IBM Security

Identity & Access Management and IoT

CHALLENGES, CONSIDERATIONS AND STRATEGIES

Dr. Angelika Steinacker
CTO IAM, IBM Security Europe

November 2018

IBM

The Charter of Trust: Cybersecurity

A critical factor for the success of the digital economy – through signing up to these principles at a high level and then developing tangible measures to adhere to these principles we as the partners aim to raise the level of cybersecurity. We will also work closely with governments across the world as a private public partnership to raise awareness in these key areas and influence government policy.

Key Principles

Charter of Trust for a secure digital world

charter-of-trust.com

01 Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "it is everyone's task".

02 Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protections across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards such as

- **Identity and access management:** Connected devices must have secure identities and safe-guarding measures that only grant access to authorized users and devices
- **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate
- **Continuous protection:** Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism

03 Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures and business models

04 User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks

05 Innovation and co-creation

Combine domain know-how and deepen a joint under-standing between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage contractual Public Private Partnerships, among other things

06 Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education and trainings – in order to lead the transformation of skills and job profiles needed for the future

07 Certification for critical infrastructure and solutions

Companies and – if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions

08 Transparency and response

Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice, which focuses on critical infrastructure

09 Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs)

10 Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay

The Charter of Trust: Cybersecurity

A critical factor for the success of the digital economy – through signing up to these principles at a high level and then developing tangible measures to adhere to these principles we as the partners aim to raise the level of cybersecurity. We will also work closely with governments across the world as a private public partnership to raise awareness in these key areas and influence government policy.

Key Principles

Charter of Trust for a secure digital world

charter-of-trust.com

01 Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "it is everyone's task".

02 Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protections across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards such as

- **Identity and access management:** Connected devices must have secure identities and safe-guarding measures that only grant access to authorized users and devices
- **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate
- **Continuous protection:** Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism

03 Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures and business models

04 User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks

05 Innovation and co-creation

Combine domain know-how and deepen a joint under-standing between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage contractual Public Private Partnerships, among other things

06 Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education and trainings – in order to lead the transformation of skills and job profiles needed for the future

07 Certification for critical infrastructure and solutions

Companies and – if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions

08 Transparency and response

Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice, which focuses on critical infrastructure

09 Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs)

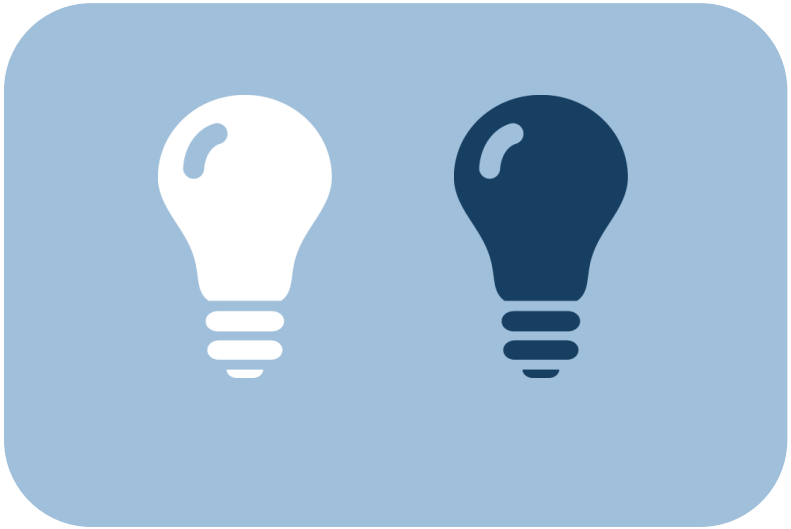
10 Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay

