Deloitte.

The future of digital identity

What does it mean to you?

By Mike Wyatt, Jan Vanhaecht and Guus van Es

MAKING AN IMPACT THAT MATTERS since 1845

01
02
03
04
05
06
07
08
09
10

Content

01 **Introduction**
Digital identities at the core of your business

02 **Digital identity for your employees and (third party) co-workers**
The paradox of facilitating employees and protecting the business

03 **Digital identity for customers**
Opportunities and responsibilities

04 **Digital identity for devices and applications**
A modernized approach

05 **How to approach the digital identity opportunity**

06 **International perspective**

07 **The role of senior leadership**

08 **Practical considerations for next steps**

09 **Digital identity for a more responsible and sustainable business**

10 **Contact**

01
02
03
04
05
06
07
08
09
10

INTRODUCTION

Digital identities at the core of your business

As wave after wave of technological progress transforms our lives, with data as its prime driver, there is one key that unlocks all the benefits: digital identity.

Around the globe, digital identities are becoming increasingly indispensable for organizations of all kinds - private companies, government bodies and civil society organizations - and for the people and organizations they serve.

Putting digital identity at the centre of your data driven business model brings concrete business benefits. More efficiency as governance and processes are aligned. Better user experience as colleagues feel facilitated in their work. More revenue as customers appreciate a better digital customer journey. Increased protection and privacy as human errors are reduced and access to data is more controlled.

Organizations today have a range of digital identities: for themselves and their employees, including (third-party) co-workers), for the people they serve (customers, citizens) and for their internet-connected devices and applications.

In this report we explore the different forms of digital identities and highlight the potential business benefits to effectively leverage digitalization in a responsible way.

01
02
03
04
05
06
07
08
09
10

Digital identity for your employees and (third party) co-workers

The paradox of facilitating employees and protecting the business

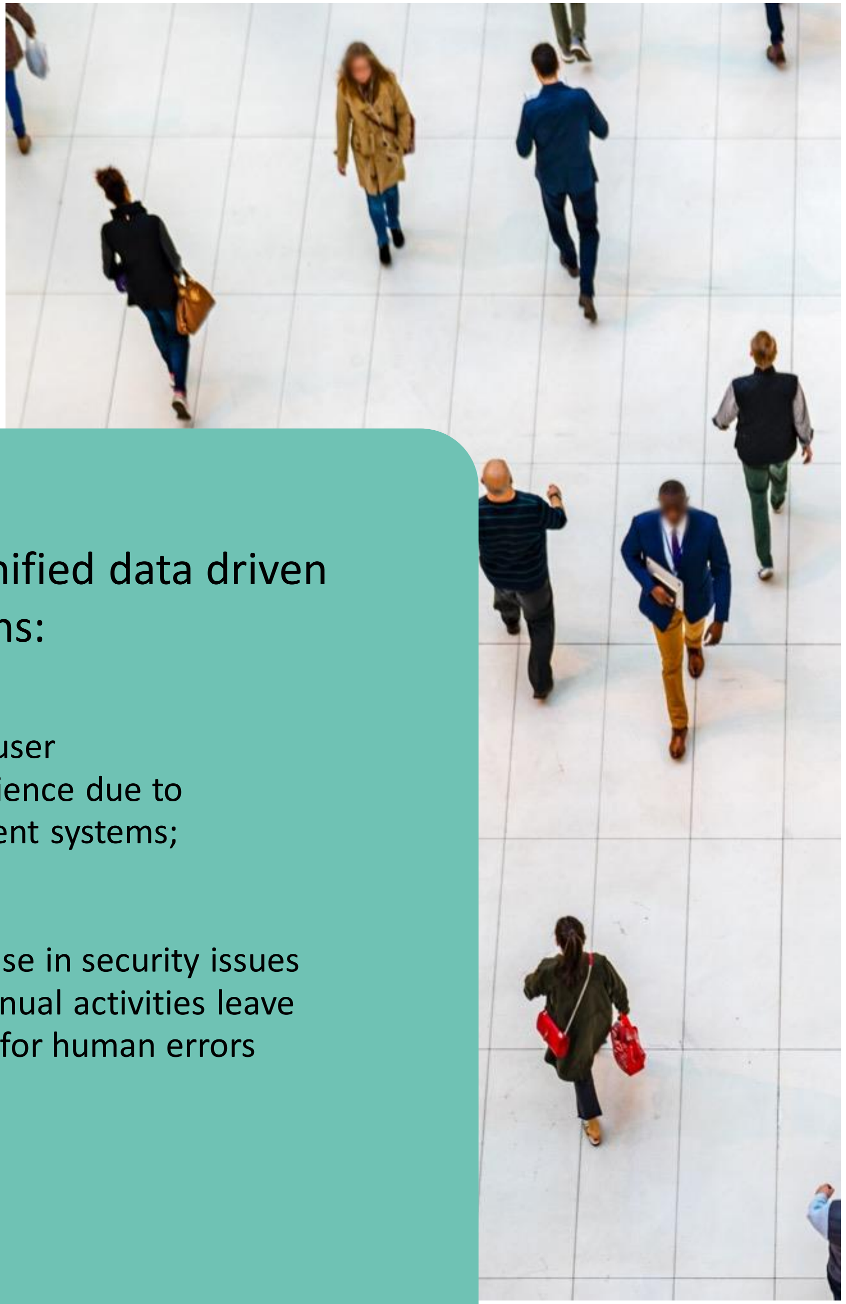
As organizations digitize and become more data driven, the purpose of digital identities is to both facilitate employees and the organization in leveraging technology and data with low friction, and to protect the organization at the same time.

