Deloitte.



Chief data officers 2.0

How CDOs are leading organizations to drive value from data, while maintaining customer's trust



Chief Data Officers 2.0

How CDOs are leading organizations to drive value from data, while maintaining customer's trust

The role of the chief data officer (CDO), a very recent addition to the C-suite, is evolving rapidly as data becomes increasingly pivotal to an organization's business strategy and success. CDOs are now responsible for much more than regulatory compliance-driven data governance and stewardship. They're being asked to champion data, and protect and grow its value as a strategic asset. They're being asked to drive change, enable and support analytics and innovation, and lay the foundation for exploiting the possibility of artificial intelligence. They're under pressure to drive value from analytics, achieve operational efficiencies, and keep costs under control.

CDOs find themselves at the forefront of some of the greatest developments transforming business, a position that brings significant challenges and opportunities alike. This paper explores the evolution of the CDO role and the issues facing its incumbents today and tomorrow.

The evolution of the CDO

A few years ago, financial institutions and other organizations realized their customer and business data needed to be treated as a strategic asset, one that played a crucial part in such functions as risk and regulatory compliance, sales and marketing, and operations. Enter the CDO, an executive leader mandated to effectively manage corporate data as an asset.

At first, CDOs were responsible for improving data availability, quality, and compliance. Though these remain table stakes for CDOs, organizations want their CDOs to be business strategists as well, collaborating with the business to capitalize on data more effectively to derive practical insights and transform operations. The increasing pace of digital, customer personalization and real-time engagement, and a swiftly evolving data privacy landscape are top-of-mind challenges. Moreover, as data sources, volumes, and vendors proliferate, CDOs face even greater challenges in managing the tracking, use, storage, and retention of customer information.

Chief data officers are now seen as key players in transforming their businesses into insightdriven organizations.

As expectations rise and challenges increase, it's becoming imperative organizations adopt the CDO role and integrate it with business, technology, risk, and corporate functions.

No one model for where the CDO and his or her supporting team should reside has emerged as the leader. Depending on an organization's requirements, the CDO could report to business, corporate, or technology groups, playing a role that emphasizes operations, policy setting and compliance, or analytics-powered innovation:

- **Reporting to business:** There's a strong need to drive business value by solving business challenges and improving customer experience through 360-degree customer information and the like. Data management capabilities and related services can be set up in and delivered through lines of business, such as digital or marketing, with the CDO reporting to the business leader.
- Reporting to corporate: The CDO reports into a corporate function such as Risk or Finance, where the driving priorities include risk mitigation or cost reduction. Data management and related services may be established and delivered through corporate functions. For example, a CDO reports to the chief actuarial officer for an insurance company that wants to streamline its underwriting process and develop complete linkages across its processes, for which the firm required quality data.
- Reporting to technology: The CDO team resides in the technology group, where there's an emphasis on establishing uniform shared data and analytics services. The technology group is responsible for data management capabilities and associated services, and the CDO reports to the technology leader.

Structural and reporting models

CDO emphasis: Policy and compliance	CDO emphasis: Operations	CDO emphasis: Analytics and innovation
 Owns enterprise policies and standards, data strategy, and roadmap Establishes/manages data governance operations, data profiling and quality management, issue and change management, data steward training Manages data management tools and technology Provides oversight/reporting on business line data policy compliance 	 In addition to policy/compliance activities: Provides shared service to lines of business such as data domain master and reference data management Owns enterprise data assets, such as data warehouse, big-data platform Maintains business metadata and data models for shared assets Drives strategic data rationalization initiative Curates and sources 	 In addition to operations activities: Drives enterprise analytics strategy and technology ecosystem Executes priority analytics on behalf of business Enables business-driven analytics Owns enterprise centre of excellence to drive data and analytics adoption/training Incubates and pilots new tools and vendors
	 Curates and sources 	

external-provider data

CDOs: Proactively embracing constant change

No matter the nature of their role and reporting relationships, all CDOs face an array of business, technology, and regulatory issues as they seek to execute on their priorities. Embracing change is proving to be a key part of any CDO's skillset.