On the internet, nobody knows you‘re a dog

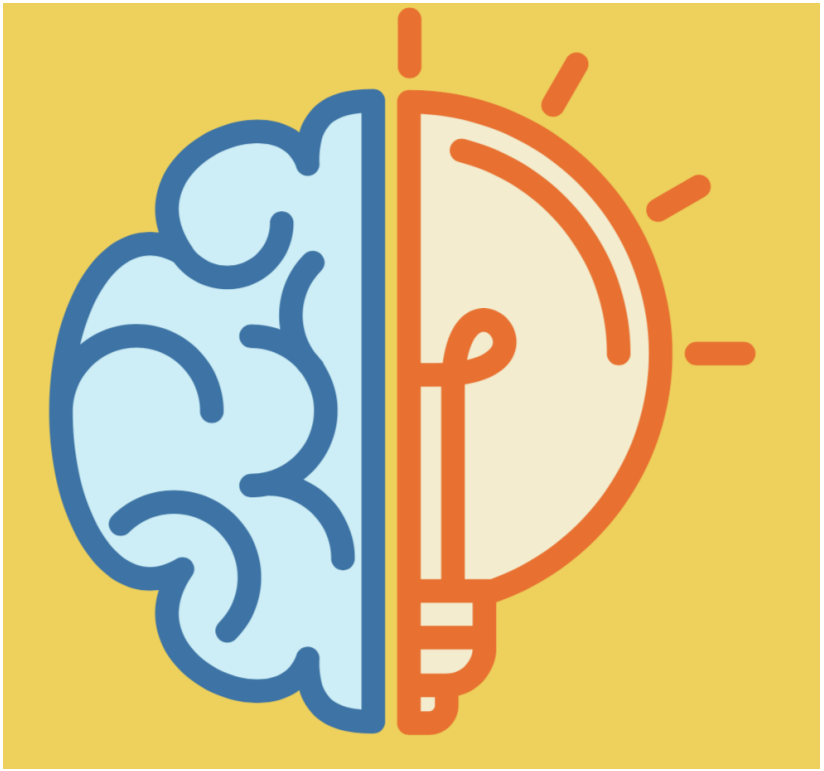
CARTOON CAPTION BY PETER STEINER
Published by *The New Yorker* on July 5, 1993

And 2018?



On the internet, nobody knows you‘re a bulb!

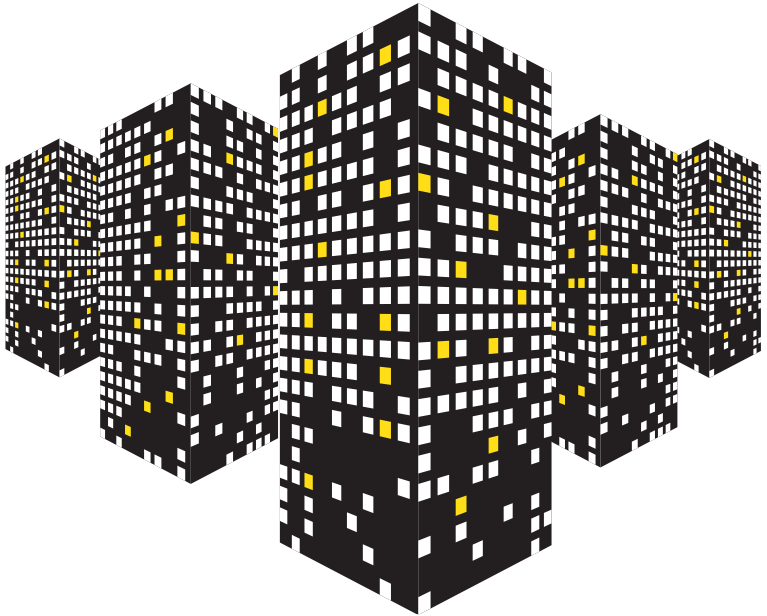
Let’s be more specific: the smart bulb



- Stakeholders
  - Company A owns a building
  - Company B has leased that building and their employees are working there
  - Company C is the facility manager
  - Company D provides applications for building insights
- Scenario
  - The building is equipped with things and an application to get insights on energy consumption, which considerably had reduced costs
  - Company B’s CISO detects that someone has hacked their database through a smart bulb in a conference room
- Questions to ask
  - Who is the owner of security?
  - How could this situation happen?
  - Did the bulb have a Digital Identity?
  - How could it have been prevented?
  - How to support stakeholders?
  - And many more …