With digital identities, you know and control who has access to which systems and data, and with which rights, this is often referred to as role based access. When employees join, switch roles and leave, their access to systems and data is adjusted. Any change in the employee ‘identity lifecycle’ will have implications on the systems and data an employee should have access to and with which rights. The relevance of protecting your data is increasingly apparent from the evolving sophistication of attackers’ social engineering techniques where through human interaction (for example text, voice or video via email, social media or phone) manipulation is used to obtain sensitive information. At the same time there is an increase in data protection and privacy rules and regulations organizations must comply with.

In summary, the paradox is immediately apparent: how can an organization minimize administrative issues, whilst protecting the organization and its data at the same time? In other words, how do you balance an easy user experience with data protection. Quite a challenge for start-ups, but even more so for organizations who have existing legacy processes, governance, and technology to deal with, especially as they become more digitized internally and externally.

Meanwhile, collaboration within industries, value-chains and across ecosystems is becoming increasingly digital, making it both more urgent and more difficult to manage digital identities. Data access rights may be more situational, for example in different cross business unit or cross value-chain project teams.

A well-executed digital identity strategy is fundamental for companies to efficiently and effectively leverage digitalization in a responsible and secure way. Senior management generally acknowledge this, but often think or act like digital identity is a technology issue as they lack clarity on how digital identities create real value for their company in the short, medium, or long term. Unfortunately, this lack of understanding can lead to reduced leadership attention or guidance, and silos within organizations.



The associated consequences undermine the success of the unified data driven business model and can impact the organization in five domains:

01 mounting inefficiencies when governance and processes are not aligned;

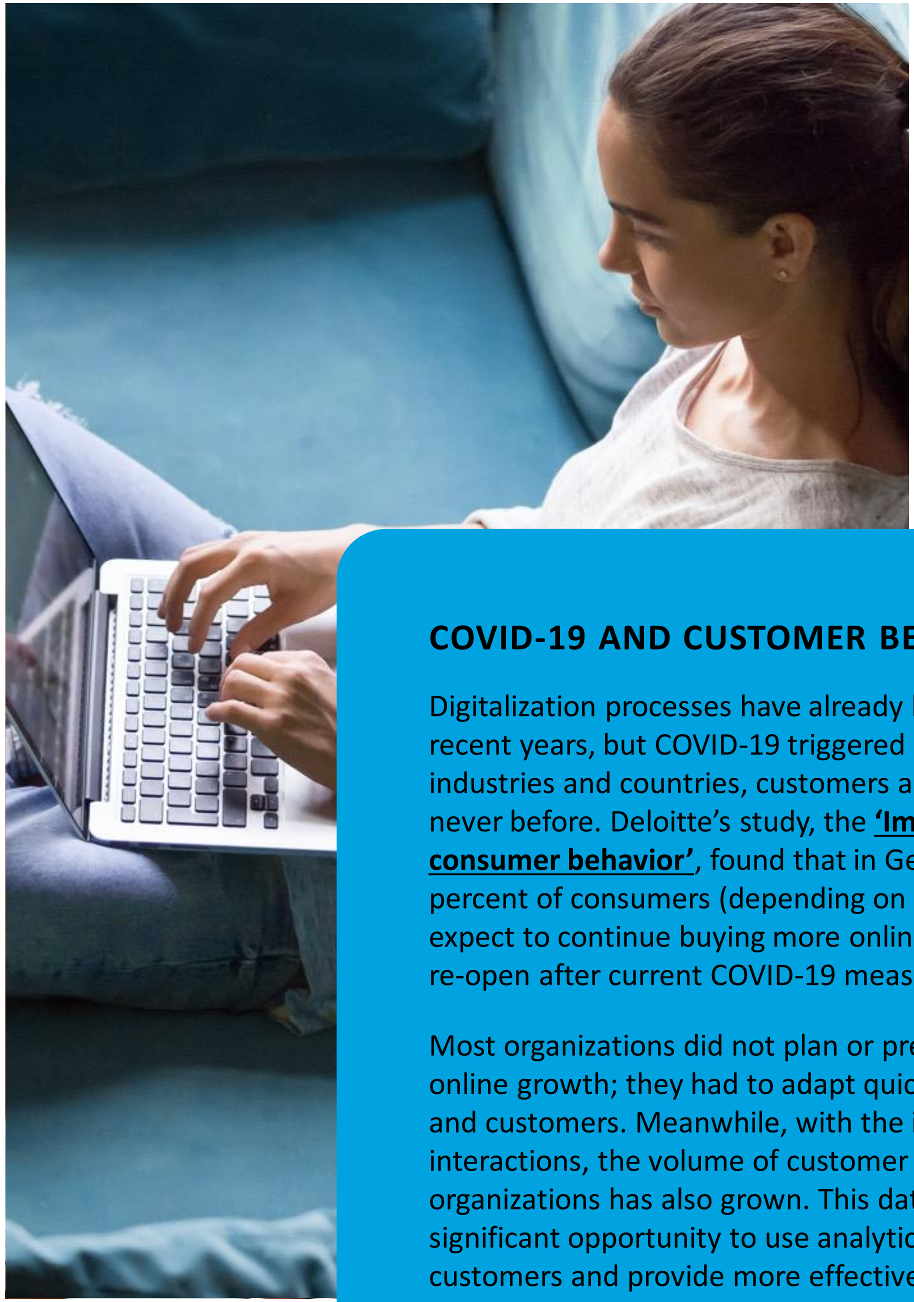
02 added complexity with isolated, often operational and technology driven decisions;

