MAGICARD®

The future of Identity

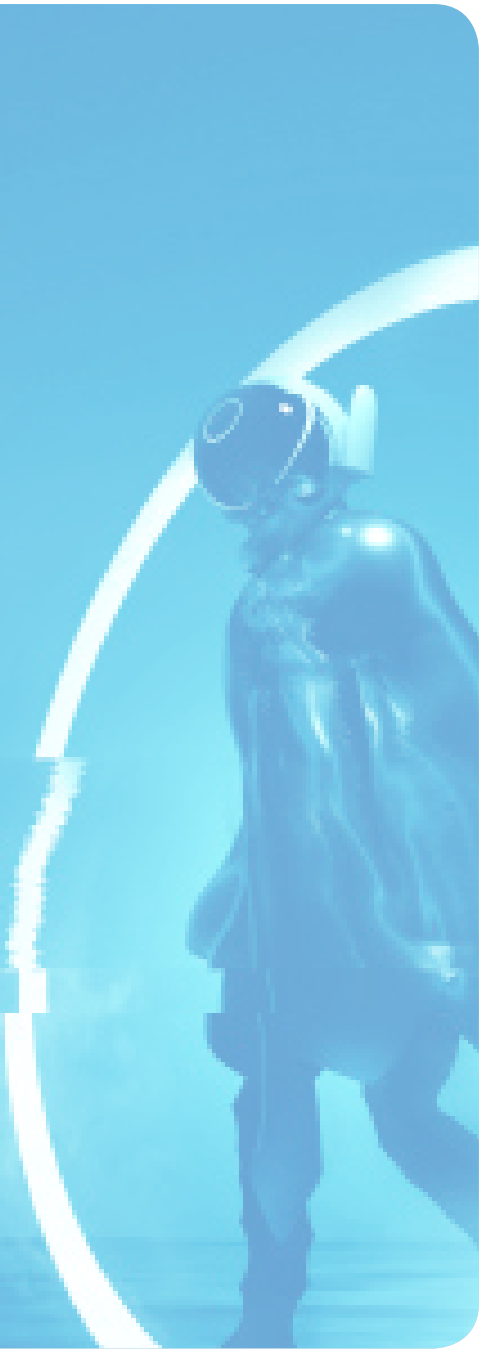
Table of Contents

Introduction

Before we take a deep dive into the future of identity, it would be prudent to understand what constitutes an individual's identity. The most visible aspect of a person's identity is his/her photograph or facial recognition. After all 'putting a face to a name' does help put things in perspective for most, often setting the right tone and expectations of your interactions ith the individual. However, identity is made up of many other aspects apart from a photograph. It includes:

- Fingerprints
- Iris recognition
- Ear prints
- Gender
- Teeth
- Voice

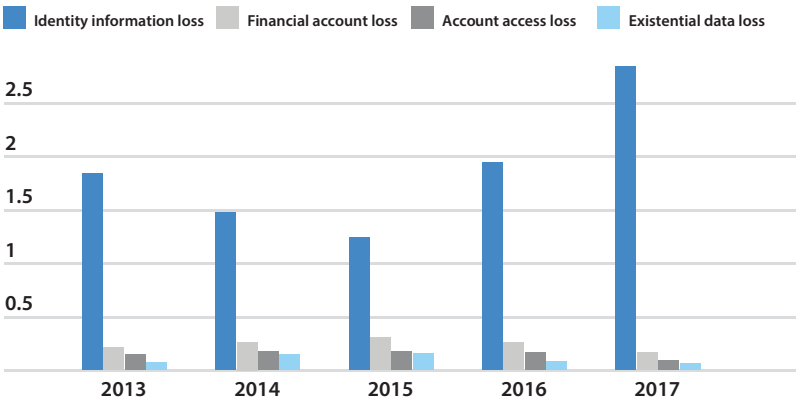
And these are just the physical form factors. If you add context, location, style of dress, signature, identity becomes a complex sum of attributes of an individual. The TechVision Research Group says that identity is one of the most fundamental building blocks for any level of communication, collaboration or commerce within and across an organisation but that it also brings with it a fair share of fundamental challenges including protecting individuals' privacy and the theft of identity data. Over the last few years many organisations have seen firsthand how these two challenges can steamroll them, resulting in identity data becoming more of a liability than an asset.



The increasing trend of identity theft

Out of all the kinds of breaches that occur – identity information loss, financial account loss, account access loss and existential data loss - identity information loss tops the list.

Data breach by type frequency scores



Frequency scores are calculated as the ratio of frequency of a type of loss and the sum of frequencies for other types of data loss[1].

Identity information includes but is not limited to names, dates of birth, addresses and account passwords of consumers. In the last five years big corporates such as Yahoo, eBay, JP Morgan Chase have fallen victim to hefty losses as a result of identity theft.

According to consumer credit reporting company, Experian, identity data ranging from subscription services, credit card data and passports can fetch anywhere between a $1 to $2000 when resold or misappropriated, clearly explaining the increasing trend of identity theft – a staggering 10 billion identities since 2013.

The healthcare industry that by far has the most number of breaches compared to any other industry also has an alarming story to tell. Prescription fraud in England – when people who are not entitled to free prescriptions assume fake identities and abuse the healthcare system – costs the National Health Services (NHS) £256m a year.

[1] The Conversation | Data Breach Live Index

What makes identity data susceptible to breach?

When it comes to managing identity data, organisations need to determine and enforce appropriate access to enterprise systems and applications and this comprises two primary components: authentication and authorisation. While authentication looks at identifying who you are via a host of enablers such as passwords, PINS, digital certificates, one-time password tokens, etc, authorisation looks at providing access to you basis your entitlement and/or affiliation once the identity has been determined.

The issue of course is the grey area of these enablers – they are imperative in today's world because self-assertion of identity simply won't suffice, but at the same time most of these enablers can easily be compromised. Shoulder surfing - the practice of looking over the shoulder of a user at an ATM or a secured access facility in order to obtain their personal identification number, password, etc is quite common. Similarly trojan software that prompts users to download fake applications can create havoc by relegating control of your device to the hacker who then proceeds to intercept messages containing OTPs etc.

The way forward: single ID solutions are NOT enough

In a world that is rapidly changing thanks to the sweeping waves of a digital transformation, a single ID solution is just not robust enough to handle the rigours of a foolproof identity and access management (IAM) system. Combining security layers or components to create a 'true identity' is the way forward.

Some of the options that have gained popularity include the usage of biometrics – fingerprints and retina scans, using a mobile phone or wearable device for easy and quick identification and even small RFID implants under the skin that grant immediate access to facilities. If the latter option seems out of a science fiction thriller, this couldn't be farther from the truth. Thousands of people in Sweden have more than just dabbled with this idea and injected microchips in their hands as far back as 2015. For many it's opened a new way of life, where the microchip replaces membership cards to gyms, provides a hassle free option of booking a train ticket, replaces the need to carry keys, etc[2].

But perhaps one of the most popular and convenient means of identification is fingerprint biometric authentication. It is used widely across organisations as a means for employees to log in and log out for the day, gain access to certain facilities etc. Fingerprints are a surefire method of authenticating an individual's identify because unlike PINS and Passwords, they cannot be stolen, lost or forgotten. In an emergency situation such as in a healthcare setup, fingerprint biometric authentication can be the difference between life and death. When the prints are stored on a smart ID card, it can limit treatment areas in the hospitals to only legitimate staff, thereby protecting patients. Patient biometric cards that are linked to crucial medical records such as blood type, drug sensitivities and allergies have huge potential in saving lives, especially when patients arrive unconscious and accurate authentication is crucial.

[2] https://www.scmp.com/news/world/europe/article/2145896/thousands-people-sweden-get-microchip-implants-new-way-life

Single trusted login vs de-centralising information - the debate is on

Governments world over are the custodians of their citizens data and they are in fact the most vulnerable to identity data breaches. While India's unique identity card database (aadhar) has received its fair share of criticism for not being secure enough, the UK government's identity assurance system – GOV.UK Verify that is intended to provide a single trusted login across all UK government digital services is facing a number of teething issues. A report from the National Audit Office claims that the UK government's flagship identification scheme has fallen way short of its target of registering 25 million users by 2020 and has only been able to notch up 3.6 million users so far[3].

A technology that is rapidly gaining ground as a potential option to safeguard personal data records is blockchain. Often misunderstood and related simply to what it has achieved in the space of Bitcoin and other crypto currencies, blockchain is a next generation database that decentralises information rather than maintaining it in one central location. This feature of blockchain is what makes it so attractive to collect, move and secure data. A common analogy is to compare the ease of robbing a house versus robbing an entire city. Blockchain will allow information to be stored across the entire city with control firmly in the hands of the individual who has the cryptographic private keys needed to access the dispersed information.

Of course it is still early days for utilising blockchain as an efficient means of managing personal data records, but the idea of encrypting data holds immense value and can be implemented swiftly. Unfortunately enough, companies till now have been found wanting in this area. Digital security company Gemalto says that of the whopping 9.2 billion stolen records that have been recorded since 2013, only a meagre 368m were concealed from potential hackers through the use of data-encoding technology.

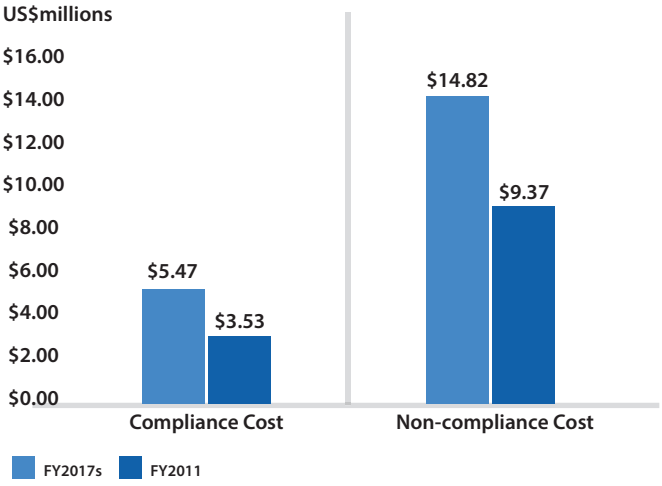
[3] https://www.bbc.com/news/technology-47444308 Verify: Inquiry criticises government ID scheme

Growing costs of regulation and why companies need to rethink how they safeguard data

One of the most defining pieces of legislation that has come out in the recent past is the EU's General Data Protection Regulation (GDPR) that seeks to enhance consumers' privacy protection, holding the companies who store the personal data records accountable and punishable by law for frauds committed if any. According to a survey conducted by global law firm, Paul Hastings LLP, the costs for a Fortune 500 company to comply with the strict guidelines of GDPR could run into $1 million just for technology alone. Of course the costs of non-compliance with GDPR are even more prohibitive, amounting to fines of €20m or 4% of a firm's global annual sales figure – whichever is greater.

Ponemon Institute and Globalscape also recently conducted The True Cost of Compliance with Data Protection Regulations to determine the full economic impact of compliance activities for a representative sample of 53 multinational organisations.

The study showed that while the average cost of compliance for organisations was currently US $5.47 million dollars, a 43 percent increase from 2011 when the study was first done, the cost of non-compliance was even higher.



Ponemon: Difference between compliance and non-compliance cost

Conclusion

Whichever way you look at it, companies can ill afford to do nothing when it comes to securing identity data. In fact it would be astute to say that identity and security go hand in hand - you can't think of securing something without knowing who is entering the system and what their rights are. Similarly you can't establish identity if the system is insecure in the first place.

With Identity management systems rapidly scaling over the next five years in response to trends such as an all-pervasive Internet of Things (IoT) ecosystem, everything moving to the cloud and increased proliferation of wireless and mobile /BYOD, organisations must act now before it is too late.

In the meantime, a step in the right direction today is the ability to capture information in a usable form. By that we mean personal information that's not simply a 2D photo ID badge as that is only useful if the person reviewing the ID is known to the badge holder. Multifunction chips which can identify an individual in the context of location, biometrics and other physical attributes in conjunction with other technology such as mobile phones are the way ahead.