Gaps in Government Funded Identity Research

This document presents an analysis of three Community Conversations conducted to collect identity problem / solution stories from subject matter experts. The objective was to identify and understand gaps between current government funding initiatives and unfunded needs. The stories are categorized according to Stakeholder Needs and placement in the Digital Identity Model. The results were compared against the funded portfolio projects to identify gaps in the funded portfolio.

The Data & Process

A series of three Community Conversations explored problems of digital identity in the context of participant stories; identifying problems and asking them to envision solutions to their self-identified problem areas. Data was collected in "story" form, a technique designed to yield rich results describing both problems and solutions. Each group was asked the following two questions:

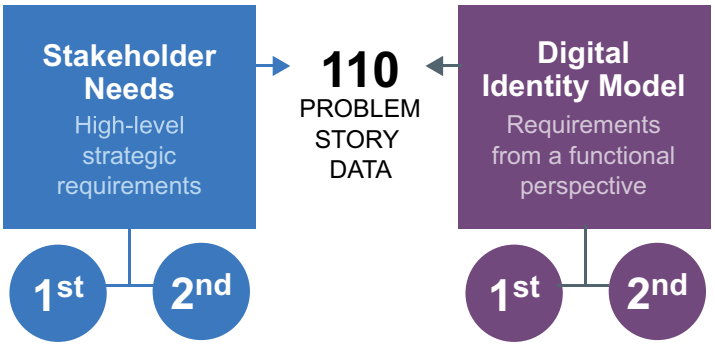
"What is missing in your industry when it comes to solving identity and privacy problems?"

"What do you want to do for your customers, constituencies, business partners, and employees that you can't do today because of this lack?"

Participants identified more than 100 identity problems and brainstormed possible solutions. These results have been categorized within Stakeholder Needs and the Digital Identity Model to discover and illuminate gaps in portfolio funding.

Analysis Overview

DHS uses two categories for understanding identity requirements and funded portfolio projects. Stakeholder Needs are high-level strategic requirements, while the Digital Identity Model looks at requirements from a functional perspective.



The data is categorized into primary and secondary areas of both Stakeholder Needs and Digital Identity Model, resulting in dual data analysis.

COMMUNITY CONVERSATION

1	2	3
04/25/2016 Mountain View, CA	03/24/2017 Laurel, MD	06/09/2017 Chicago, IL
~50 people across 7 industries	10 people in 2 groups	16 people in 4 groups 1 story per person
Identified 113 situations with 60 unique problems	Identified 35 stories	Identified 13 stories

Gaps in Stakeholder Needs

This analysis compares Stakeholder Needs categorized data to DHS funded projects. The delta identifies capability gaps between funded projects and desired features.

GAPS

Sign-In

Sign-in is primarily invested in via mobile portfolio projects; however there were multiple concerns raised with sign-in needs for smart devices, connected vehicles and other non-human account holders.

