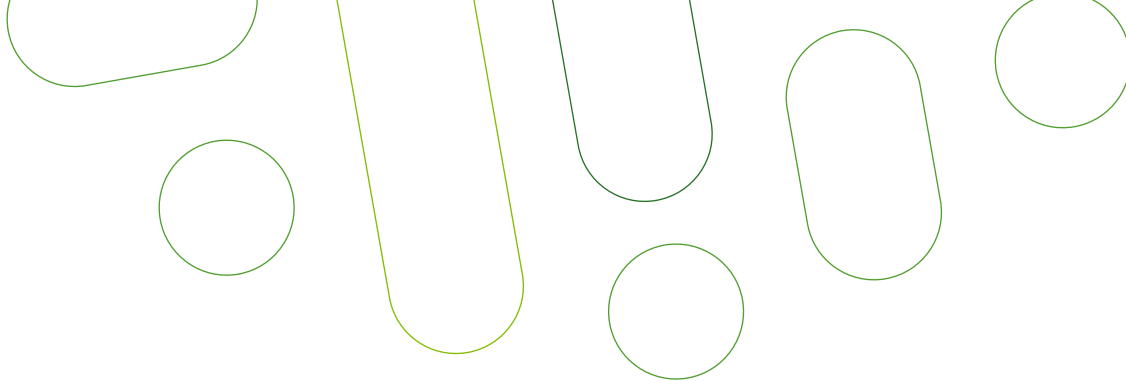


Driving Digital Transformation in 2019: Charting a Roadmap for Success

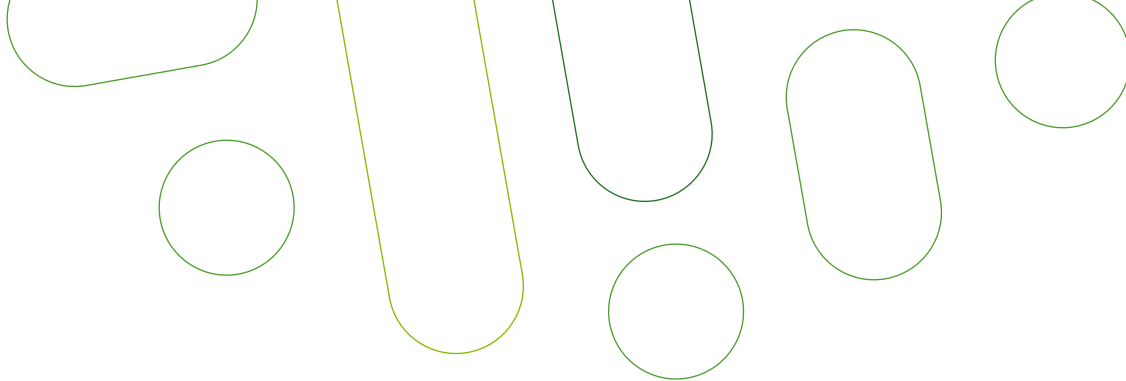


Digital transformation can mean different things to different people, depending on your industry and the nature of your business. Yet one common thread runs through all interpretations; the importance of data and data governance.

Digital strategies must ultimately focus on improving business processes and business outcomes, like offering new digital products or increasing your customer engagement. Yet the means to that end lies in how organizations improve management of their data.

Right now, we are experiencing a perfect storm of factors changing the competitive dynamics of many industries. A confluence of technologies – including cloud, artificial intelligence / machine learning (AI/ML) and the Internet-of-Things (IoT) – are helping companies to aggregate, process, analyze and act upon ever-growing volumes, variety and velocity of data. New business models are also emerging to disrupt incumbents across a variety of sectors, from retail and hospitality to financial services – which is forcing established players to re-think legacy operations and embark on their own digital transformation journeys.

In this paper, we examine five key components underpinning digital strategies and the data governance challenges organizations face along their journey.