Use case: Smart Building – Building insights and reaction

- Industry Trends
  - Challenges in Facilities
    - Operations consume 70% of TCO for a facility*
  - Use data from various sensors and devices to
    - Optimize building efficiency, e.g. for energy
    - Perform maintenance at an early stage
- Characteristics of use case
  - Sensors, devices and platform
- Security and IAM Challenges
  - Multiple vendors, infrastructure, contractors and unclear ownership for security
  - Inconsistent security frameworks lead to interoperability and trust issues
  - No single method for authentication that meets IoT device security and computational requirements.
  - Current authorization techniques fall short for IoT requirements
  - Authentication and authorization for human interaction not adequate
  - Governance of data and privacy is evolving
  - Newer approaches may not work due to constrained networks.

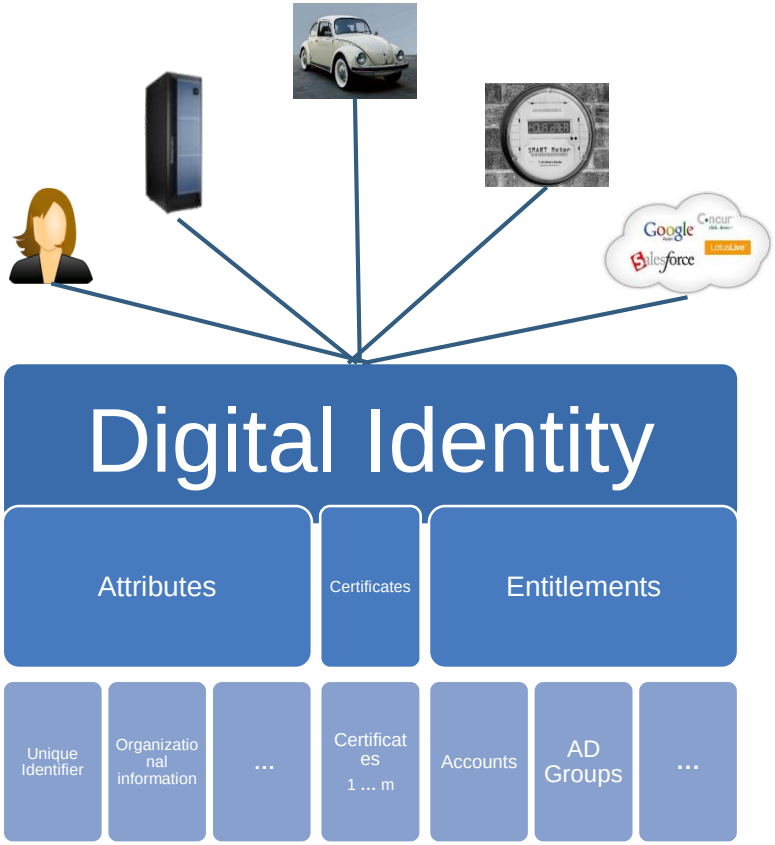


Source: BOMA 2016 Office Experience Exchange Report (Office EER)