Data Regulation

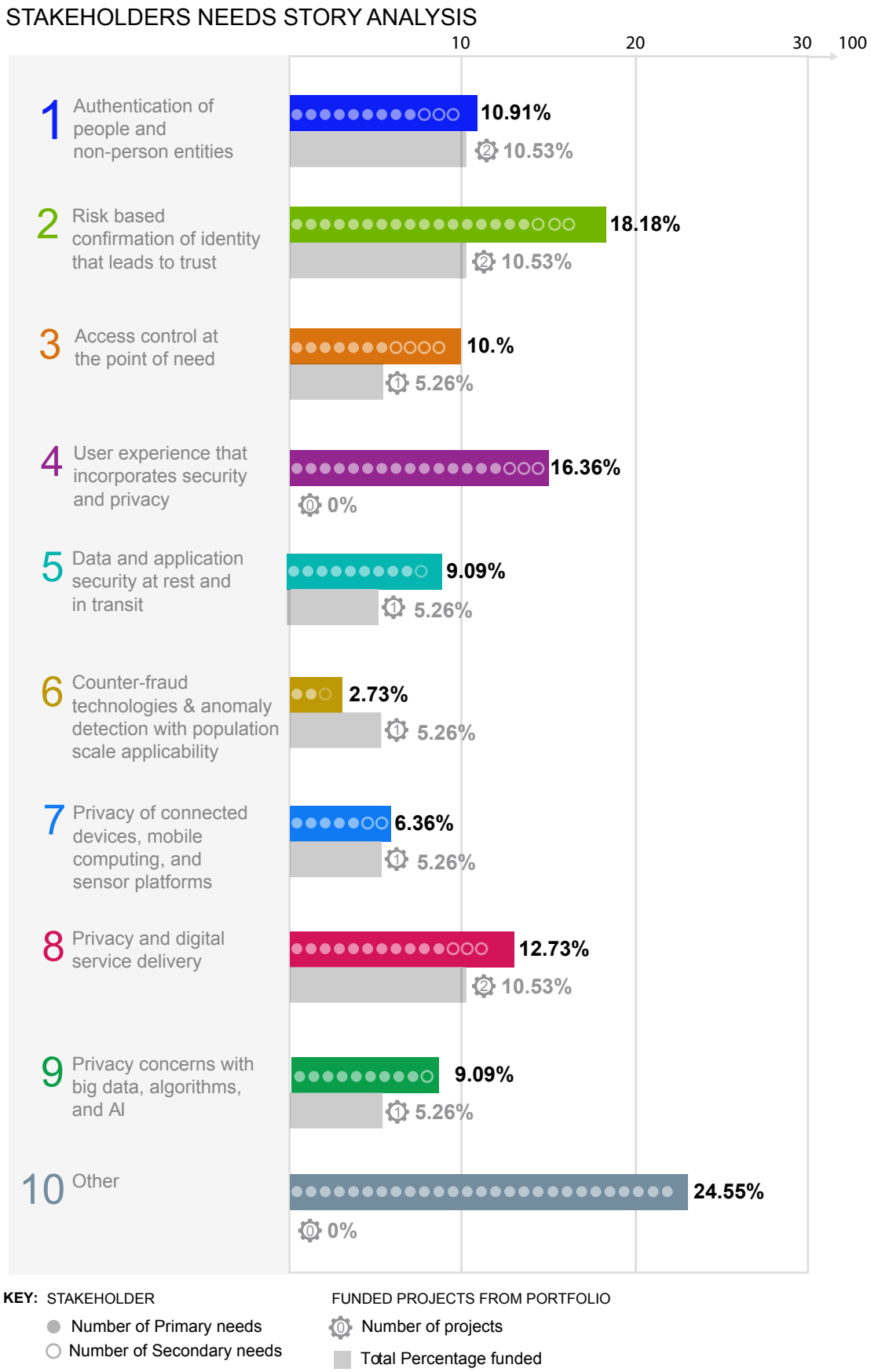
Data regulation is inconsistent, with some data regulated (HIPPA and COPPA), but much more collected without regulatory oversight. Data is under increasing attack by state run actors, hackers and blackhats. Governments are not able to keep up with the pace of technological change and be pro-active. In addition, data laws are dissimilar in US states and around the world.

Delegated Accounts

Delegated accounts are the ability to give others access to your account to do things on your behalf or to access to your data. Delegation situations include an individual person accessing multiple accounts as well as multiple people accessing multiple accounts.

New Areas for Identity

Several new technologies were identified as critical for new identity models. These include virtual reality (VR), augmented reality (AR), IOT smart devices, and using blockchain technology as an identity platform. Three infrastructure projects explore blockchain as a technology innovation and this is exactly the kind of research that should be funded.



Gaps in Digital Identity Model

This analysis compares Digital Identity Model categorized data to funded projects. The delta identifies gaps between funded projects and desired features.

GAPS

Data Security and Interoperability

Data is collected, shared and utilized by different entities in multiple industries using disparate collection and security methods. This causes interoperability issues between industry "silos." This problem fits into the Consent and Authorization categories, an area that did not have any DHS funded projects, with one exception in the Mobile area.

