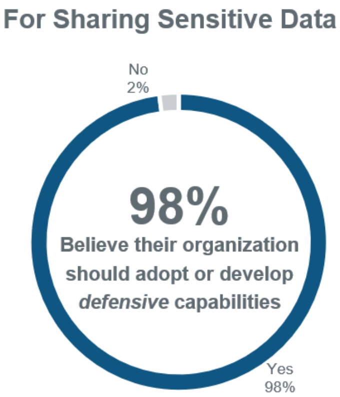
Defensive plays for sharing sensitive data

The roundtable explored the role of defensive strategies in sharing sensitive data, and opportunities to create alignment to move forward. Attendees said defensive strategies to govern data and limit risk include:

- Defending against breaches & fraud, promoting safe access, use & sharing
- Creating better data environments (predictable, manageable, disassociated)
- Governance and data management, ethics, and trust

The poll results below show audience perspectives on opportunity and possible organizational pain points. They suggest many factors are preventing the adoption or development of defensive capabilities for sharing sensitive data, including accountability and responsibility, privacy and security concerns, poor data literacy, and even that a strategy is missing. However, the vast majority believe their organization should adopt or develop defensive capabilities to share sensitive data.


Preventing Adoption or Development of *Defensive* Capabilities


For Sharing Sensitive Data

The following ideas emerged from the roundtable discussions.

How to facilitate defensive strategies:

- Defensive strategies are built around three pillars: people, processes, and technology.
- It is important to bring stakeholders (e.g., legal, privacy and security) into the conversation early to avoid siloes. Go to people before you need them.
- Focusing on the business need rather than on privacy and security can speed up negotiations significantly.
- Having standard data sharing processes, agreements and frameworks with appropriate training can also facilitate the process.

Potential barriers to defensive strategies:

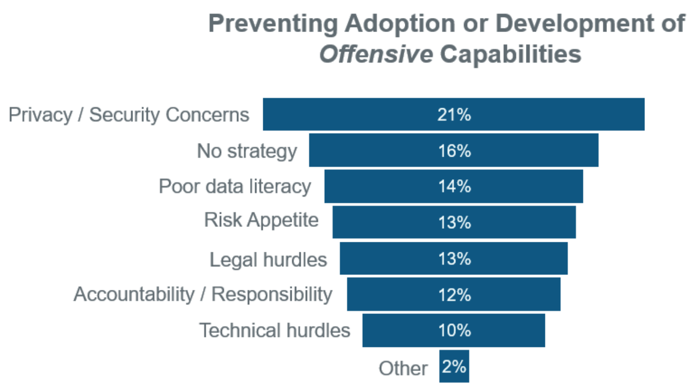
- Laws and regulations often already require significant defensive investments. Some stakeholders may question the need for further defensive measures.
- People fear that data will be misinterpreted. To avoid this, data needs to be curated properly and explained.

Offensive plays for sharing sensitive data

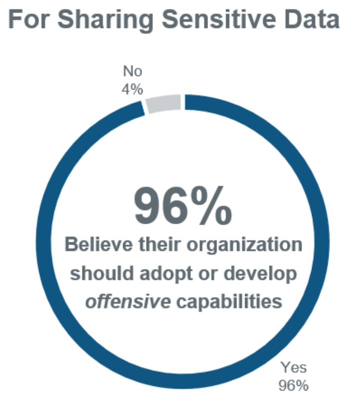
The roundtable explored the role of offensive strategies in sharing sensitive data, and opportunities to create alignment and move forward. Offensive strategies to drive business opportunities and realize new value when sharing sensitive data include:

- Enabling data access across departmental siloes to solve organizational problems
- Creating value through data sharing and the use of data products
- Developing key applications or infrastructure capabilities for the above

The poll results below show audience perspectives on opportunity and possible organizational pain points. They suggest that privacy and security concerns are dominant factors preventing the adoption or development of offensive capabilities for sharing sensitive data, with no strategy and poor data literacy as contributors. However, the vast majority believe their organization should adopt or develop offensive capabilities to share sensitive data.



Preventing Adoption or Development of *Offensive* Capabilities



For Sharing Sensitive Data

The following ideas emerged from the roundtable discussions.

How to facilitate offensive strategies:

- It is better to focus on the compelling business reasons that drive data sharing rather than the data sharing itself.
- Small, regular wins can help to convince stakeholders of the value of data initiatives.
- Part of the data leader’s role is story telling: talking about both internal and external data initiatives with real stories can motivate stakeholders.
- Stakeholders will more likely be onboard with data initiatives if they can participate in them and see first-hand what they involve.

Potential barriers to offensive strategies:

- Data sharing should be ethical: would there be general support for the sharing and is it respectful of people in the data? Ethics should be considered upfront.
- Participants felt that current privacy regulations can stifle innovation and limit the benefits of data use. More focus on the benefits from data sharing is needed for a balanced approach to privacy.

Why a playbook now?

During our event on May 19, 2021, we heard that data leaders are looking to increase data sharing so they can improve decision making and drive innovation. Demand is up for using data to drive value, as data leaders struggle to find the right balance between defensive and offensive plays. Are they two sides of the same coin, or do they play a more active, strategic role? For example, do defensive plays allow the data leader to better position themselves to launch offensive plays with more agility and better timing to achieve impact?

Interplay between offensive and defensive plays

- Whether to go defensive or offensive will often depend on the context and use case.
- Deciding between offense and defense involves balancing benefit and risk.
- To balance offense and defense, one should have a clear business strategy, tech strategy and data strategy. They all go hand in hand.

The discussion was rich with insights and this summary only captures some of the main points by theme.

Acknowledgments

We wish to thank the executive data leaders that participated in the roundtable discussion by sharing strategic insights based on their combined knowledge and experience.

- Joy Bonaguro, CDO, State of California
- Kamayini Kaul, VP, Global Head of Information Insights and Analytics, at CSL Berhring
- Douglas Lee, VP, Enterprise Data, Analytics & Data Science, Healthcare at Harris Computer
- Raj Nimmagadda, Global Head R&D Office, Digital Data Sciences, R&D, Sanofi
- Ima Okonny, CDO, Employment and Social Development, Government of Canada

Finally, we wish to thank the host, Richard Y. Wang, Founder & Director of the MIT CDOIQ program.

About Privacy Analytics

Privacy Analytics provides data anonymization services and software with auditable proof of privacy protection. Our expertise has enabled business leaders at more than 200 organizations across consumer and healthcare industries to safely deploy transformative data strategies. With 100+ in-house experts and scalable commercial software, we've anonymized thousands of datasets over our 14 years in business, giving clients an edge in the hyper-competitive race for innovation and new revenue streams. Our proven approach to data anonymization makes sure our clients are CCPA, HIPAA, and GDPR-ready, turning their most sensitive data into their most powerful asset. www.privacy-analytics.com

About MIT CDOIQ

The MIT Chief Data Officer and Information Quality Symposium (MIT CDOIQ), now in its 15th year, is one of the key events for sharing and exchanging of cutting-edge ideas, content and discussions. Our purpose is to advance the knowledge and accelerate the adoption of the role of Chief Data Officer (CDO) in all industries and geographical countries. As Data is a critical aspect of every organization, the symposium is focusing on the management and leadership of this critical element for the 21st century that will benefit every organization.

Against the backdrop of Data Analytics, Machine Learning, Data Quality and Data Management, the MIT CDOIQ Symposium will host its event virtually and will explore delivering mature data & analytics capabilities for ROI, including local organizational issues to global challenges, through case studies from industry, academic, financial, government and healthcare leaders. https://cdoiq.mit.edu