1

The Cloud

The economics of cloud infrastructures and architectures have begun to reach a tipping point. Cloud service providers (particularly large IaaS vendors) have achieved the scale that enables them to offer an ever-more compelling value proposition. That value is not simply found in low-cost provisioning of computing or storage space; but is increasingly focused on the software-defined automations that enable easier access and control of those resources.

Digital businesses need to be agile. They need to innovate quickly, which means testing things out with their user base (eg. A/B testing) to determine what works and what doesn't. They also need to scale quickly and offer continuous uptime.

These requirements lend themselves well to cloud native architectures, tools and practices. Using a DevOps approach to quickly move from development to production. Breaking down complex systems into a myriad of microservices that are built-to-fail and have resilience built into their DNA. These are just a couple of example practices that have evolved in tandem with the proliferation of the cloud.

From a data management perspective, cloud architectures also offer a variety of features – from multi-tenancy to content delivery networks – that enable easier access, re-use and distribution of data.

While cloud architectures have enabled agile use of data and IT, they have also introduced their own governance challenges. For example, data sovereignty and audit requirements mean many organizations – particularly within regulated industries and those managing confidential datasets – will need certainty in where their data resides (which hasn't always been possible in the past).

Similarly, while cloud can enable easier access to data, this can also stoke concerns around information security. Organizations need to leverage all features on offer to ensure data remains encrypted at-rest and in-transit; and deploy relevant access controls to treat cloud as extensions of private infrastructure.

The use of SaaS within organizations also needs to be properly monitored and managed. While cloud has enabled much easier access to enterprise grade software and infrastructure, this has also given rise to the next generation of Shadow IT. Simply knowing which applications are being used across their organization and which datasets reside in those applications is a challenge for most organizations.

Finally, organizations will also need to consider issues around vendor lock-in and the portability of data that resides in clouds. Most vendors will happily facilitate the transfer of data into clouds. But before embarking on such migrations, organizations will need to evaluate how easily they can get that data back should they so require.

By the numbers

Cloud:

"Worldwide spend to reach \$160 bn in 2018 (Y -on- Y increase of 23%) and projected to grow at CAGR of 21.9%"
– IDC

"Infrastructure-as-a-Service is fastest growing segment and forecast to grow 36% in 2018"
– Gartner

"85% of enterprise keep sensitive data in the cloud"
– Vormetric

Artificial Intelligence / Machine Learning:

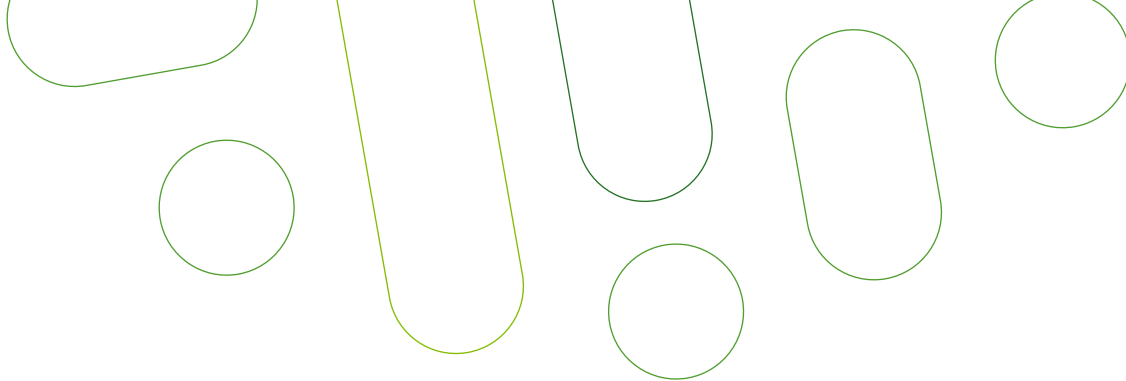
"Global business value of AI will reach \$1.3 trillion in 2018 (up 70% over prior year)"
– Gartner

"Worldwide spend on Cognitive / AI to reach \$77.6 billion by 2033 (37.3% CAGR)"
– IDC