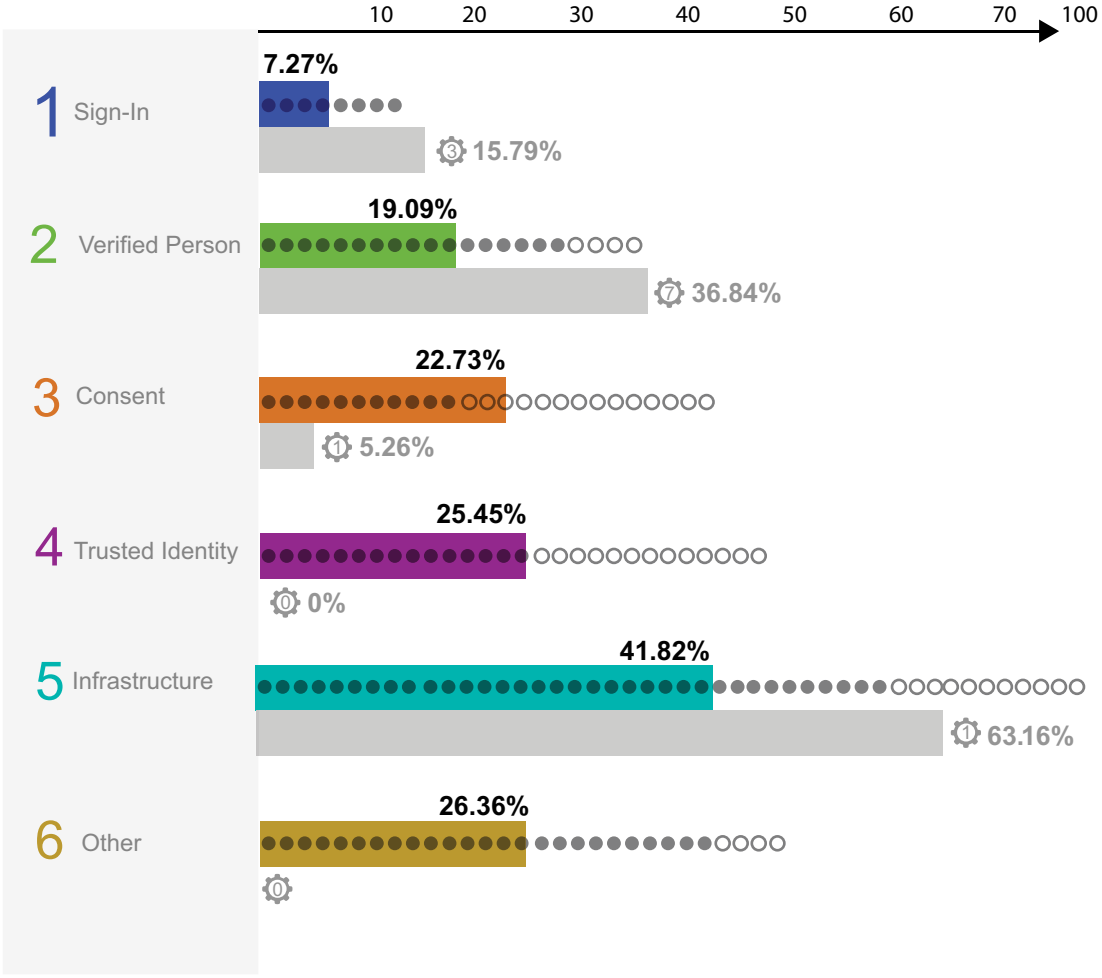
User Experience

Lack of good user experience around identity and security was raised across many verticals, yet no portfolio projects addresses this problem. While companies say the security and usability are of equal importance, when it comes to brass tacks, companies prioritize technology over user experience. Unfortunately this leads to security issues due to unsecure user behavior due to lack of usability.

Market Driven Technology

There was an understanding among participants that there is not enough technology available to solve their identity problems. This impression may be due to market solutions focused on specific problems within specific industries, rather than general problem solving for a broader application cross-industry. The market driven approach to technology development does not support an attitude to develop identity technology that can be utilized across industries.