03 lack of control when activities are predominantly manual; and

04 poor user experience due to different systems;

05 increase in security issues as manual activities leave room for human errors

01
02
03
04
05
06
07
08
09
10



Digital identity for customers

Opportunities and responsibilities

Properly managing the digital identity of the people you serve (customers, citizens, or other businesses, let's just call them customers here) can lead to increased customer loyalty and revenue. After all, people favor data-driven organizations offering better digital customer journeys. Other benefits include increased data and privacy protection, thanks to a reduction in human errors and more tightly controlled data access rights.

COVID-19 AND CUSTOMER BEHAVIOR

Digitalization processes have already been speeding up in recent years, but COVID-19 triggered a quantum leap. Across industries and countries, customers are embracing digital like never before. Deloitte's study, the **'Impact of COVID-19 on consumer behavior'**, found that in Germany, between 24-46 percent of consumers (depending on the market segment) expect to continue buying more online, even when stores re-open after current COVID-19 measures are relaxed.

Most organizations did not plan or prepare for this level of online growth; they had to adapt quickly to retain business and customers. Meanwhile, with the increase in digital interactions, the volume of customer data held by organizations has also grown. This data availability offers a significant opportunity to use analytics to better understand customers and provide more effective and personalized customer contact and user journeys. But simultaneously, the increase in valuable data has led to an increased risk of cybercrime. Privacy obligations have grown and compliance is a bigger challenge.

COVID-19 has made proper management of your customers' digital identities even more important. Decisions of organizations and their senior leaders concerning digital identity strategies and operations will help define your customers' digital experience. This digital experience, in turn, will determine their willingness to become customers in the first place, their loyalty level and their inclination to recommend you to others.

Customer requirements

With the acceleration of digitization, customer requirements around digital experiences have changed. Why do customers select a specific company for their initial service or product purchases? And what turns them from one-time customers into repeat ones? To a large extent, it's their digital experience, including the following factors:

> How easy it is to register as a customer?
>
> How seamless it is to access information of interest?
>
> How personalized the service is?
>
> How easy it is to purchase and pay?
>
> How secure they feel the service is, including how their own personal data is handled?

Your customers' digital experience is defined by identity management. In the future, customers will increasingly expect your organization to have a single digital identity for them, a seamless 'hybrid' experience that connects their physical and digital behavior not only within individual organizations, but across multiple organizations and governments.

An example of this so-called hybrid or single identity is the use of biometric client identification in retail stores. This process involves identifying a client at a store's entrance and continuously monitoring his purchases, which are then charged automatically into their credit card when on leaving without the need to physically check out. In the future, it is likely that customers will increasingly expect your organization to have a single digital identity for them, one that connects their physical and digital behavior not only within individual organizations, but across multiple organizations and governments.

01
02
03
04
05
06
07
08
09
10

Benefits of customer identity management

Improving your customer's digital experience with proper identity management has many benefits, depending on the type of organization and the chosen strategy.