Business and technology trends

C360: The need for a 360-degree view of the customer

Financial institutions and other organizations continuously engage with their customers through a variety of channels, whether online, mobile, telephone, or in-person. This generates an incredible wealth of customer data; unfortunately, much of this is stored in silos. This makes it difficult for organizations to access and exploit relevant insights and moments of impact along customer journeys. Customer 360 views can be useful for:

- Lead identification and lead sharing across lines of business
- Faster, more efficient customer and product onboarding
- Developing highly personalized products and services by understanding customer interactions and transaction patterns
- · Improved understanding of customer cost-to-serve and profitability
- Modernization of new business underwriting in insurance through the use of third-party data sources, advanced analytics, and automation
- Improved fraud monitoring through holistic view of transactions and network analytics

To realize the potential benefits of C360 insights, CDOs must ensure those insights can be operationalized. To do that, organizations must combine the setup of the CDO role and the supporting office with the production of analytics in order to control the data used by robotic process automation (RPA), natural language processing (NLP), artificial intelligence (AI), and other analytics initiatives, not to mention for regulatory reporting.

In addition, CDOs need to align with solution architects and core platform owners to integrate analytics insights and models into workflows that are largely operationalized through employee interactions with core platforms. This way, organizations can establish the vital processes required to run a CDO office while also feeding the business tangible analytics products and relevant insights.

Cognitive technologies

From the use of social media to device sensors, data is constantly being generated. The amount is only going to grow as more businesses become digital and more devices connect to the internet. Research and advisory firm Gartner forecasts that by 2020 there will be 20.8 *billion* connected devices in use, part of the Internet of Things (IoT) supplying a steady, constant stream of data.¹ As the amount of data rises, so too will the amount of useful information that can be gleaned from it.

Much of this data is—and will be—unstructured. Sources of unstructured data include emails, instant messages, documents, device logs, and notifications, including those from IoT devices. New data sources include digital still images, audio, and video files. Finally, there are deep-web sources that are curated by academics, business consortia, government agencies, communities, and third-party domains.

1. www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology/ gx-tech-trends-the-kinetic-enterprise.pdf

To realize the potential benefits of 360-degree customer insights, CDOs must ensure those insights can be operationalized.

Cognitive technologies are poised to disrupt financial services and other industries as companies seek to use data to understand their business and customers, automate tasks, and gain efficiencies.

The expanding digital universe 2013–2020

In 2020, the digital universe is expected to reach 44 zettabytes. One zettabyte is equal to one billion terrabytes. Data valuable for enterprises, especially unstructured data from the Internet of Thing and non-traditional sources, is expected to increase in absolute and relative sizes.



Source: Deloitte Tech Trends 2017

Deriving meaning and insight from this immense torrent of data, both structured and unstructured, will require advanced analytics and, increasingly, artificial intelligence and machine-learning systems. These cognitive technologies are poised to disrupt financial institutions as organizations seek to use data to understand their business and their customers, automate tasks, and gain efficiencies.



CDOs will need to drive both awareness and adoption of AI, machine learning, and other emerging cognitive technologies. They'll also need to ensure there is clarity and transparency about the organization's use of customer data, as well as appropriate oversight and controls regarding automated decision engines in order to mitigate bias and risks associated with the data.