DIGITAL IDENTITY STORY ANALYSIS



KEY: DIGITAL IDENTITY MODEL

- Number of Primary needs
- Number of Secondary needs

FUNDED PROJECTS FROM PORTFOLIO

- Number of projects
- Total Percentage funded

> "We need to understand where the rest of the world is heading and solve those problems, or we're always behind and always reacting."
>
> *–Participant*

Determine New Critical Capabilities

Based on the gap between funded projects and desired features, the following project areas are recommended to identify new capabilities.

Delegation

Delegated accounts delegate authority for access to an account or account data on the account holder's behalf. There are many medical, education and government situations wherein this is important. This is a problem that will increase in importance as digital agents are used on behalf of human and intelligent objects.

Problem: *What are the delegation situations in the 16 critical infrastructure sectors for human/cyber entities? How do we permission an account to access the account holders data/account actions without giving away the token to access the account?*

User Experience

We continue to see problems with the lack of education around digital identity. Exacerbating the problem are the many definitions of identity that will continue to be complicated as we add non-human identity paradigms (vehicles, IOT, digital agents). Security suffers when security measures don't consider human limitations.

Problem: *What are the security methods that consider human factors to ensure security while maintaining the effectiveness of the security method?*

Digital Only Accounts

There are an increasing number of smart objects, connected vehicles and digital agents that have unique identity and security needs. These cyber entities will interact on behalf of humans and collect data about human and non-human activities. Our current identity paradigms are inadequate and originate from an insufficient human centric identity perspective. Without considering new identity paradigms, governments will be in an even worse position to respond to the effects of new technology.

Problem: *What are the new identity paradigms for cyber entities and how do they support or extend current identity examples?*

The Future of Digital Identity

Through the course of the conversations, multiple participants communicated a desire to look at identity through a new framing. What could an integrated identity model – that takes current and near future requirements for human and cyber entities – look like?

Problem: *What is the future of digital identity for humans and cyber entities, in 2020, 2050 and beyond?*

In 2011 & 2012, SWIFT spearheaded the Digital Asset Grid (DAG) R&D project, that explored some aspects of this question. This work can be synthetized and expanded with current and near future trends. Two participants of the DAG project worked on this report.

Identifying New Capabilities

We recommend exploring these four areas to identify and detail new capabilities.

STEP 1.

Document Emerging Concepts: Research and document the projected impact of emerging technology on digital identity, security and privacy in the context of the four areas.

STEP 2.

Create Narratives: Create narrative use cases that detail how future technologies might be used and their second and third order impacts as well as how the government can proactively consider regulatory and policy impacts.

STEP 3.

Identify Critical Capabilities: What are the technology capabilities needed to address the four topic areas? Which ones can be satisfied with current or emerging technology (e.g. blockchain) and which ones require new innovations creating new capabilities?

Information in this report is based on research funded by the U.S. Department of Homeland Security Science & Technology Directorate (DHS S&T). Any opinions contained herein are those of the performer and do not necessarily reflect those of DHS S&T

APPENDIX I: Stakeholder Needs Detail

Over 100 problem / solution stories were collected from the three Community Conversations.These were categorized into the following Stakeholder Needs. Some items are in multiple categories due to primary and secondary categorizations.

1

Authentication

Account access

Authentication has matured from basic system accounts to complex system accounts using various security technologies. Each system may have different security rules. Some standards exist, but they may not meet all the market needs. This can create a nightmare for the individuals attempting to successfully leverage all aspects of security technology.

- Tension between the cost of security and usability. Companies tend to sacrifice usability for security technology, but in sacrificing usability, users sabotage the security.
- Remote access: securely connecting to a remote vehicle or device. Can a device authenticate for you?
- Need for continuous authentication or one-time authentication.
- Misunderstanding between your account and your identity.
- Expense of two-factor and multi-factor authentication due to human factors (lost hardware, personnel changes).
- Hacking concerns of password, biometrics, IOT smart objects.

2

Identity Confirmation

How do we know you are who you say you are?

For many activities, individuals need to legally prove who they say they are. In the past this was done through in-person meetings with legally acceptable documentation. The demand to conduct confirmations digitally raises a number of concerns.