Challenges for IAM and Security for IoT

Challenges	
What are things and THINGS and scenarios?	THINGS are composed of other things, e.g. a camera on a phone, a sensor in a car A classification and taxonomy for things and scenarios not generally available
Who owns the thing?	Many and highly dynamic relationships between entities, e.g. one user to multiple devices, one device shared between multiple users; things have relationships to other things and within THINGS
Who owns security and IAM?	Multiple vendors, infrastructure, contractors and unclear ownership for security across a scenario Unclear ownership for security in IoT within one organization Inconsistent security frameworks lead to interoperability and trust issues
What is my Identity?	Digital Identity needed for all entities: humans, servers, things and THINGS across the entire lifecycle
How to build and prove security?	Risk-based security architecture needs to be designed and implemented across the scenario for all entities: humans, servers, things and THINGS, and their lifecycle Certifications for entities need to be set up
How to authenticate and authorize?	Current authorization techniques often fall short for IoT requirements Authentication and authorization for human interaction not adequate No single method for authentication that meets IoT device security and computational requirements, so many different to handle, human/device to device, biometrics, behaviors, API, PKI, …
What else a thing can do?	Cybercriminals can use IoT devices as jumping points to launch attacks
Whom belongs the data?	Privacy issues, although governance of data and privacy is evolving