Cognitive case studies: SEB, Nordea Bank

2. www.americanbanker.com/opinion/capital-one-shortens-the-machine-learning-curve

3. www.eweek.com/cloud/capital-one-taps-open-source-cloud-big-data-for-advantage-in-banking?page=3

4. www.finextra.com/newsarticle/30759/nova-joins-the-robot-revolution-at-norde

Capital One first used machine learning to analyze clickstream data that reveals which pages people visit on its website and what actions they take while they're there. Now the bank has a solution that uses machine learning to customize website content in real time for each user, based on the person's behaviour during the session. Clients, or potential clients, looking at a reward card, for example, would be served different content than those looking at a savings account.²

Capital One also uses predictive analysis and machine learning as a way to discriminate normal from abnormal behaviour. This helps identify malware or anomalous behaviour or other kinds of similar indicators of threats in this environment. These efforts also help to drive customer growth, increase associate productivity, reduce analogue costs, enhance risk management, and improve the digital customer experience. For example, the institution recently launched a product called Second Look that notifies it if a customer leaves an unusually large tip at a restaurant. The bank can then send its customer a notification in real time saying essentially, "We noticed you left a large tip; did you intend to do that?" ³

Sweden's biggest banks are pioneering new AI technology. One of them, SEB AB, is introducing a virtual customer service representative. Called Aida, it will allow the human employees to concentrate on tasks that are more complex while it takes care of simple, frequent tasks. A similar initiative is being undertaken by Nordea Bank AB at its life and pensions unit in Norway. It's launching Nova, a chatbot that can respond to customers' questions regarding pension and insurance. The ultimate goal is to train the chatbot to guide customers to log into a secure environment, enabling them to perform tasks and obtain advice there.⁴





Cognitive case studies: Leading financial

institution

Life event/stage-driven marketing: Al-based solutions could be used to predict life events with greater accuracy, and analyze large data sets combining multi-channel interactions and structured and unstructured information for targeted offers.

At the same time, CDOs will need to ensure the data used by their organization's cognitive systems is trustworthy, credible, and high quality. Data quality plays a pivotal role in determining whether an organization's AI and machine learning systems deliver useful outcomes and competitive advantage. Given the vast amounts of unstructured data that cognitive systems must sift through, some degree of data-cleansing and pre-processing is essential if a company's analytical algorithms are to produce accurate and useful insights.

Regulatory trends

Fundamental Review of the Trading Book

The Fundamental Review of the Trading Book (FRTB) is a set of market risk capital rules that are designed to redraw the boundary between banking and trading books, and raise the bar for internal models.⁵ The FRTB requires all banks to implement the revised market risk standards by January 2019.

The new rules pose significant challenges for banks, which in response will have to reconsider their business model and their approaches to measuring market risk as well as refine their balance sheet management strategy. FRTB also requires banks to have goodquality static data associated with each risk factor. CDOs will need to ensure adequate historical data sources are available, and that their organization maps and buckets data for specific requirements.6

CDOs will need to drive both awareness and adoption of AI, machine learning, and other emerging cognitive technologies. They'll also need to ensure there is clarity and transparency about the organization's use of customer data, as well as appropriate oversight and controls regarding automated decision engines in order to mitigate bias and risks associated with the data.

A leading FI wanted to shift to a more customer-centric approach to doing business. It therefore brought together its business units around a common goal: to understand how AI and machine learning could facilitate this shift. They identified a number of use cases that would help the organization achieve its goal:

Spend insights: Al could be used to make personalized recommendations to customers based on their individual lifestyle, spending patterns, budgets, savings goals, and investment styles.

Wealth management: AI could be used to provide personalized customerservice solutions that mimic human interaction, make automated saving and investment decisions for users based on transaction profiles and preferences, and identify opportunities for cost savings, tax efficiencies, and alternative investment strategies.

> CDOs need to ensure cognitive systems use trustworthy, credible, and high-quality data.

www.risk.net/to1pics/fundamental-review-of-the-trading-book-frtb

^{6.} www2.deloitte.com/content/dam/Deloitte/ie/Documents/Risk/FRTB%20Article.pdf

EU General Data Protection Regulation (GDPR)

On May 25, 2018, the European Union's General Data Protection Regulation (GDPR) comes into force. Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), a data privacy law that governs how private sector organizations collect, use, and disclose personal information, is comparable.