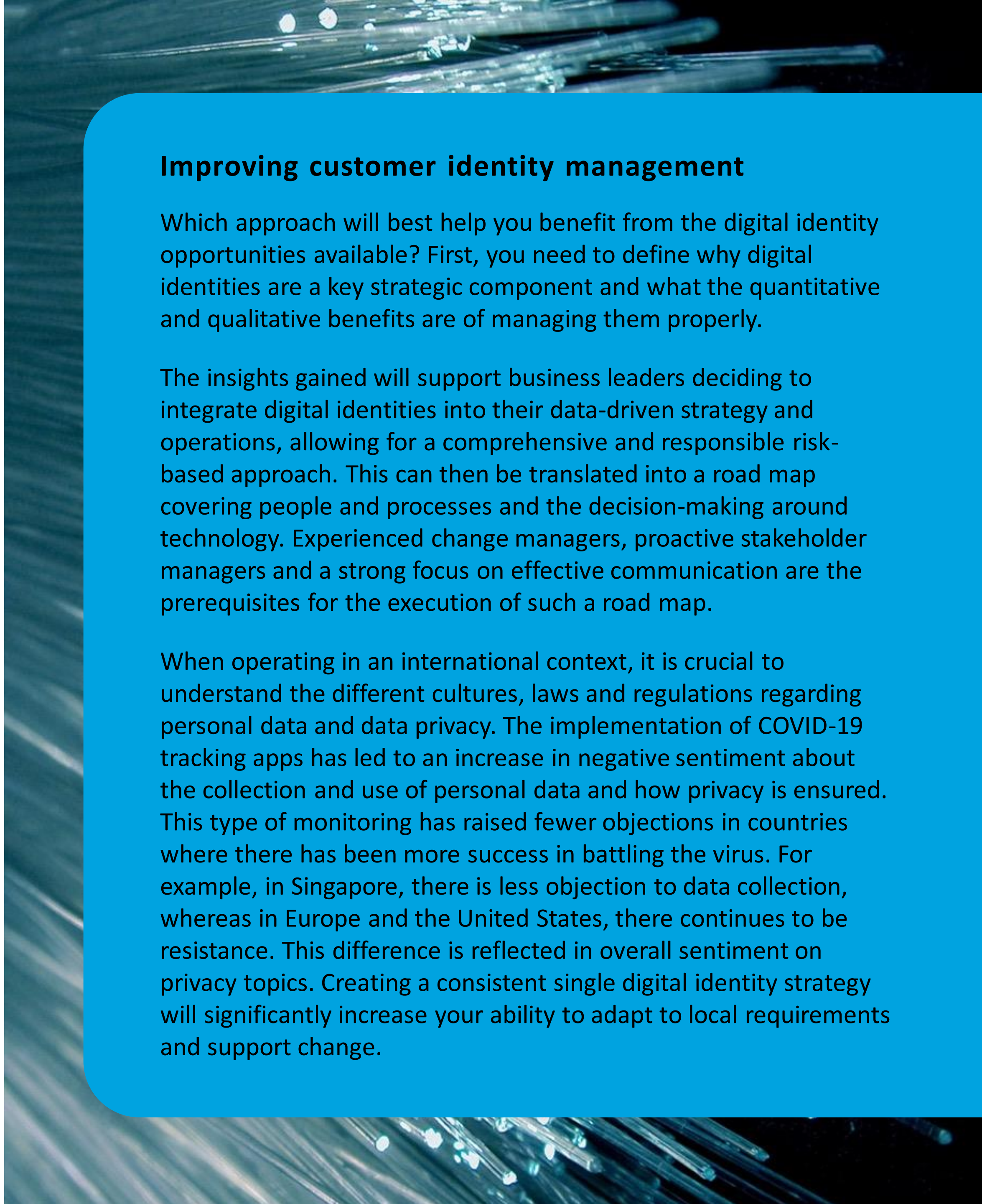
Brand integrity protection. A responsible organization wants to be known for protecting customer data and privacy. Breaches damage brand integrity, leading organizations to lose the trust of investors and customers.

Increased sales. By using data to improve user journeys, your customers are likely to be more loyal. Seventy percent of customers are more likely to buy from an organization demonstrating the highest privacy standards.

Increased operational and cost efficiencies. By creating centralized governance and automating processes, you can reduce manual activities and their associated costs. Examples include validating and registering new customers and automating promotions based on profiles.

Accelerating value chain transformation for b2b and b2b2c. By properly managing numerous digital identities—both those of employees and customers—it becomes easier to transfer authority. Each person will have their own set of mandates across the value chain, supporting business integration.

More business control. An increase in security by allowing for real-time automated reports into who has access into which systems and associated data improves governance, privacy and audit compliance.



Improving customer identity management

Which approach will best help you benefit from the digital identity opportunities available? First, you need to define why digital identities are a key strategic component and what the quantitative and qualitative benefits are of managing them properly.

The insights gained will support business leaders deciding to integrate digital identities into their data-driven strategy and operations, allowing for a comprehensive and responsible risk-based approach. This can then be translated into a road map covering people and processes and the decision-making around technology. Experienced change managers, proactive stakeholder managers and a strong focus on effective communication are the prerequisites for the execution of such a road map.

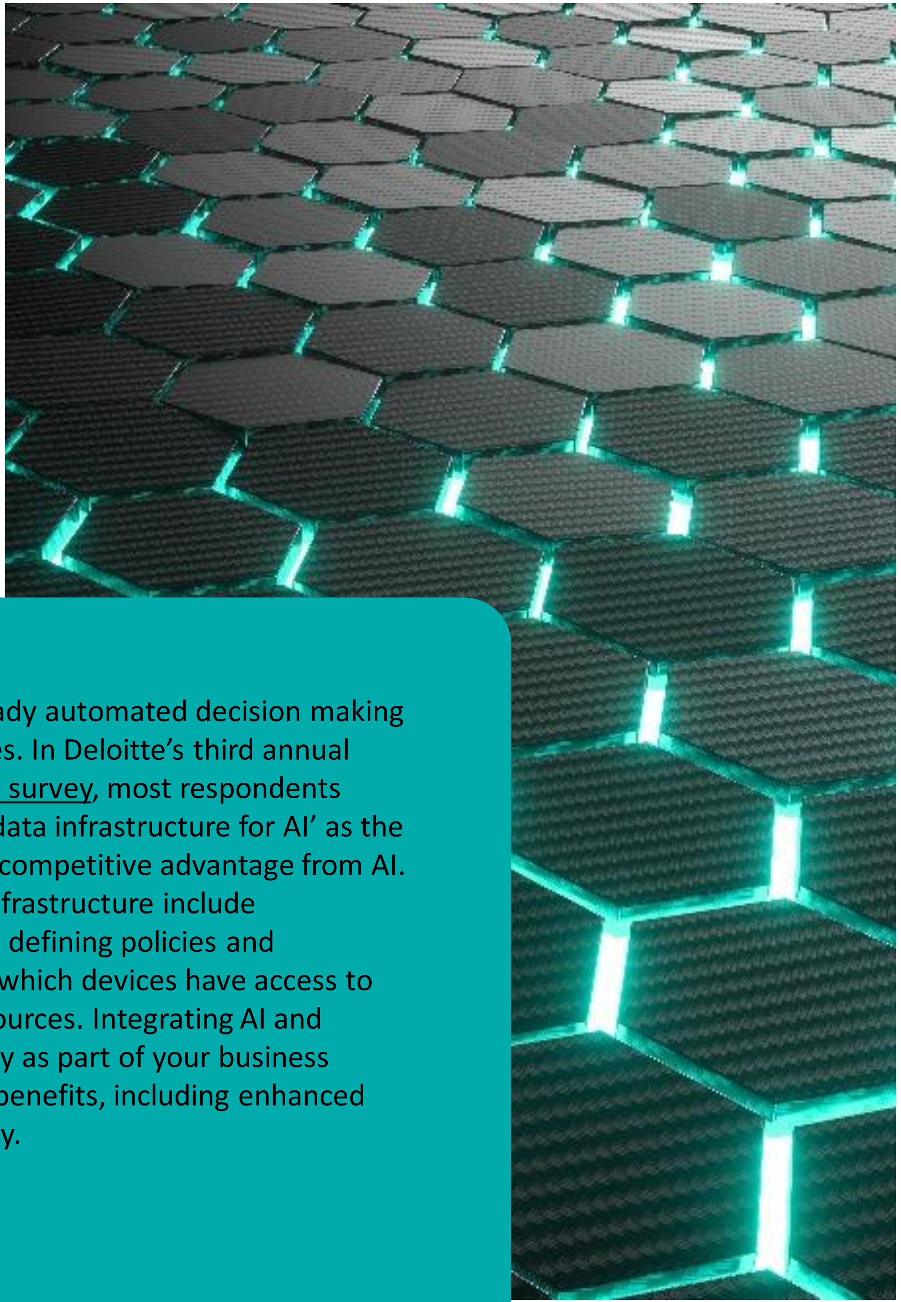
When operating in an international context, it is crucial to understand the different cultures, laws and regulations regarding personal data and data privacy. The implementation of COVID-19 tracking apps has led to an increase in negative sentiment about the collection and use of personal data and how privacy is ensured. This type of monitoring has raised fewer objections in countries where there has been more success in battling the virus. For example, in Singapore, there is less objection to data collection, whereas in Europe and the United States, there continues to be resistance. This difference is reflected in overall sentiment on privacy topics. Creating a consistent single digital identity strategy will significantly increase your ability to adapt to local requirements and support change.

01
02
03
04
05
06
07
08
09
10

Digital identity for devices and applications

A modernized approach

The data revolution requires a new approach to digital identity. These days, digital identities are needed not just for people and organizations but also for devices (any piece of equipment connected to your organizational network) and applications (any computer program designed to perform a task in one of your organizational processes).