- Which confirmation method is used: Password, biometric, fob, other?
- Secure systems are accessed various ways: internal, mobile, BYO access, federated identity?
- What legal proof is required? Is it a one-time requirement or ongoing confirmation?
- The impression of increased security introduces new vulnerabilities caused by users' risky behavior. For example, a fob may be seen as more secure, which might cause users to increase risky behavior.
- Incorrect use of data, even in an aggregate, use can disclose PII.
- The ability to give others allowed access to your account or data to do things on your behalf, e.g. delegation.

3

Access Controls

Gaining access to a system, sometimes from another system

We have more interconnected systems today than before. People and devices need to access multiple systems using various authentication methods. Accounts can request access on a multitude of IOT platforms in addition to human users accessing other human user systems.

- Mobile access controls for single sign on and custom tech stacks.
- Provisioning and deprovisioning enterprise IDs on multiple systems with multiple access controls when staff is hired, changes roles or leaves.
- Complex government IDs are comprised of combination of a classified account details and civilian details.
- BYO Access (traveling or working at home) and the impact to sensitive corporate data.
- The increased security threat to sites, platforms, and systems that aggregate passwords and system data.
- Password/token/cards used to authenticate remote access to other systems (IOT devices, connected vehicles).
- The ability to give others (human accounts, IOT devices, etc.) access to your account or data to do things on your behalf, or to access data for a delegated account (parent/minor for education or grown child/older parent for financial/health).

4

User experience

Human-centric security paradigms

Technical solutions do not always consider human behaviors or misunderstanding of account systems and identity.

- Definitions of identity are fluid and change depending on the user.
- General education and best practices are not well documented and disseminated to end users.
- Provisioning and deprovisioning enterprise IDs on multiple systems with multiple access controls when staff is hired, changes roles or leaves.
- Complex government IDs are comprised of combination of classified account details and civilian details (e.g. your personal ID is tied to iPhone).
- Delegated accounts: the ability to give others (human accounts, IOT devices, etc.) access to your account or data to do things on your behalf, or to access data for a delegated account.

> "You need to use your identity for access, which exposes it, makes it vulnerable." *–Participant*

5

Data and Application Security

Securing the system, data in the system, system software, hardware, and protocols

- Trusted computing (TPM). Using a third party Privacy Certification Authority (PCA) to insure a system is a "secure."
- System resilience after hacks and phishing attacks to minimize damage once access has been gained or data has been compromised.
- Communication protocols that encrypt data.
- IOT devices communicating with each other.

6

Fraud

Unauthorized access to systems

Fraud is one of the Internet's most lucrative and aggressively evolving business models.

- ID verification (e.g. KYC) via online video and mobile devices when opening accounts, after an identity theft event.
- Long term security concerns using biometric security methods.
- Authentication fraud with stolen credentials.

7

Privacy of connected devices/platform

Device privacy

Smart objects have a different set of requirements for account creation, data privacy, and security. They are an increasing target for hacking and breeches.

- IOT objects are often groups and some are connected in a peer-to-peer manner while others are hierarchal.
- Unclear how regulations apply to IOT collected data.
- IOT objects are an increasing attack vector.

8

Privacy with sharing delivery

Privacy and consent of shared data

One of the largest concerns is how data is shared. Who gives consent to share the data and how this consent is revoked or otherwise managed.

- Concerns about how data is used and how networks access your data.
- Ensuring trust between multiple entities.
- Delegated accounts: the ability to give others (human accounts, IOT devices, etc.) access to your account or data (medical, school, non-profit, government, criminal, investigation related) to do things on your behalf, or to access data for a delegated account.
- Challenges matching IDs for data sharing: matching an ID across platforms, authentication of the ID across platforms, dealing with siloed IDs, dealing with composite IDs and dealing with delegated IDs (accounts being accessed by someone other than the primary account holder).
- Regulations for sharing data, especially with data collected from IOT objects.

9

Privacy in regards to Big Data, AI, and Algorithms

Data that is analyzed by machine learning, and how it is used

Most people don't understand the depth of the data collected on them or the scope on which that data is shared, sold and otherwise used. There are concerns about what data is collected and how it is used.