The GDPR is designed to strengthen and unify data protection for all individuals within the EU. The new regulation introduces or expands a number of rights and requirements: ⁷

- It expands the definition of personal data and introduces the new concept of pseudoanonymous data. These updated definitions will put even more emphasis on data classification and governance.
- Organizations will need to create and maintain an inventory of data processing activities in order to demonstrate an understanding of what data they hold, where it's stored, and with whom it's shared.
- The ability of consumers to request the deletion of their data is being strengthened. The enhanced right to be forgotten may require organizations to conduct wholesale reviews of their processes, system architecture, and third-party data access controls. Even archived media may need to be reviewed so that data can be deleted.
- · The new right to data portability—the right to request standardized copies of data could create a number of challenges, such as reaching clarity on which data needs to be provided, how to provide it in an industry-standard form, and how to extract the data efficiently.

Organizations outside the EU that collect or process the personal data of EU residents are subject to the new rules; CDOs will need to ensure their organization is in compliance with the regulations.

Basel III

Basel III is a series of measures developed by the Basel Committee on Banking Supervision (BCBS) as a response to the financial crisis of a decade ago, to which nations around the world have agreed to be subject. These measures are intended and designed to strengthen the regulation, supervision and risk management of banks worldwide.8

The BCBS 239 measure requires effective data aggregation, risk reporting, and maintaining and demonstrating high data quality at all times, which in turn requires financial service institutions (FSIs) to define strong requirements in terms of data management.⁹ Solvency II stipulates that data used in FSIs should be free from any material errors and that the data processing should be done in a transparent and structured manner while ensuring high data quality and accuracy. Solvency II also requires insurance and reinsurance undertakings when using external data to demonstrate the importance of use of external data and ensure the origin of external data is known.¹⁰

Basel III has direct repercussions on how financial institutions manage data. CDOs must ensure their organization can demonstrate data quality and traceability for ad hoc reporting requests. They need to ensure the necessary processes are in place to ensure data integrity, especially since data is often sourced from a variety of functional areas and product lines.¹¹ They must also make sure appropriate data-guality monitoring activities are established, which should include defining a single source of truth and maintaining a cross-functional data dictionary.12

IFRS 17

IFRS 17 aims to bring more transparency to the insurance industry's financial reporting and requires more granular data, with a particular focus on cash flows and cash-flow adjustments. The need for more data granularity, especially with respect to the inception or fulfilment of an insurance contract, will lead to increased data volumes, while source data from feeder systems will need to be extracted and optimized. Current application architectures will be challenged to store and process larger data volumes in a timely fashion.¹³

The CDO'S role in ensuring regulatory compliance

GDPR	Build a data inventory and track data	'Right to be forgotten': consumers can request deletion of their data	Right to data portability: individuals can request data in standardized format	New definitions of data – GDPR places greater emphasis on data classification and governance
BASEL III	Demonstrate data quality and traceability	Build processes to ensure data integrity	Define single source of truth	Maintain cross- functional data dictionary and data accuracy
FRTB compliance	Ensure good- quality static data	Ensure adequate historic data is available	Map and bucket data for specific requirements	

First step in governing: Create a data catalogue

Whether to secure competitive advantage or meet regulatory requirements, organizations are being challenged to manage ever-increasing data volumes in a changing business landscape. To ensure data is coordinated and available across the enterprise, CDOs must rethink how to efficiently manage and govern a vast wealth of structured and unstructured data.

^{7.} https://www2.deloitte.com/nl/nl/pages/risk/solutions/general-data-protection-regulation-gdpr-vision -approach.html

^{8.} https://www.bis.org/bcbs/basel3.htm

^{9.} https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-basel-iii.pdf

^{10.} Official Journal of the European Union, Non-legislative acts

^{11.} www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu_it-implications-basel-iiicrd-iv 06102014.pdf

^{12.} www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/lu-basel-iii.pdf

^{13.} www2.deloitte.com/content/dam/Deloitte/ch/Documents/financial-services/ch-fs-white-paper-ifrs-17.pdf

Data consumption and governance

A one-stop shop approach to data access can provide critical controls that are missing in many organizations.

Many organizations lack repeatable processes for accessing and using the data they've collected. As a result, teams can easily spend considerable effort working through the same problems and issues. More often than not, the teams are using manual processes to extract and compare data from sources scattered across the organization. With few controls in place, these manual efforts suffer from questionable data integrity, limited transparency, and limited traceability, all of which make it difficult for decision makers to trust in either the data or the derived insights.

Establishing a one-stop shop approach to data access can provide the critical controls that are missing in many organizations. It can help assure users of data quality and integrity, speed up the insight process, and provide decision makers with the confidence to trust in the data and insights presented to them.

There are several key elements to any one-stop shop model. First, it needs consistent frameworks and data governance. Organizations must develop business rules and glossaries for data storage, management, and use. They must also clearly set out a single data governance process that centralizes authority and is organized along domains that cut across enterprise functions and lines of business.

As well, organizations need to establish a single home for their data—a centralized, authoritative copy or catalogue of all data assets. This central data catalogue ensures that all data conforms to business rules and governance controls, providing users with one source for quality, trustworthy data. Data and data sets should be curated and profiled for quality before being included. Machine-learning technologies can help to create the catalogue by developing a common language that seamlessly links to the existing data lexicons used by business lines or functions; the CDO needs to be a facilitator in the data-definition work with the business.

In addition to leading the establishment of their organization's one-stop shop for data, CDOs will also need to drive a cultural shift to ensure that all data-related processes, projects, and initiatives abide by the new centralized approach.

Self-service capabilities

Once it's in place, the centralized data catalogue will empower the organization's people to access and use quality data themselves, eliminating the need to collect data from across disparate sources haphazardly. Business functions and lines can use the catalogue to curate customized, traceable data sets based on their interpretation of the data, and view data sets curated by other groups.

Centralized virtual data-services help desk

A one-stop shop for data will inevitably create a need for a single, centralized point of contact for responding to user queries and issues regarding data sets, data curation, or even data elements. Workflows can be created to direct requests to specific data stewards as needed.

Developing talent: Building analytics teams

Any organization that aspires to become an insight-driven organization must eventually deal with the question of talent. The CDO plays an important role in ensuring his or her organization brings in the right mix of cross-functional talent needed to not only conduct analytics, but to ensure data-driven insights address meaningful business issues and translate into real action.

Most organizations understand they need data engineers and modellers, technology architects, software developers, and other such "red skill" individuals on their insight teams. These are the people who bring sophisticated statistical, data management, and technology skills to the table.¹⁴

But red skills alone aren't enough. To encourage business adoption of data-led decision-making and accelerate a company's transformation into an insight-driven organization, insight teams also need people with blue skills. These are the change managers, business analysts, political navigators, and senior executives with the business acumen and the communications, storytelling, and persuasion skills needed to identify what business questions need to be asked—and how to get people to act on the data-driven answers.

The most effective insight teams, then, comprise a mix of red- and blue-skilled people (and occasionally, a purple individual who possess both red and blue skills). Combined, these individuals form a purple team—a powerful force for change that can break down organizational barriers to deliver faster, better business outcomes.

Ideally, a CDO will be supported by a mix of cross-functional purple teams, all empowered to make decisions, execute strategies, and drive toward specific outcomes. Where talent is scarce, a group of data resources could act as a specialized team collaborating with business and technology teams across the organization as required. The exact nature of the cross-functional team model will reflect the role of the CDO office and its attendant reporting relationships, and it will need to be developed with input from business and technology teams across the organization.

As the CDO role and the supporting team evolve and grow in stature and influence, CDOs will need to guard against inadvertently building their own hierarchy and organizational silos. They should strive to be collaborators and business enablers, operating with enough autonomy and authority to directly influence data strategy, provide guidance on data policy, and ensure work supports the overall business vision. CDOs play a key role in ensuring the organization recruits the right mix of crossfunctional talent to form purple teams.



