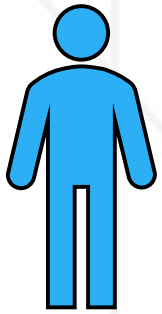
# Identity in a Digital World

## Key concepts and definitions

**Natural Person**



**Personal Identity**

How a person sees themselves

e.g., 25yrs old forever

**Persona**

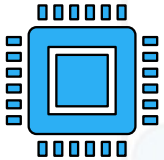
How a person presents themselves to others in different situations,
e.g., work colleague, friend, parent.

**Digital Persona**

How a person presents themselves online (or how an external entity perceives a person),
e.g., game avatar.

**Machine**

(Application, system, process, bot, robot, etc.)



When a machine is given a digital identity,
the identity must be assigned a human owner.
The owner is accountable for how the identity is used.

**Digital Identity**

A set of data about a subject (person or machine) that allows the subject to engage in digital transactions,
e.g. NHS number & Date of birth

A digital identity and an account can be identical or different.

**Account**

A representation of a digital identity that enables authentication, authorisation and accounting within a specific digital system.

**Identity Proofing**

The act of establishing to a specified level of assurance that a digital identity can be associated with a unique natural person, e.g., a bank requires more proof than a conference organiser.

**Identity Mapping**

The act of establishing to a specified level of assurance that multiple digital identities belong to the same person.

**Authentication**

The act of verifying to a specified level of assurance that a subject in an online transaction is the digital identity being asserted,
i.e., I am who I say I am.

**Authorisation**

The act of verifying that an account is entitled to engage in a specific digital transaction, i.e. has permission from the owner of the resource being accessed.

**Accounting**

The act of recording the activity performed by an account to a specified level of granularity (aka 'logging').

CYBILITY SAVVY

Cybility Consulting Ltd
+44 (0)204 583 2468
enquiries@cybility.co.uk
https://www.cybility.co.uk



CYBILITY
Demystifying Cybersecurity

# Board Assurance – Identity and Access Management

1. **Who is accountable for identity and access management?**
   Whilst IT are typically responsible for operating the access control processes in respect of IT systems that they manage; accountability may best sit with an executive with HR in their remit.

2. **Do we have a definitive list of everyone that is working for us at a given moment in time?**
   If not, what assurance can they give you that only people that currently require access to systems have it.

3. **Does this include external parties that can access our systems such as contractors, IT support providers, work experience students, and so on?**
   If not, it should. Those that pass through may increase the risk of a data breach if they are not identified and provided with security guidance.

4. **How robust is our joiner, mover, and leaver processes?**
   This is absolutely fundamental; without it a security program will not be as effective as it needs to be.

5. **Do they incorporate or trigger the processes for other areas such as facilities, IT, payroll and other system owners across the organisation?**
   If not, the handoffs between processes are likely to result in errors; in particular, movers and leavers may not have their access revoked from all systems in a timely manner.

6. **Do we know which cloud services people are signed up to so we can disable them when they leave?**
   One of the challenges with software-as-a-service is that it's so easy for people to sign up that we can end up with data proliferation without knowing it and putting the services that depend upon it at risk should the only admin leave or cancel the service without retrieving the data for the organisation.

7. **What are we doing about 'insider threat'?**
   Cyber-criminals such as Lapsus$ compromised some large organisations by offering a bribe. Are we compensating our staff well enough? Do we have a culture where it is safe to report incidents?

8. **If someone were bribed or blackmailed for their credentials to access our systems, could we detect it?**
   Whilst not easy or cheap; there are systems that monitor user behaviour over time and can flag unusual activity.

9. **How many 'god' accounts do we have that are active? (domain admins, global admins, etc.)**
   Typically organisations have too many of these as it is easier than figuring out what the minimum privileges required are to perform a task.

10. **Do we have excessive 'local admins'?**
    This increases the chance of an attacker installing malicious software and moving through a network.



CYBILITY
Demystifying Cybersecurity