DIGITAL POLICY, STRATEGY AND ADVISORY

CORPORATE DIGITAL IDENTITY: BIG CHALLENGES…AND BIG REWARDS

Technological advances and 24/7 business will make corporate digital identity increasingly important. But how will it work? What benefits could it deliver? And can challenges such as cybersecurity and data privacy be overcome?

Corporate digital identity is similar to personal identity: it is how the unique attributes of an entity (or person) are captured and stored so that they can be transmitted electronically to establish they are who they claim. For corporates, a digital identity gives them the potential to access services and interact with various parties in the course of business, without having to resort to human intervention or the use of physical documentation.

In our personal lives, our eyes, fingerprints, passport or social security numbers can serve as identifiers. For corporates, there are a narrower range of identifiers given the absence of physical characteristics. But company registration numbers, bank accounts or sector/industry memberships – often in combination with one another or through a specific channel – can serve a similar purpose. Just as for individuals, the bedrock of corporate digital identity is authentication and trust.

The goal for corporates, and for the financial sector as it seeks to enable its clients to operate in an increasingly digitised world, is to find a straightforward way to prove identity and make that verification clear to others – just as a tick gives Twitter or Instagram users confidence that they are dealing with a genuine person. Moving from physical to digital identification will only be successful if it makes life easier and safer.

Is corporate digital identity a reality?

Countries around the world have widely differing levels of maturity when it comes to corporate digital identity. Those countries that have made significant progress, such as Singapore, United Arab Emirates, New Zealand and Estonia, started by developing a digital identity framework for individuals before subsequently adding corporations. It is notable that countries at the forefront of such developments are smaller and often unencumbered by legacy systems compared with larger countries.

Estonia has perhaps the world's most advanced country digital corporate identity; its scheme allows companies to establish residency without a physical presence. It can also be used to make transparent and automated tax payments. Estonia's corporate digital identity has been leveraged by private sector companies, enabling insurance claims to be paid out rapidly and to provide authorizations for banking services, for instance.

Critical to these examples is the establishment of trust and confidence in the network. Government involvement is important in this respect: most people are comfortable with the idea of governments creating and safeguarding what is known as our 'foundational 'personal identity as part of a national identity scheme, for instance.

Typically, this foundational identity is built on (either by government or private entities) to create a 'functional' or 'industry based' identity. For example, in the medical sector practitioners have a registration number that identifies them as a consultant with a particular speciality. A third type of identity is known as 'transactional' and can be used to facilitate financial or other transactions. One example in the banking world is an international bank account number.

While governments are important for establishing foundational digital identities for corporates, private-sector initiatives can help to ensure standards and interoperability. The Global Legal Entity Identifier Foundation, established in 2014, provides trusted services and open, reliable data for unique legal entity identification worldwide: its 20-character alpha-numeric code Legal Entity Identifier (based on an ISO standard) ensures a counterparty is always identified on financial transactions in the same way.

Why is corporate digital identity valuable?

Corporate digital identity offers a range of potential benefits. At a national level, Estonia has gained significant tax revenues by making it easier for companies to register in the country without having a physical presence.

Digital identity makes it easy to pay taxes (improving convenience for users and satisfaction with government) and stood the country in good stead during the COVID-19 pandemic when digital provision of services ensured that 99% of government services remained available.[1]

For businesses, corporate digital identity offers a way to tackle longstanding challenges. Global trade is complex with multiple players, including exporters, importers, banks acting on behalf of each party, customs, freight forwarders, shippers and insurers. Establishing identities across this chain is critical both to ensure the security of trade and to facilitate efficient access to finance through the issuance of letters of credit or other instruments.

Another use case reflects a more contemporary trend: companies increasingly operate 24/7 and globally. Traditionally, multinational companies had in-country operations and bank accounts to pay suppliers and collect from customers. Technological advances mean that many leading Fortune 500 companies operate an asset-light model with a limited (or non-existent) physical presence. However, they still need to transact cross-border. To do so, they must be able to establish their identity.

[1] https://www.weforum.org/agenda/2020/07/estonia-advanced-digital-society-here-s-how-that-helped-it-during-covid-19/

At the heart of this challenge is increasingly onerous know-your-customer regulations (KYC), which are costly for banks and create potential delays for corporates. Financial services firms are eager to find ways to make KYC more efficient in order to avoid false-positives and distinguish between similarly named companies or multiple entities within a group. Corporate digital identity is widely seen as key to improving how KYC works.

Overcoming challenges

The range of hurdles to establishing viable forms of corporate digital identity are formidable. Most obviously, a digital ecosystem must be created that is robust enough to withstand the proliferation of cyber threats. Moreover, while the pace of technological change is accelerating, in many instances there is limited regulatory infrastructure to support deployment of technologies such as blockchain or the internet of things. International standards also need to be developed to support the exchange of data across borders and data protection laws must be updated to ensure security and privacy.

Given the tense geopolitical climate, building a consensus on such issues – and facilitating interoperability more generally – could be challenging. However, as the implementation of the GDPR in Europe shows, it is possible to design-in protections that meet regional regulatory requirements and still allow for global operations. Similar adaptability is evident in corporates' efforts to accommodate US concerns about the data security of popular mobile apps.

Nevertheless, there are also significant challenges at company level. For an interoperable corporate digital identification scheme to be successful, corporates will need to reassess their business strategy, how they store and exchange data, and integrate new technologies such as artificial intelligence to process and interpret it. Central to this is understanding the impact on entitlements to information, to ensure that only the right people can access information, having received appropriate authorisation.

Change will be incremental

Compared to digital identification for individuals, digital identification for corporates it at a nascent stage, with efforts to date largely focused on research rather than implementation. In the near term, the success of closed networks, such as that in Estonia, is likely to spur other countries to embark on similarly ambitious national projects that encompass corporate digital identity. Scalable global networks – in which banks are likely to play a pivotal role – are expected to take many years to emerge.

The long-term timescale of such developments should not discourage governments, banks and corporates from seeking to tackle the challenges of corporate digital identity, however. Rather than a big bang approach, there are likely to be a series of incremental gains that will offer opportunities for greater efficiency, enhanced resilience, and improved flexibility to meet the needs of companies in an increasingly connected, always-on and instantaneous world.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

GRA32034 12/20