Traditional ways of organizing and accessing data will not be sufficient as we move towards artificial intelligence (AI)–based decision-making. This means machine learning (ML) will augment and in some cases replace human decision-making. AI will help organizations create and adopt automated processes across industries, thus replacing low-level or non-scalable human decision making with machine-made decisions. It is expected that costs to organizations in the future will be a fraction of what they are today, thanks to the capability, speed, and scale of machine-based decision-making. To fully leverage such automated decision-making, organizations must analyze which operational processes require human access, which data is involved, and where privileged access is needed.

Some companies have already automated decision making as part of larger AI initiatives. In Deloitte’s third annual State of AI in the Enterprise survey, most respondents selected ‘modernizing our data infrastructure for AI’ as the top initiative for increasing competitive advantage from AI. Examples of modernizing infrastructure include conditional access, which is defining policies and configurations that control which devices have access to various services and data sources. Integrating AI and machine-to-machine activity as part of your business model will bring increased benefits, including enhanced control, privacy, and security.

01
02
03
04
05
06
07
08
09
10

Benefits of device and application identity management

Facilitating and protecting your data-driven business processes with device and application-based identities provides clear business benefits. These depend on your type of organization and chosen strategy, but can include:

Brand integrity protection.

A responsible organization wants to be known for protecting customer data and privacy. Incidents involving data leakage can damage brand reputation and potentially lose the trust of investors and customers. A modernized identity approach, with fewer human interactions can reduce the risk of incidents thus protecting brand integrity.

Increased sales.

Customers' online buying behavior is characterized by what is available and how easy it is to obtain. Ten years ago, Amazon estimated that every 100ms of latency costs the company 1% in sales1. Automating your device and application identities approach improves process efficiency, removes friction from digital customer journeys and therefore enables faster, undisrupted purchasing activity and increased sales.

Increased operational and cost efficiencies.

By creating centralized governance and automating processes, you can reduce manual activities and their associated costs. Examples include validating and registering new customers, and automating sales promotions based on customer profiles. Some organizations have opted to move their identity stack to the cloud, consuming identity-as-a-service, or implementing advanced authentication methods to ensure they protect their users' data whilst benefitting from associated operational and cost efficiencies.

More control and better protection.

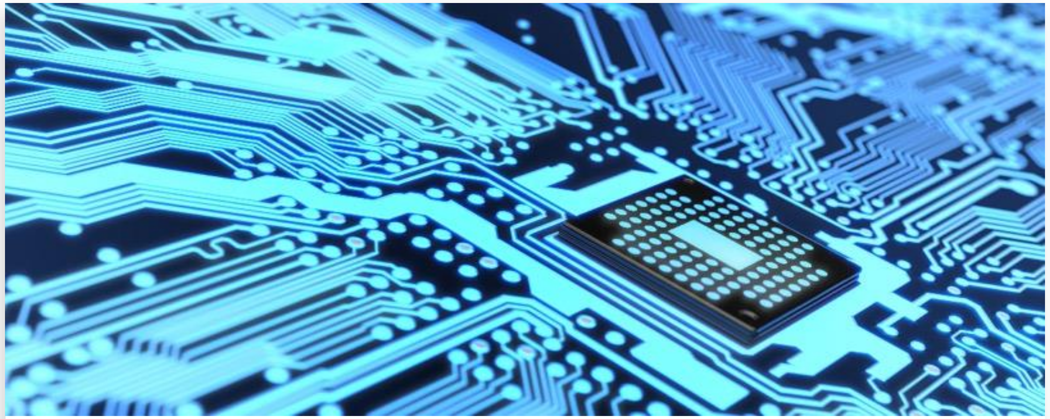
Security risks are increased by the ever-expanding organizational ecosystem caused by moving to cloud and hybrid IT environments, increasing numbers of cloud-based systems, and more remote workers and connected devices. To manage these risks, organizations should have an automated risk-driven approach to data access, including the principle of least privilege. This means a minimum set of users, applications, and devices have access to data and applications, thus providing more control and better protection.

How to approach the digital identity opportunity

There are some key factors to consider in getting things right. Your starting point depends on how far along that digital identity transition journey your organization is. The early stage involves a business benefit specification, making clear why digital identities are a key strategic component for the organization. C-level business leaders require insight into both quantitative and qualitative business benefits of a digital-identity-enabled user experience. They will want to know exactly what operational and cost efficiencies it will deliver, and how it will impact their control.