Internet of Things

"8.4 billion connected 'things' in 2017 to reach 20.4 billion by 2020. Total spend to reach \$2 trillion in 2017 "
– Gartner

"B2B spend on IoT to reach \$296.8 billion by 2020"
– Boston Consulting Group

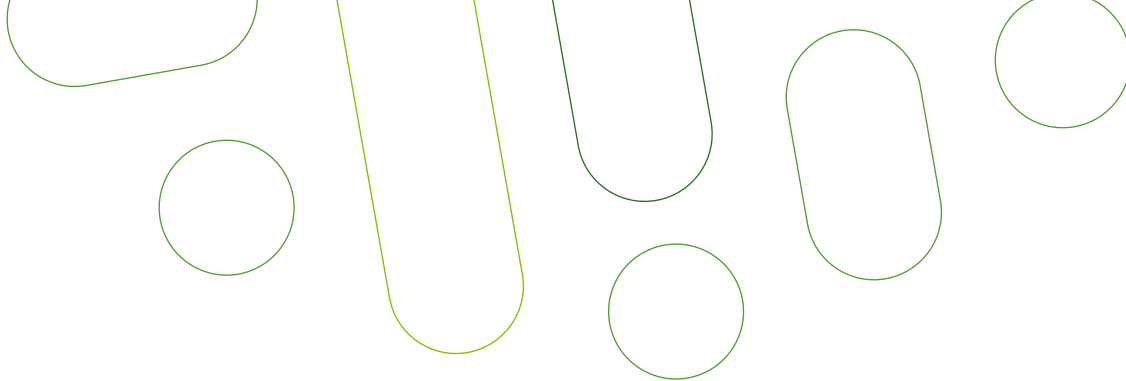


2

Artificial Intelligence and Machine Learning

Just as cloud has enabled more agile and scalable IT infrastructures – capable of aggregating, processing and distributing more data – AI and ML have provided tools for more scalable and meaningful analysis of that data. By facilitating processes such as natural language processing, image and speech recognition – AI and ML have begun to automate tasks that previously could only have been performed by humans. Customer-facing applications are the ones that achieve most instant-recognition – from digital assistants (like Alexa, Google, Siri and Cortana) through to chat bots and autonomous vehicles. However, there are a myriad of use cases where AI / ML is used in the background to automate complex and/or large-scale data processing – everything from automating insurance claims and optimizing financial models, to performing medical diagnoses.

AI and ML can have a huge impact on an organization. By training algorithms to recognize patterns and trends, organizations have the potential to automate some of their data analysis, which becomes more important considering the ever-growing volume, variety and velocity of data. However, new technologies also bring new challenges. AI and ML place a great onus on ensuring data inputs are accurate and reliable. It is impossible for algorithms to make meaningful interpretations if the underlying data is of poor quality. Similarly, AI/ML models need to be carefully trained. Without proper guidance, they can tend to over-fit models or uncover spurious correlations. This, in turn, raises the issue of transparency. It is vital that organizations using AI and ML techniques ensure tight oversight and an understanding of the logic underpinning that analysis. While neural networks were traditionally black boxes, the transparency of AI/ML decision-making is beginning to improve, which will be vital to support increased adoption.



3

Internet of Things (IoT)

While cloud and AI/ML allow for more scalable IT to better aggregate, store, process and analyze data, IoT is really about the proliferation of data sources. With many more devices, or ‘things’, becoming internet-enabled we will inevitably have much more data to collect.

These ‘things’ can be owned by individuals in the form of wearable devices, medical implants, cars, doorbells, thermostats, kitchen appliances, etc. They can be owned by companies, covering everything from electricity meters, weather sensors, close circuit television and fleet tracking devices, to agricultural sensors, commercial drones and industrial machinery. Or they can be owned by governments looking to promote smart cities, enhance security surveillance, or better monitor and manage traffic and infrastructure.