- Batch data is not as anonymous as it has been in the past. Identity can be determined with minimal anonymous data points. This is especially important in the context of increased data breeches and reduced system security.
- Consumer fear about how data is collected and used by others. There is little to no transparency from companies on how data is gathered and used or sold. Often the data collected is not easily available to the user, or in usable format.
- Education about data use is complicated because everyone does it differently.
- Consumer corporations drive the innovation, while the government is in the role of responding to the market. A proactive government approach is impossible.
- Regulation is inconsistent across marketplace verticals: HIPPA, COPPA, parent/student educational needs.
- Delegated accounts: the ability to give others (human accounts, IOT devices, etc.) access to your account or data (medical, school, non-profit, government, criminal, investigation related) to do things on your behalf, or to access data for a delegated account.

10

Other

Results that didn't fit into the other buckets

Problem stories outside the nine main categories.

- Identity concerns in new medias: VR, AR, IOT.
- User demand for harmonization for seamless experience through multiple access points and platforms.
- People have multiple identities that are multi-faceted–this is not always reflected in current technology solutions.
- Identity is a HARD problem to solve with many "moving parts."
- What are legacy application requirements for interoperability with new technology?
- Standards and regulations vary in different environments and locals, for example international standardization efforts and the different laws in the EU vs US.
- Needs to be better clarification about public-private data sharing partnerships.

APPENDIX II: Digital Identity Model Detail

Over 100 problem / solution stories were collected from the three Community Conversations.These were categorized into the following Digital Identity Model. Some items are found in multiple categories due to primary and secondary categorizations.

1

Sign-In

These results were consistent across both Stakeholder Needs and Digital Identity Model sign-in categorizations.

- User experience that facilitates security best practices vs going around security due to poor usability.
- The legal needs of deploying technology in rigorous corporate environment.
- Non-humans authenticating for account access.
- Security concerns with 2FA.

2

Verified Person

Verification and Validation

How the identity of an account or individual is verified. These stories fell across a variety of Stakeholder Needs areas.

- Security concerns when verifying account holders using passwords, 2FA, security fobs, and/or encryption.
- Dealing with composite identities and corporate permissioning: giving and revoking account access due to being hired, changing roles or leaving.
- Verifying device access: phone, IOT, vehicle.
- Using data without explicit consent for “personalized” experiences.
- Using anonymous/classified information to gain access to classified areas.

3

Consent and Authorization

Most of these stories were in the service delivery and data privacy sections of Stakeholder Needs.

- Sharing data securely among systems, for delegated accounts and across various data silos (medical, educational, IOT, children, government).
- General concerns with how data is shared: lack of transparency.
- Specific concern with data collected and shared from IOT objects.

4

Trusted Digital Identities

Improving the user experience for users of an identity system as well as corporate roles that implement enterprise identity technology.

- Identity is complex. An account is for user access, while an identity is a complex concept, especially in regards to data sharing and delegated accounts.
- There are new issues for non-human identities.
- There are tradeoffs between security technology, best practices, and usability. There is limited education, understanding and conflicting information.
- There are challenges implementing identity technology in enterprise environments.

> “If it’s not about secrets, then it’s about behavior and actions. Behavior is what dictates your authorization to act.”

5

Infrastructure

The largest number of stories ended up in this category because many of the problems encompass security, privacy, fraud and cross-system functionality.

- Sharing data, including sharing with delegated accounts.
- Concerns with identity theft, fraud, and other security vulnerabilities. Future attacks may include false attribution, spoofing identity, and false tax returns.
- The more devices that access identity systems equal more vulnerabilities and attack vectors.
- Concerns with system security including: BYO access to corporate networks; authentication methods (2FA, fobs, biometrics, passwords, etc.); single sign on using federated identity; KYC identity proving; human vs non-human identities; and enterprise identity systems.
- Concerns with privacy due to user illiteracy, differences between EU and US laws, and breeches of private data.

6

Other

Stories that did not fit into other areas of the Digital Identity Model.

- Delegation situations with an individual person accessing multiple accounts and multiple people accessing multiple accounts.
- Developing appropriate law and policy for digital identity.
- Public/Private partnerships between the government and private companies.
- Verified Claims and how they should work with digital identity.