Examples of potential business benefits are:

- **Drive digital transformation – once you have aligned governance and processes, and simplified your technology architecture, you can accelerate and control digital transformation across the organization as well as in any merger and acquisition activity.**
- **Improved user experience – as you have an improved security posture with advanced authentication, users have a better experience and the organization has a higher level of authentication assurance.**
- **Increased operational and cost efficiencies –by creating centralized governance and automating processes such as new joiners, movers, and leavers processes, you can reduce manual activities and their associated costs.**
- **More business control – you can create real-time automated reports into who has access to which systems and associated data, enabling governance, privacy and audit.**



By providing business leaders with insight into the quantified and qualified business benefits of digital identities, you add strategic value to the business model. This will support the integration of digital identities into the data driven strategy and operations allowing an overarching and responsible risk management based approach to business priorities. This can then be translated into a roadmap covering people and processes, and the associated decisions around technology.

The majority of such roadmaps unfortunately do not succeed to deliver the business benefits in full. This is a result of appointing inexperienced teams with knowledge of their part of the organization but no change management skills and/or understanding of other business areas. This leads to silos and poor collaboration across roadmap clusters, teams, and regions. At the same time the communication plan often ignores important stakeholders who are not engaged due to a lack understanding of the roadmap benefits and their role. As such, key success factors in any such roadmap include experienced change management, proactive stakeholder management, and a focus on effective communications.

01
02
03
04
05
06
07
08
09
10

International perspective

Within an international organization, levels of digitalization (in terms of adoption and risk appetite) can differ from country to country.

Across the Asia Pacific region, for example, digital identity strategies adopted by more regional oriented companies are diverse, but tend to fall into four broad regional categories:

In South East Asia, companies are on the cusp of introducing digital identities systems, but many are struggling with how to include them in their overall strategy.

Australia is more advanced, with some companies developing their own systems and some buying off-the-shelf solutions.

In India, companies are making sure their data sets are integrated and their channels updated to capture the mobile and web traffic of the growing population.

In China most platforms are developed and run by Chinese organizations with significant market dominance.

Therefore, to create long term value as a business leader, it is relevant to understand that there are different, culturally determined approaches to defining and executing data-driven business models and digital identity plans.

The role of senior leadership

As important as digital identity is, it tends to be viewed by senior management as a tech issue rather than a value creator. Failure to address this issue at senior management level has risks, however:

- Mounting inefficiencies when governance and processes are not aligned
- Poor user experience due to different systems
- Added complexity with isolated, often operational and technology driven decisions
- Lack of control when activities are predominantly manual
- Increase in security issues as manual activities leave room for human error

In Deloitte's 2020 CSO Survey, 70% of respondents rated disruptive growth fueled by a data-driven business model as critical for their organization's success. However, only 13% believed that their organization could deliver on this strategic priority. This survey emphasizes the need for senior leadership team effort when adapting to digital age changes.

01
02
03
04
05
06
07
08
09
10

As stated in our Executive Summary on the Future of Digital Identities, each member of the senior leadership team has a different role to play in developing and implementing the digital identity strategy:

The **Chief Executive Officer (CEO)** is ultimately accountable for the integrity of the brand of the organization. For brand integrity, stakeholder trust is vital. Stakeholders such as investors and clients rely on an organizations' ability to avoid and manage malicious attacks generated through social engineering and misuse of digital identities. The CEO should lead by example by positioning digital identity as key to protecting brand integrity as part of the data driven business model. Top down leadership will have major influence on an organization's risk management as they digitize with digital identities at the core.

For the **Chief Financial Officer (CFO),** control and real time insight into the business is fundamental. In addition, the CFO and its department are a popular target for malicious social engineering to obtain sensitive data and trick organizations for example into incorrectly transferring money. As such, CFOs should ensure proper, automated segregation of duties and advanced authentication to significantly increase control and mitigate the risk of compromised credentials.