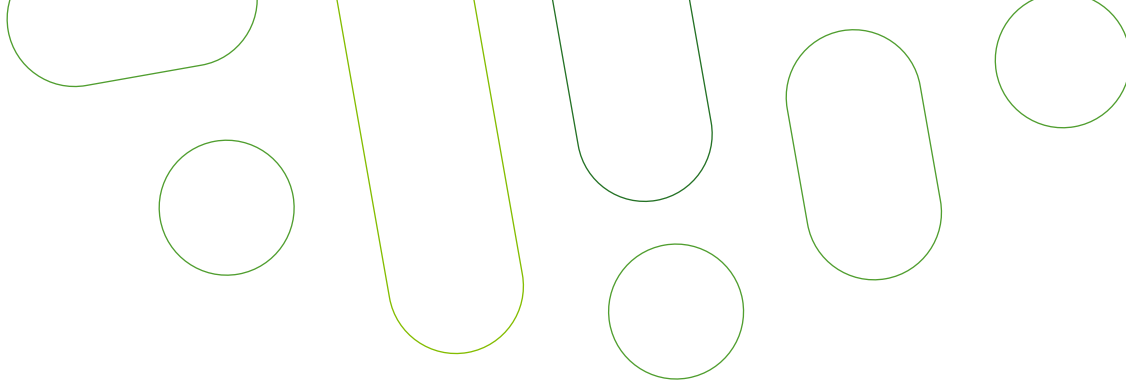
In all cases, the proliferation of data-gathering devices will provide an explosion of data to analyze, interpret and ultimately guide business decisions.

Just as IoT covers a wide variety of use cases, it also poses a broad range of data management challenges. Some of these are architectural or related to information security. Poorly secured IoT end-points have been blamed for several recent distributed-denial-of-service (DDoS) attacks. One of the first considerations should therefore be around how to ensure ‘things’ are protected from hackers. Equally because of the distributed nature of some devices, network bandwidth considerations and communication protocols need to be properly evaluated.

Other considerations posed by IoT are more ethical. For example, gathering data from car telematics to assess accident risk and determine insurance premiums is becoming widely accepted. But what if an insurer denied you medical insurance based on data collected by an implant or wearable device?

On a broader societal scale, the ethics of surveillance may soon be tested as governments risk impinging individuals’ rights to privacy by pursuing their own motivations to prevent crime¹.

1. <https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html>



4

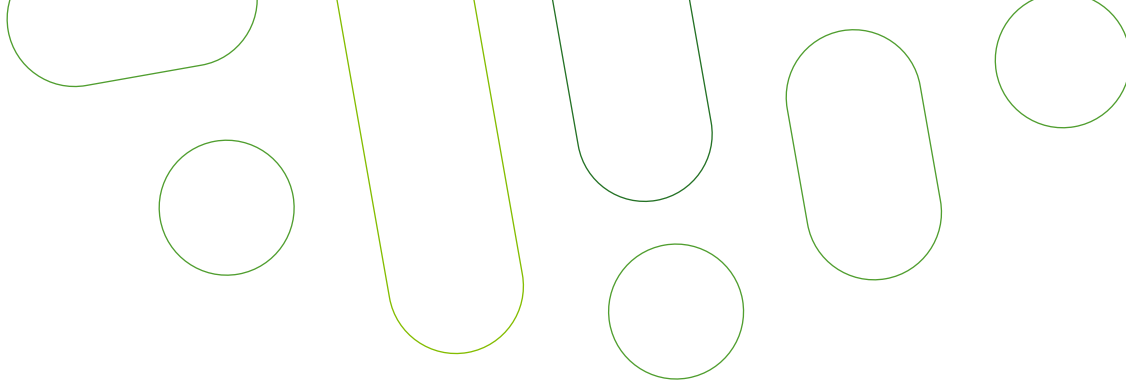
Data Privacy and Ethics

Digital transformation is all about getting new and useful insights into markets, business processes and/or customers. Yet it also poses ethical questions. Every industry will come across its own unique dilemmas.