Red skills:

Sophisticated statistical, data management and technology skills, e.g. data engineers and modelers, technology architects, software developers, testers

Blue skills:

Business acumen, communications, storytelling, and persuasion skills, e.g. change managers, business analyst, political navigators, senior executives

Purple skills:

Combination of both red and blue skills

http://images.info.deloitte.ca/Web/DeloitteManagementServicesLP/%7Bea8a1ed5-e366-4c4f-a24d-9b4f2f1d-610f%7D_ca-en-insight-driven-organization.pdf



Data privacy, security need to be top-of-mind for CDOs

As organizations grow more connected, the data becomes more vulnerable and the risk of a data breach grows.

The volume of data being produced and stored is growing at an exponential rate, and more devices are connecting to the internet each day. As organizations grow more connected to their customers, vendors, and other third parties over networks and IoT devices, their business and customer data is becoming increasingly vulnerable—and the risk of a data breach is steadily rising. CDOs will need to ensure their organization takes appropriate steps to mitigate this risk and respond to breaches swiftly when they occur. New technologies can play a pivotal role.

Large-scale data breaches at companies such as Equifax, JP Morgan Chase, and Verizon-to name only a few—have demonstrated the pressing need for tighter data controls at financial institutions and other companies alike. The rising trend for organizations to store their data in the cloud is only intensifying the need for rigorous data-security measures. CDOs will need to work closely with their organization's risk officers to ensure adequate data encryption and monitoring mechanisms are in place, and be actively involved in developing controls related to cloud purchase, use, and vendor evaluation.

As well, they will need to take the lead in ensuring their organization takes appropriate care that collected customer data isn't used for unintended purposes. CDOs must be aware of how customer data is or could be used, and play an active role in managing any privacy issues that may arise. CDOs should also make sure customers are told in clear, simple terms how their data will be used and how it will benefit them.

Companies have been concerned with cybersecurity for 20 years, if not more. Today, new technologies—machine learning, artificial intelligence, and blockchain among them have emerged as powerful tools in the ongoing battle to prevent, detect, and respond to data breaches.

Al systems can examine and scan many activities to identify patterns, coincidences, and anomalies to detect both internal and external threats. Machine learning can be used to analyze and monitor data and network transactions, and to process large volumes of historical data to predict and prevent threats. It could also have use in anticipating potential threat or fraud scenarios to bolster data security efforts. ^{15, 16}

Internal data security also a concern

As organizations move towards centralizing and sharing data across functions to provide an integrated view of their customers, protecting data and customer privacy inside the organization is becoming equally important. Those within the organization must understand what information can be shared based on customer consent; CDOs must work with privacy officers to establish appropriate privacy standards depending on how and where customer data is being used. CDOs must also team with privacy and risk officers to ensure operational controls are in place to maintain data integrity and safety while supporting an open data and insight environment within the organization.

CDOs and their risk and privacy counterparts should apply the privacy by design framework, which calls for privacy to be built directly into the design, operation, and management of a business process or system.¹⁷ There should be guidelines about the appropriate and ethical use of customer data, the starting point for which should be how such use will benefit the customer-not how it will benefit the organization.

If CDOs discover their company has talent gaps in the area of data security and privacy, they should move swiftly to close those gaps. Ideally, they would want a combination of staff knowledgeable in the use of AI and machine learning to support data privacy and security as well as a team of data security and cybersecurity experts who could collaborate with business and technology functions to mitigate the organization's data-related risks. ^{18, 19}

CDOs need to help ensure their company mitigates its data risks, including those involving the appropriate use of customer data.

CDOs and their risk and privacy counterparts should embrace privacy by design, building privacy directly into the design, operation, and manage*ment of a business* process or system.

^{15.} www2.deloitte.com/insights/us/en/focus/tech-trends/2017/moving-beyond-artificial-intelligence.html 16. www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF 17. www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF 18. www2.deloitte.com/insights/us/en/focus/tech-trends/2017/moving-beyond-artificial-intelligence.html 19. www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF

Open banking and data monetization: The new frontiers

APIs at a glance

There are three types of application programming interfaces (API) model: public, private, and partner. Currently, private APIs are the most commonly used, although partner APIs are gaining momentum due to regulations coming from the United Kingdom's Competition and Markets Authority and others.

Public APIs are used by external partners and developers who build innovative apps and products. These APIs help extend market reach while encouraging innovation by engaging the developer community.

Private APIs open parts of application details to be used by developers in the enterprise. Use of private APIs in a traditional banking organization can help enhance operational efficiency and reduce costs, and help share customer data that's typically siloed in the organization.

Partner APIs are usually between a bank and a strategic business partner, and are not available to the public. These APIs help maintain close-knit partner integration, and can enable banks to create new channels, refine partner strategies, monetize APIs, and help a business partner to complete its offering. From instilling a data culture, recruiting the right talent, navigating business and regulatory issues, and tackling data privacy and security, there is no shortage of important challenges facing today's CDOs. Yet in an ever-changing landscape, these officers and their organizations must prepare for emerging challenges and opportunities, particularly the rise of open banking and the potential for data monetization.

Open banking is coming

Open banking refers to a new platform whereby banks use APIs to share their data with third parties in order to enable the development of innovative products and services and enhance the customer experience. It's a development that reflects many customers' day-to-day habits: according to the World Retail Banking Report 2017, more than one in four (26.5 percent) consumers do their banking with both traditional banks and non-traditional fintech firms. A further 2.9 percent of consumers do all their banking with fintechs.²⁰

Regulators are pushing for open banking as well. The EU issued its revised Payments Services Directive 2 (PSD2), which requires banks to open up their data to third parties. The United Kingdom's Competition and Markets Authority has mandated the United Kingdom's largest banks to adopt open-banking standards. In Singapore, home to a large fintech sector, the Monetary Authority of Singapore is encouraging financial institutions to share APIs.²¹ Australia and Iran are also taking steps to adopt and promote the platform.

As open banking takes hold, it's inevitable that banks will need to give up some degree of control over their customer data. Offsetting this is the fact banks will gain new opportunities to retain and grow their customer base by offering innovative, personalized third-party products and services. Indeed, it's likely that open banking will enable financial institutions and fintechs alike to capitalize on their respective strengths to deliver a better customer experience and grow their businesses.

Of course, open banking also raises significant data privacy and security concerns about data sharing. (A leading telecom company faces a \$750-million lawsuit over the alleged sale of consumer data.) CDOs will need to take the lead in driving the effective integration of data into any open-banking strategy. This will include establishing a privacy and security structure for all enterprise data and ensuring that different data categories are appropriately identified and secured, so that data is shared with third parties according to proper protocols and security standards.



20. msenterprise.global.ssl.fastly.net/wordpress/2017/07/World-Retail-Banking-Report-2017.pdf 21. www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2017/Singapore-FinTech-Journey-2.aspx



From data management and insights to data monetization

As financial institutions and other organizations strive to unify data assets spread across the enterprise and deploy AI and machine learning to derive insights from vast volumes of internal and external customer data, they're taking the first steps toward a new opportunity: data monetization.

Companies can monetize data for a variety of reasons: to create a new revenue stream, introduce a new line of business; gain competitive differentiation or advantage; strengthen relationships with partners, suppliers, or customers; and drive corporate or shareholder value.

The insights derived using cognitive technologies—whether through proofs of concept, pilot programs, or full-production initiatives—can be used to elevate existing customer data collections into enormous and valuable customer-base data sets. These data sets can in turn be licensed for use by other organizations. Already, innovative algorithms some even available in the public domain—are enabling startups to build data sets that can be patented and turned to competitive advantage. Google and Facebook are perhaps the greatest examples of consumer companies whose proprietary user data sets have helped them achieve unparalleled market dominance.

In the enterprise world, where so many companies still struggle with disparate, fragmented data sources, organizations that possess large, high-quality, centralized data sets have an enormous potential competitive advantage, because they have an asset that is more readily monetized.

Organizations can monetize data indirectly or directly. With indirect monetization, data is used to reform internal processes or improve product offerings based on data insights— monetization takes the form of cost reductions or increased revenue in existing lines of business. Direct monetization, on the other hand, can involve the sale of data directly through licensing or subscription, or in exchange for other products or services. Analytics solutions themselves can also be sold to other parties.²²

Looking ahead, it seems likely that CDOs could be made responsible for commercializing their organization's unified data assets and for purchasing other companies' data assets. Gartner forecasts that by 2020, one in four major organizations will become data suppliers or consumers through formal online data trading.²³

Companies can *monetize data for many* reasons, including to secure new revenue streams and competitive advantage or to build stronger relationships with partners, suppliers, and customers.

^{22.} Gartner - Prepare to Monetize Data From the Internet of Things. ID: G00309409 23. Gartner - Predicts 2017: Licensing, Legal and Language Lessons for Data and Analytics Leaders ID = G00316495

Organizations that have large, centralized, high-quality data sets have an enormous potential competitive advantage, because they have an asset that's more readily monetized.

CDOs could enable opportunities to monetize their organization's data in several ways. They could sell or license data sets to third-party vendors, or use internally generated (or externally purchased) data sets to enhance existing products. For example, an insurance company could purchase data from external sources and combine it with available internal data to develop new risk models for providing better prices and products to customers.

Alternatively, they could purchase external data from third-party vendors to gain a sharper understanding of the marketplace or customer and prospect needs and behaviours. This external data could be used to determine product performance and be compared with competitors' products, track industry, or consumer trends to improve existing products or services or introduce new ones.

Data monetization many not be on the immediate horizon for most organizations, but it's an opportunity many CDOs will need to deal with soon. They can prepare for it today by considering how their own organization could monetize its own data assets and identifying the kind of data sets the organization might want to buy in the years to come.

CDOs face an exciting and challenging future

The role of the chief data officer has evolved rapidly since it first emerged several years ago. It will undoubtedly continue to change as data takes a more crucial role in every organization's business, and advances in cognitive and other technologies make exciting new opportunities possible. Adapting to the pace of change and responding positively to the issues and opportunities that result will undoubtedly challenge CDOs.

Yet CDOs can overcome these challenges by ensuring the role, reporting, and priorities of their supporting team are clear; by successfully establishing and promoting a centralized data culture throughout their organization; by developing purple teams with the right combination of red and blue skills to execute the data strategy; and by anticipating and capitalizing on new developments and opportunities as they arise.

If there's one thing that can be said about the role of the CDO, it's this: it will never be dull.





Contacts

Gordon Shields Deloitte Canada gshields@deloitte.ca

Jasjiv Jaaj Deloitte Canada jjaaj@deloitte.ca

Nira Sivakumar Deloitte Canada nsivakumar@deloitte.ca

Harman Singh Deloitte Canada harmasingh@deloitte.ca

Frederick Blackwell Deloitte Canada fblackwell@deloitte.ca

Jojy Mathew Deloitte Consulting LLP, United States jojymathew@deloitte.com

Larry Manno Deloitte Consulting LLP, United States Imanno@deloitte.com

Nicolas Griedlich Deloitte Luxembourg ngriedlich@deloitte.lu

Natalie F Williams Deloitte United Kingdom natalwilliams@deloitte.co.uk

Contributing team

Aprajitha Venkat Deloitte, Canada apvenkat@deloitte.ca

Zaib Mithani Deloitte Canada zmithani@deloitte.ca



www.deloitte.ca

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 220,000 professionals are committed to making an impact that matters.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018. For information, contact Deloitte Touche Tohmatsu Limited.