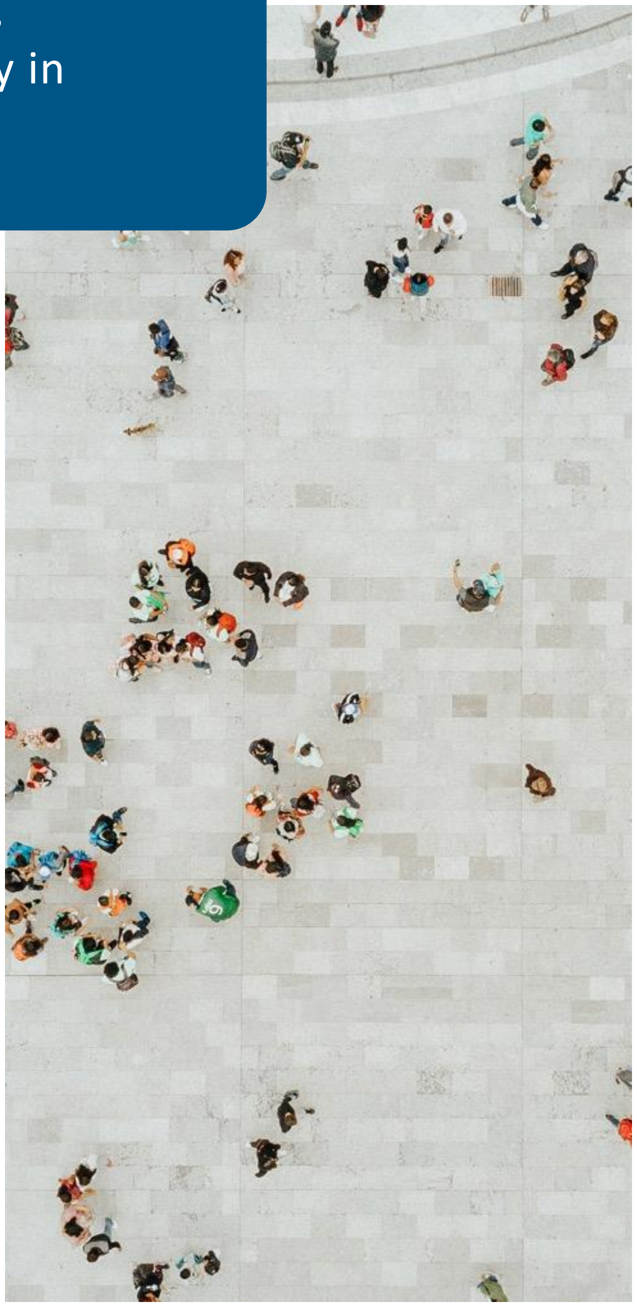
Above all, digital identity is a people challenge that requires the right governance, processes, and technology to succeed. Employees are challenged to demonstrate consistent security "hygiene". It is up to the **Chief Human Resources Officer (CHRO)** to ensure continuous awareness training as part of the training curriculum as well as efficient, uniform HR processes. In that context the (CHRO) must work alongside the **Chief Information Officer (CIO)** and **Chief Information Security Officer (CISO)** to limit human weaknesses as well as IT vulnerabilities.

The **Chief Information Officer (CIO)** is responsible for the infrastructure surrounding business operations. This includes responsibility for all customer data flows. The **CIO and the Chief Security Officer (CSO)** must ensure that the customer has a seamless, frictionless and secure digital experience, and they have to provide the CMO with access to all the right customer data analytics.

For the **Chief Marketing Officer (CMO)** and the **Chief Data Officer (CDO)**, collaboration has never been more important. They should be aligned on how the digital identity strategy supports their wider business requirements. The increase in data will also aid the CMO in understanding the customer and create a consistent hybrid user experience. This can only be done effectively if the CDO monitors how data is gathered, stored and used and if they ensure compliance with privacy laws and regulations.

The **Chief Privacy Officer (CPO)** needs to prevent and contain brand-damaging privacy incidents, as they impact customer trust and loyalty. They should pursue privacy by design, including changes around legacy business processes or systems. To be effective, the privacy officer should be involved in the early phase of each (digital) change process.

It's their joint challenge to align on corporate goals and the overarching business case, while at the same time managing their own interests: the CIO has to achieve the same or more with less budget and resources, while the agendas of the CMO and CSO require investment.



Practical considerations for next steps

We emphasized the importance of incorporating digital identity into your data-driven business model. Strategy development and execution cannot be siloed. To generate effective results, organizations need foundational elements in place.

Firstly, organizations need an empowered strategy function. Whether it is the Chief Executive Officer (CEO), Chief Security Officer (CSO), or any other executive, an empowered executive strategy leader is critical to effective strategy development and execution. In collaboration with the CIO, the strategy leader can help influence and educate executive leaders and board members. This should lead to tech-savvy senior leaders working alongside business-savvy leaders across operations and technology.

With this executive structure in place, senior leadership can ensure that strategy assumptions are properly challenged and that the organization’s security risk appetite is defined. Doing so allows the organization to communicate a consistent message about business priorities, including guidance on digital identity.

01
02
03
04
05
06
07
08
09
10

Digital identity for a more responsible and sustainable business

An effective digital identity approach is about defining business benefits and the ability of an organization to leverage digitalization in a responsible way.

As such, digital identity is core to any organization's data-driven business model and operations. If each executive board member properly manages their specific role, an organization can effectively leverage the endless possibilities of this digital era.

Start improving your digital identity management now!

01
02
03
04
05
06
07
08
09
10

Contact

Would you like to know more about integrating digital identities into your strategy and operations? Visit our website for the latest insights or get in touch with one of us using the contact details below:

Michael Wyatt
Global Identity Offering Leader
miwyatt@deloitte.com
+1 512 226 4171

Jan Vanhaecht
Belgian Cyber domain leader
JVanhaecht@deloitte.com
+ 32 473 62 56 36

Guus van Es
European Identity Offering Leader
guvanes@deloitte.nl
+31 616588460

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 330,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") 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 representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.

DTTL and each of its member firms, and their related entities, are legally separate and independent entities.