IAM and the Digital Identity



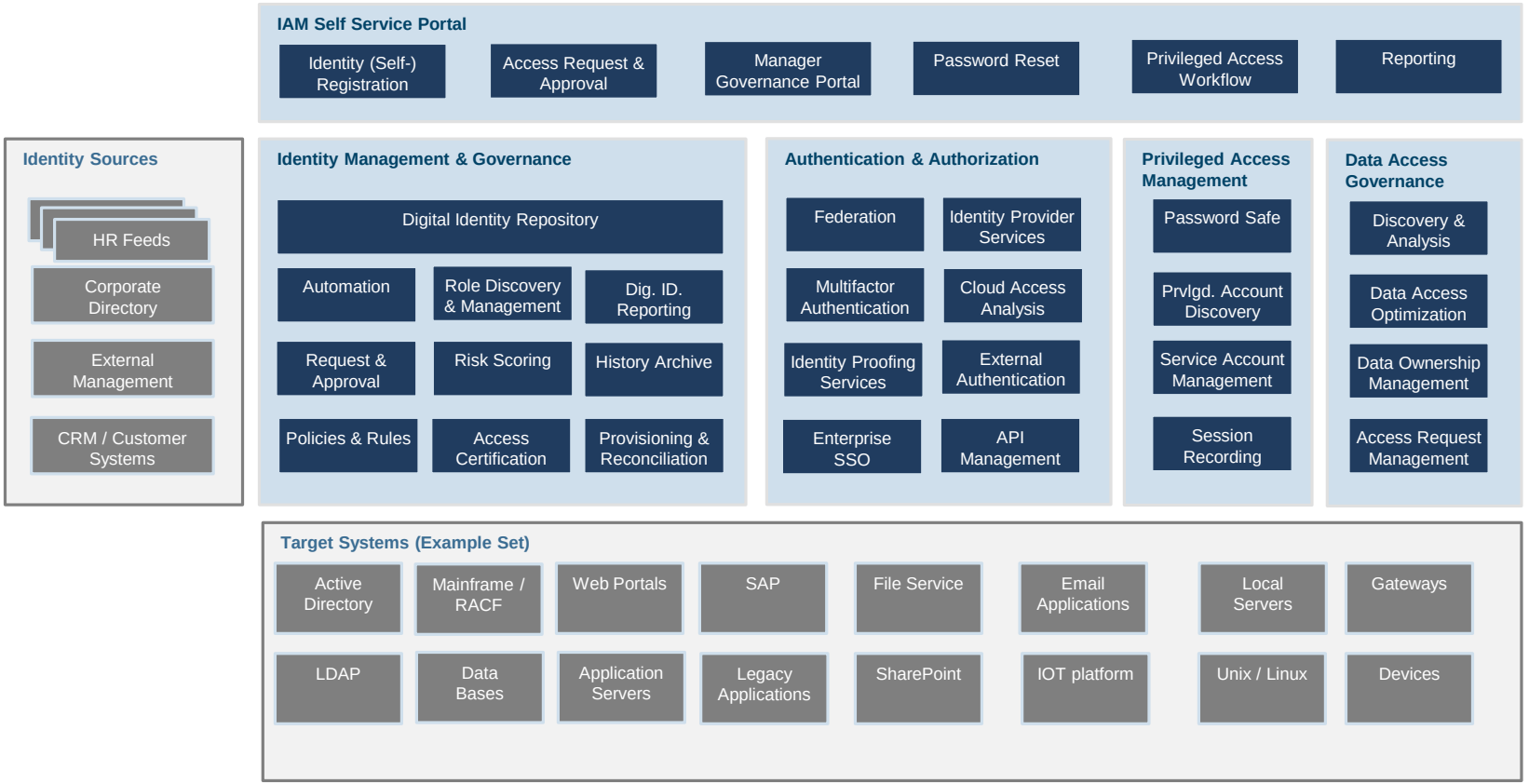
Identity & Access Management

- is a set of **processes** and **technologies** that deals with **who** and **what** has access to **which information** and **resources** over time;
- ensures that the **right Digital Identities** get access to the **right resources** at the **right times** for the **right reasons**, enabling the **right business outcomes**;
- this includes Digital Identities for **individuals**, **devices**, **'things'** and **systems** with their **entitlements** and the **relationships** between them.

A Digital Identity

- is the **representation of all identity and access information** for an individual person, device or system, 'thing' or THING in **an IT environment**,
- comprising of attributes, assigned to that entity, e.g. names, organizational unit to which the identity belongs, unique identifier to reliably connect the Digital Identity with the real world entity,
- assigned entitlements and credentials such as user accounts, certificates, roles and access rights, e.g. Active Directory group memberships, SAP roles, LDAP groups.

IAM Capabilities (extract)



IAM for IoT – How we can use it today

- Get back to the basics: Requirements
  - Establish Identity Assurance Requirements for device classes before setting up an IAM framework for IoT
  - Identity Assurance might vary on the device class, type of application, strength of network, sensitivity of data, criticality of operations and impact of a potential compromise through unauthorized access, and more
- Define an Enterprise Security and IAM Architecture
  - Use a recognized method for an enterprise security and IAM architecture, e.g. SABSA
  - Adopt a graded trust model for IAM capabilities
  - Design authentication & authorization schemes based on risk models
- Establish an appropriate organization
  - Work across the business units
- Integrate IoT implementation into an existing IAM framework
  - Establish an extensible identity lifecycle for all categories of Digital Identities, especially for on-boarding/registration
  - Establish relationship mappings between all categories of Digital Identities
  - Implement more restrictive logic in identity management workflows
  - Integrate IAM with asset management repositories
  - Establish authentication and authorization procedures for local access or when only intermittently connected to the network
  - Implement a privileged user management system to ensure that administrators accessing systems and devices are under control
  - Define privacy protections required for different data categories
  - Integrate with analytics solution

IAM for IoT – some ideas what organizations can do now

- Get back to the basics: Requirements
  - Establish Identity Assurance Requirements for device classes before setting up an IAM fra… for IoT
  - Identity Assurance might vary… type of application, stre… of data, criticality of … potential compromise… access, and more
- Define an Enterprise Se… Architecture
  - Use a recognized method fo… and IAM architecture, e.g. SA…
  - Adopt a graded trust model for…
  - Design authentication & authoriz… based on risk models
- Establish an appropriate organization
  - Work across the business units

Taxonomy, Standardization and (industry-based) IAM frameworks are needed!

- …T implementation into an existing …rk
  - …xtensible identity lifecycle for all …igital Identities, especially for on-…tion
  - …hip mappings between all …l Identities
  - …rictive logic in identity …ys
  - …set management repositories
  - …entication and authorization …res for local access or when only …ittermittently connected to the network
  - Implement a privileged user management system to ensure that administrators accessing systems and devices are under control
  - Define privacy protections required for different data categories
  - Integrate with analytics solution

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM