MITRE ENGENUITY

CYBER RISK MODEL FOR MOBILE FINANCIAL SERVICES

Bringing the best of MITRE to private sector to create generational impact for our national and economic security

May 2022

MITRE ENGENUITY™

Improving Cybersecurity | Mobile Digital Financial Services

Focus: People in developing countries increasingly use mobile devices to store, transfer, and save money.

Secure access to money is essential for individuals to achieve political stability, gender equity, and economic advancement.

Investing in security solutions requires a decision tool (**risk model**) that accounts for hundreds of ecosystem components that create risks to people, hardware, and software.

MITRE ENGENUITY

Background | What is a risk model?

Identify the risk	When system components (people and things) interact, even benign interaction creates risk to the system's integrity. More than one system creates a system-of-systems. A risk model helps understand system-of-systems security.
Model the risk	A risk model is a decision framework that analyzes how system actors and components, or multiple dependent systems, interact and create cybersecurity risks, and what can be done to protect the ecosystem.
Apply the model	The model enables a user to identify and isolate relevant system components (people and things), which then highlights likely system risks, and what solutions the user should be invest in to reduce system risk.

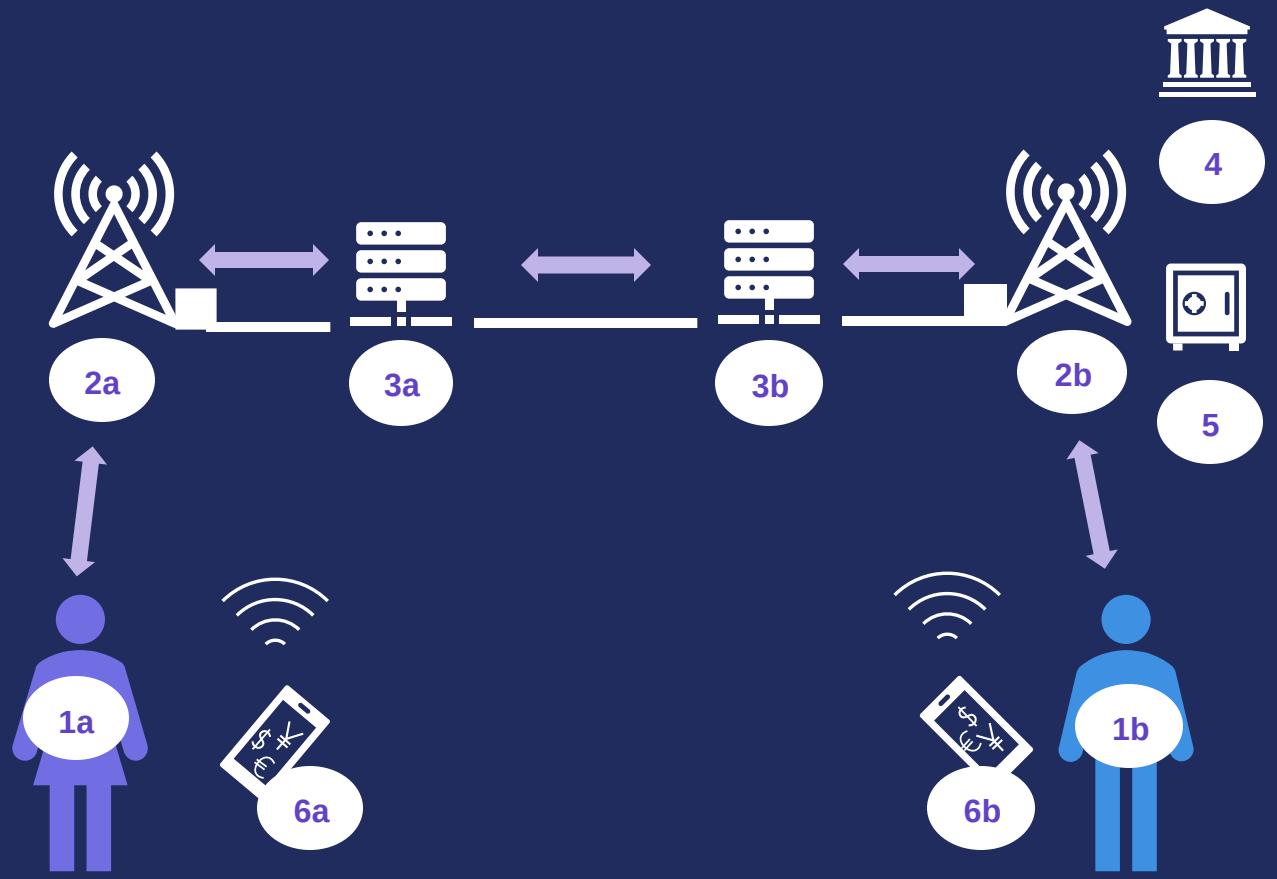
MITRE ENGENUITY

Mobile Digital Financial Services Ecosystem

Modern money transfer involves a complex, non-linear movement of information in an ecosystem. Each part and associated technology create risk of attack to the transfer's integrity.

Many potential actors participate:
(1) users,
(2) wireless companies,
(3) internet service providers,
(4) government agencies;
(5) banks; and
(6) mobile hardware/software developers.

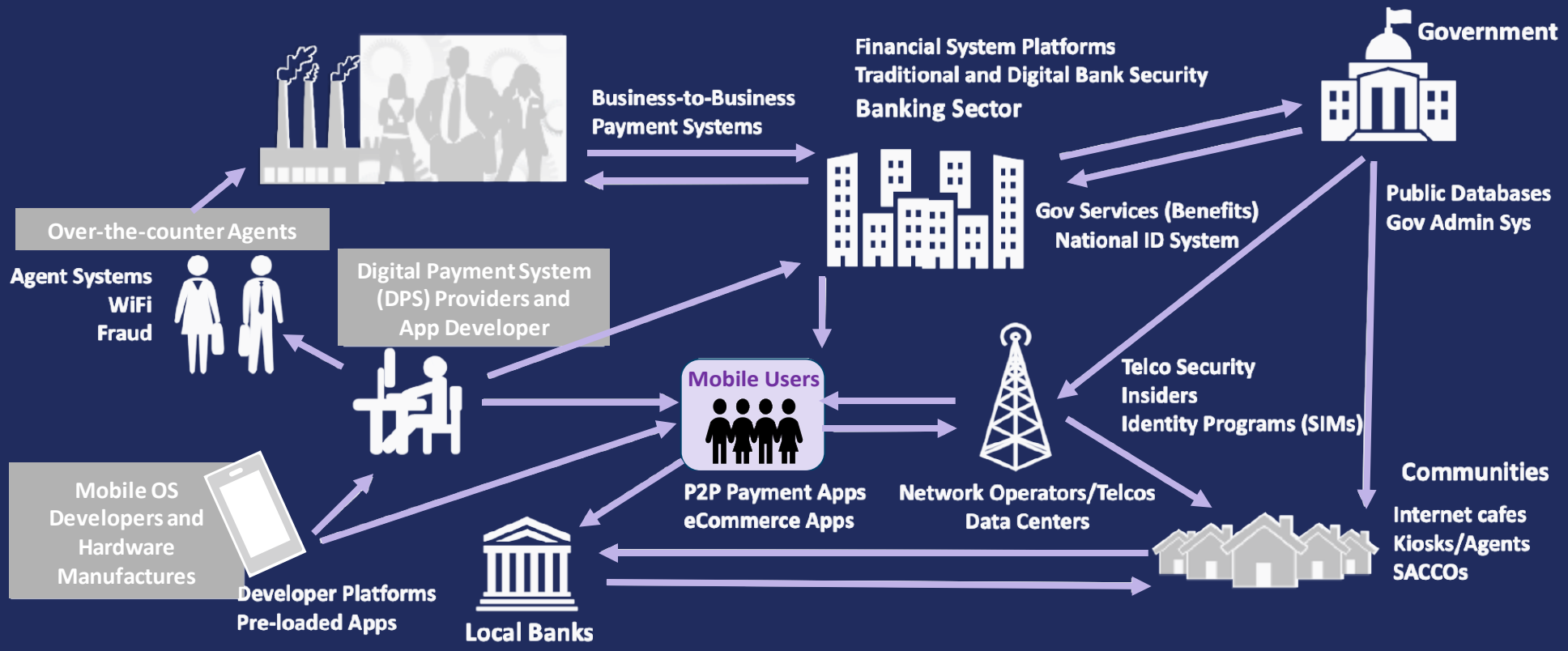
This is a simple illustration. The next slide shows the complete system of systems involved in mobile money transfer.



MITRE ENGENUITY

mDFS Money Transfer | Complete Picture

Key Takeaway: The mDFS ecosystem is extremely complex. Each actor participates and manages technology differently, which creates risk of attack to money transfer's integrity. Understanding the "system of systems" risks requires this complete picture.



MITRE ENGENUITY

Engenuity Cyber Risk Model | Two-Lens Approach

Like 3D glasses, the complete picture of the mobile digital financial service security still is not clear unless viewed through two lenses.

Understanding how hardware and software interact, how adversaries can attack (vectors), and what improvements can stop attacks (mitigants).

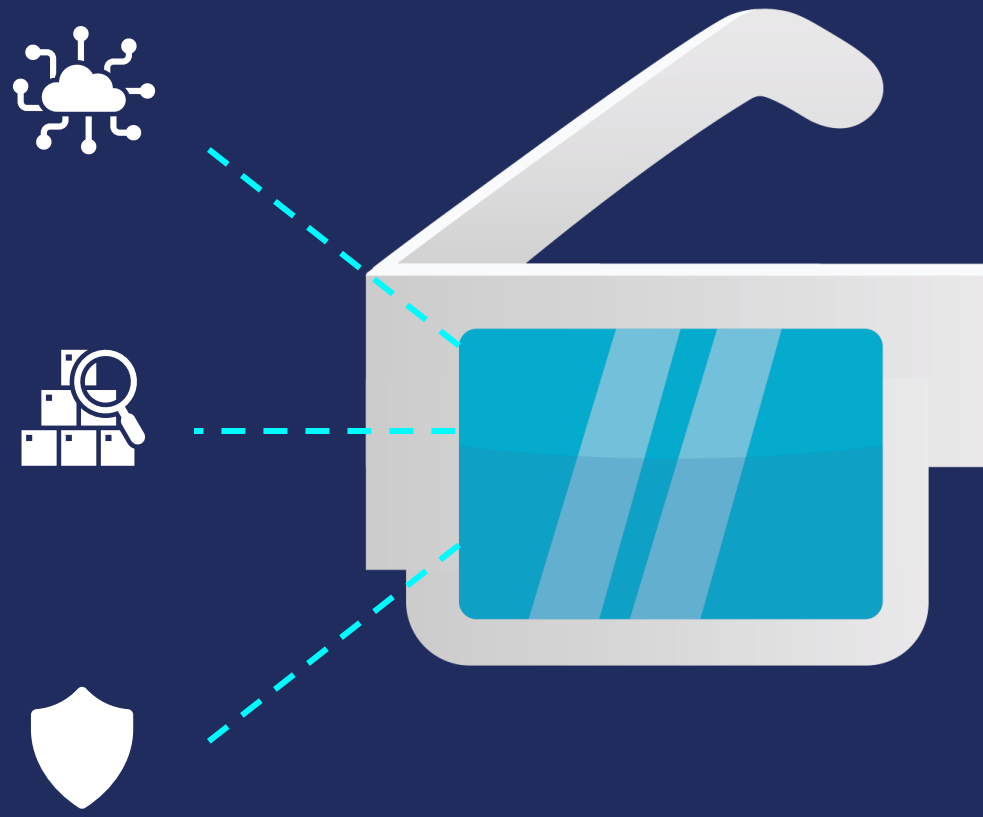
Understanding how policies, laws, governance, and education affect people's interactions with technology and can strengthen access to mobile money.

MITRE ENGENUITY

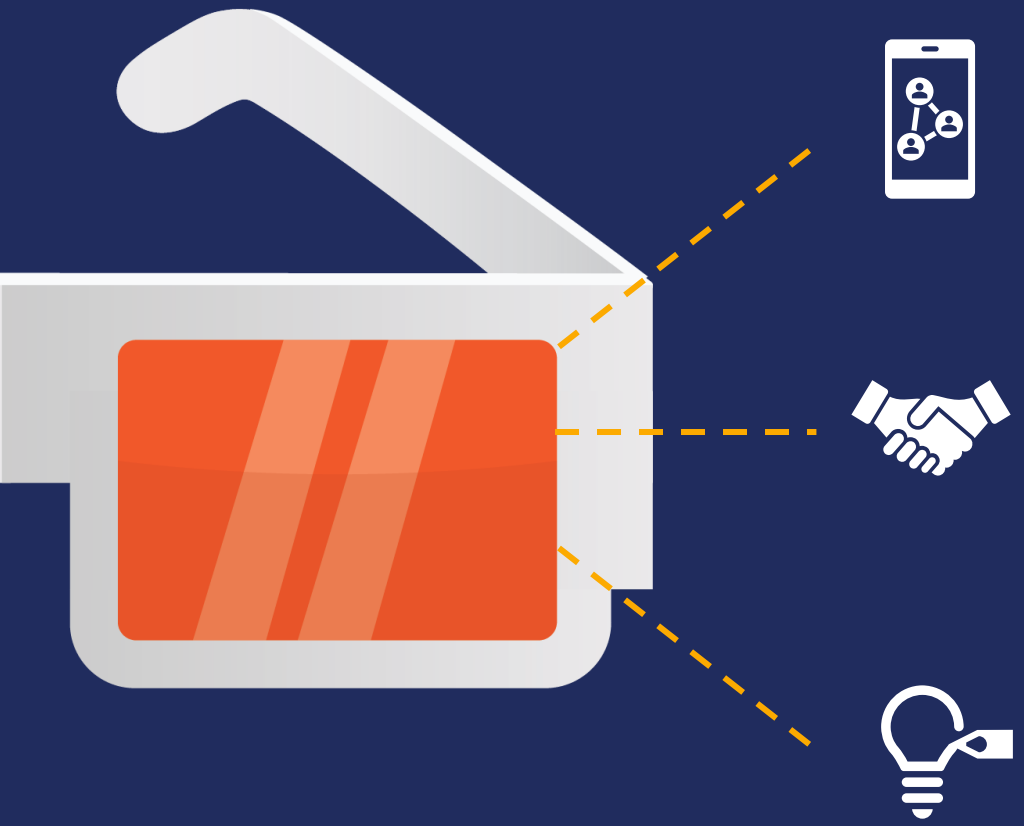
Engenuity Cyber Risk Model
Technical Lens

The technical lens focuses on three concepts.

- Identifying hardware/software that enable mobile money from transfer to receipt, given technology maturity and use.
- Identifying vulnerabilities in ecosystem hardware and software, grouping them by methods of attack (threat vectors) and common “planes” that enable vectors (threat domains).
- Recommending techniques to lower the risk of attack given specific hardware and software combinations used to transfer money.



MITRE ENGENUITY



Engenuity Cyber Risk Model
Non-Technical Lens

The non-technical lens focuses on three concepts.

- Identifying the mobile users' access to network services, e.g., easy and reliable versus difficult and unreliable.
- Identifying the best stakeholder to implement non-technical solutions in a country or region, e.g., banks, private industry, or government.
- Recommending the best opportunities (laws, training, and policies) that strengthen people's access to and reliance on secure mobile money systems.

MITRE ENGENUITY

Apply the Cyber Risk Model | Inputs

Step 1 **What hardware and software does a country or region use for people to transfer money on mobile networks?**

- Are phones and networks on 3G versus 5G?
- Do people transfer money via bank apps (mobile wallets) or non-bank apps?

Step 2 **What is network access like, and who is in the best place to help implement non-technical solutions?**

- Is network access difficult or easy? Dependable? Trustworthy?
- What organizations are in the best place to implement recommended non-technical solutions, e.g., technology standards, gender inclusion, or regulation?

MITRE ENGENUITY

Apply the mDFS Cyber Risk Model | Output

Based on all responses to model input questions, the threat model identifies most likely technical threats, and technical mitigations and non-technical opportunities to increase entire mDFS ecosystem security.

- State-of-the-art technical and non-technical recommendations guide security investment decisions for improving risk reduction, based upon a country's unique mobile network and political posture.

- Users can modify inputs to see recommended changes based on mobile money technology and political landscape of a given country or region. Tactical, operational, and strategic perspectives can benefit from the model.

***Stay tuned for launch of open-source prototype software tool to use mDFS cyber risk model.**

MITRE ENGENUITY

THANK YOU

CYBER RISK MODEL FOR MOBILE FINANCIAL SERVICES