Executive Summary

Digital identity should be at the core of any data-driven organization. How do you, as a senior leader, achieve this and help differentiate your organization?

What is digital identity? It is information used by computer systems to identify and establish trust that an organization, person, application or electronic device is what is claimed.

Digital identities are becoming the foundation of our rapidly evolving technology-based and data-driven economy and society. It is a trend across organizations of all kinds; private companies, government bodies and civil society organizations, and the people and organizations they serve.

If an organization gets it right it leads to efficiency and revenue and transformational benefits with an enhanced user experience for colleagues, and a differentiating digital journey for customers or citizens. Data-driven organizations outperform their competitors, being 23 times more likely to gain new clients. Digital identity is also foundational for inclusive growth. Deloitte’s 2019 Future of cyber survey and Rediscovering your Identity support these statements.

But there is a big obstacle to overcome. Too many organizations are failing to put digital identity at the center of their business model and operations and, by this omission, are likely to miss out on the full benefits of responsible digitalization.

Different sources of digital identity create unique personas. An organizational identity is, for example, that of a business or government, or one of its employees. A personal identity is that of a customer of a business, or a citizen of a country. An application or device identity is that of a mobile phone, computer or piece of industrial equipment.

A person’s digital identity, and his or her interactivity with the world, will be multi-faceted and unique to each experience. For example, when an online banking service requires a password and other information from a customer and receives the correct information, the bank knows it is dealing with that customer and no-one else. The customer, meanwhile, knows it can trust that the bank’s digital identity checks will prevent identity theft and the possible consequences associated with that.

All well and good. However, the customer’s digital identity may be unique to only that part of the bank, such as retail accounts, and may not work with other parts, such as the credit card or mortgage divisions. Even if the customer has a single identity covering the entire bank, it will probably only work with that bank. When communicating online with other banks, and indeed any other organization, the customer will need a separate identity. In addition, each organization will carry out additional verifications of the customer’s identity to manage
access, protect personal data and reduce the risk of fraud. These extra checks are inefficient, influencing the customer experience negatively, and the lack of process alignment could lead to damaging audit findings.

What these inefficiencies illustrate is that, despite recent developments, the world of digital identities is far from perfect. Further work is needed to streamline the processes involved and reduce the number of identities each organization, person or device needs. As part of that streamlining it needs to be considered that personal data belongs to the person, and that person will increasingly control their ownership, supported by regulation. As such, data governance and privacy need to be part of an organization’s digital identity strategy.

Creating a digital identity system in the data-driven world

This report examines what business leaders must do to ensure they have a digital identity system in place for their organization, the people it interacts with and its devices that is truly fit for purpose. The system should be designed so that it could, ultimately, be part of a wider ecosystem involving many other organizations, thus allowing the same digital identity to be used across all of them.

Several key factors need to be considered:

- **Business model and strategy.** Senior leadership needs to buy in to the importance of digital identity. They should understand that it must be at the center of the organization’s business model and strategy to strengthen the intersection between security and business service lines.

- **Customer relations.** A seamless and secure digital journey in an omni-channel environment should be created to improve relations with customers and citizens, improving on what most other organizations can offer.

- **Talent.** The right people, with the right knowledge and skills, should be allocated to the appropriate tasks.

- **Legal and regulatory compliance.** A digital identity system should comply with all relevant laws, regulations, industry standards and internal policies, especially those relating to data privacy, data protection and fraud prevention.

- **Execution.** The implementation of a digital identity system should adhere closely to the agreed plan, with little or no deviation.

- **Processes.** The processes involved should be seamlessly integrated across the whole organization’s operations and its objectives, in support of an enhanced user experience.

- **Technology transformation.** A modern approach to technology infrastructure should be taken to facilitate the data-driven organization.

Large enterprises, most medium-sized enterprises and governments already have a digital identity system, so they have to ask themselves, how mature is it? There are five stages to a digital identity journey for each of the above listed key factors

1. **“Unaddressed”**: This is where the organization has made no attempt to get to grips with the issue. All but the smallest organizations will have passed this stage some time ago.

2. **“Rarely addressed”**: This is where a significant proportion of organizations sit. They have started looking at digital identity, but take only tactical and infrastructure-oriented actions, if any.

3. **“Planned”**: This is where most long-established organizations find themselves. They are considering the options for a digital identity system, but have not yet taken any concrete action.
4. “In progress”: This is where steps are being taken to create a system. This stage that has been reached by some long-established organizations, and by all new “digital first” companies that have recently emerged to disrupt the norm. Digital first companies are conceived with digital identity systems in their DNA, and at their inception are already operating these systems and fine tuning them.

5. “Realised”. This is the final state that only a few traditional companies are closing in on, but most fully operational digital first companies are there or close to it.

Where does responsibility lie?

The creation of an effective digital identity system is the responsibility of senior management, the “C-suite”, and the equivalent leadership teams in government organizations. The Chief Operating Officer, for example, has to ask, “How do we stay in control during our digital transformation and limit access to our network only to authorized employees?”, while the Chief Risk Officer will ask “What are the risks of unauthorized staff accessing parts of the network they should not?”

The Chief Marketing Officer will ask, “How do we help our customers navigate our digital channels and make their journey as easy as possible?”

The Chief Security Officer will ask, “How do we keep all our devices, information systems and operational technology safe from cyber attack?”

Governments have a major role to play in creating a supportive legal, regulatory and technical environment. The European Union, for example, has constructed a world-class digital identity and verification infrastructure for its public services and is encouraging the private sector to do the same.

The British government, in response to a “call for evidence” on digital identity, has said it will work with the private sector “to create trust in digital identities”. It has said it will “remove regulatory barriers which prevent the use of secure digital identities” and promote the development of international standards in this area.

More needs to be done

More progress is needed on Identity and Access Management (IAM) if organizations are to achieve the full potential of our technology based, data-driven economy and society.

It is vital for all C-Suite executives, and their equivalents in government, to put digital identity at the center of their data-driven business models and operations and understand its impact. It is their decisions that will determine if their organization can differentiate itself from others and lead change, or be left behind.

So the question they need to ask themselves is this: “What role must I play to help our organization use digital identities to differentiate us from the rest?”
Footnotes


iii Deloitte reports supporting the statement:
Deloitte, Rediscovering your identity, 2019
https://www2.deloitte.com/content/dam/insights/us/articles/6359_rediscovering-your-identity/DI_rediscovering_your-identity.pdf

This publication contains general information only and Deloitte Risk and Financial Advisory is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC. All rights reserved.