At the very least, organizations will need to satisfy existing regulations relating to data privacy, which for multi-nationals involves complying with a complex matrix of obligations impacting different jurisdictions. New rules such as the General Data Privacy Regulation (GDPR) in Europe and the California Consumer Protection Act are providing a benchmark for what constitutes strong privacy regulation. Yet the global perspective is fairly mixed, with many regions lacking similar provisions². As legislation continues to evolve, organizations will be hard pressed just to keep track of all the emerging regulations that are applicable to their business.

Generally, issues of client consent and transparency will be crucial. Equally, customers are more likely to provide consent to organizations that they trust. That trust is often reinforced when a company can add value to the user's experience. Modern digital titans (like Apple, Amazon, Netflix and Google) have done a good job at demonstrating value by carefully studying and modelling users' behavior to present them with more relevant advertising, product or viewing suggestions. A newer wave of companies (such as Airbnb and Uber) have used data and technology to connect new sources of supply (peoples' spare rooms or those who want to earn money by providing rides) with demand for those services. Just as demonstrating value is of paramount importance to elicit consent, breaches of trust can be equally catastrophic. Facebook's recent turmoil is a case in point. Not only have the short-term PR implications been scathing, but there are potentially longer lasting repercussions on the business.

2. <https://www.dlapiperdataprotection.com/index.html>



5

Chief Data Officer and Organizational Structures

Some key roles are critical to driving digital transformation. The Chief Data Officer is one. Appointing a board-level executive responsible for data is a crucial first step in recognizing the value of that data to any organization. Given the importance of data to digital strategies, the Chief Data Officer serves a critical role in driving digital transformation for many organizations. Other organizations have even looked to designate a ‘transformer-in-chief’ by appointing Chief Digital Officers to lead their digital transformation journeys.

While these roles are undoubtedly important, true digital transformation requires cooperation from across the entire organisation. A single person may be charged with defining a company’s digital strategy, but it will take agreement from across the organization to execute against that strategy.

Many digital transformation projects require organizations to break down data silos, which in turn will require support from business units that own those silos. Others may require setting up new businesses and/or adopting new practices, which could be seen as threats to established operations. Simply sprinkling data and analytics over an existing organizational structure has turned out ineffective.

Overcoming these hurdles will not be easy. Organizations need to stay focused on business outcomes. Whether that means having a better understanding of customers to develop more compelling products and services, or a better understanding of business processes and supply chains to optimize production of those products and services – data management will invariably hold the key.

Conclusion

The competitive forces of digital transformation have been in motion for some time. Organizations that view data as an asset will inevitably be better at mining, refining and extracting value from it. In doing so, they will discover innovative ways to optimize business processes and deliver value to their customers. In turn, as customers begin to expect more from their product/service providers, they will become more discerning with their purchasing decisions. Staying still is therefore no longer an option.

Technology serves as a key enabler to digital transformation. Cloud infrastructures allow organizations to store, process and distribute ever larger volumes, velocity and variety of data. AI and machine learning have provided the tools to mine that data in pursuit of meaningful insights. And the Internet-of-Things provides a much greater variety of end-points with which to collect new datasets and derive new insights.

But in order to be effective, technology needs to be supported by the right people and process. As organizations seek to leverage their data assets, they will encounter numerous governance challenges. Who owns the data? Where is it stored? Is access properly controlled? Are there restrictions on its use? All these questions need to be answered in tandem with the key commercial imperative: how can I make use of data to add value to my business and better serve my customers?

Learn more about how Collibra can help you on your digital transformation journey:

As the leader in data governance and catalog software, Collibra helps organizations across the world gain competitive advantage by maximizing the value of their data across the enterprise. Collibra is the only solution purpose-built to address the gamut of data stewardship, governance, and management needs of the most complex, data-intensive industries. Our flexible and configurable cloud-based or on-premises solution puts people and processes first – empowering every data citizen to find, understand and trust the data to unlock business value. Learn more at collibra.com.

Data Governance

Catalog

Data Privacy