

MITRE ENGENUITY TECHNICAL REPORT

MITRE Engenuity Report

Securing the Mobile Money Ecosystem: Dynamic Cyber Risk Model for Improving Secure Access to Mobile Digital Financial Services

July 2022

The views, opinions, and/or findings contained in this report are those of MITRE Engenuity, LLC and should not be construed as an official position, policy, or decision, unless designated by other documentation.

©2022 MITRE Engenuity, LLC.
All rights reserved. Approved for public release.
Document number ME0044

Table of Contents

1	Project Purpose and Goals	1-6
1.1	Cyber Risk Frameworks and Technical Trends	1-6
1.2	International Technical Strategy, Policy, and Governance	1-7
1.3	Technical Risk and Policy/Governance Opportunities Synthesis	1-8
2	Background	2-1
2.1	From Mobile Phones to Mobile Money	2-3
2.2	Mobile Agents	2-6
2.3	Digital Currencies	2-8
2.4	The Complex mDFS Risk Landscape	2-11
2.5	The Impact of Cybercrime	2-12
3	Challenge Description	3-1
3.1	Actors and Factors	3-4
4	Target mDFS Use Cases	4-1
4.1	Cash In/Cash Out	4-1
4.2	Remittances	4-1
4.3	Utilities/Pay as You Go	4-1
4.4	Payments for Goods/Services	4-2
4.5	Person-to-Person (P2P)	4-2
4.6	Business-to-Person (B2P)	4-2
4.7	Government-to-Person (G2P)	4-2
5	Research Observations	5-1
5.1	Characteristics of Prominent Mobile Money Models	5-1
5.2	The Role of Telcos	5-2
5.3	The Role of Government	5-2
5.4	The Role of Regional Organizations	5-4
5.5	The Role of Cybersecurity Experts and App Developers	5-4
6	Model Development Methodology	6-1
6.1	Assumptions	6-1
6.2	MITRE Engenuity’s System-of-Systems Approach	6-2
6.3	mDFS Risk Model Development	6-3

6.3.1	Threat Identification and Mitigation (Technical Ecosystem).....	6-7
6.3.2	Non-Technical Ecosystem Factors	6-15
6.3.3	Combining the Technical and Non-Technical Lenses.....	6-18
7	Framework Validation and Key Stakeholder Interviews	7-19
8	Recommendations for Stakeholder Engagement	8-20
9	General Recommendations for Improving National mDFS Ecosystem Access and Security	9-21
9.1.1	Improving Cybersecurity of mDFS	9-21
9.1.2	Improving mDFS Usage through Trust	9-22
10	Recommendations for Stakeholder Program Planning to Improve mDFS Security and Access.....	10-23
10.1	Regulation, Compliance, and Reporting	10-24
10.2	Customer Identity and Privacy	10-25
10.3	Technical and Policy Controls to Protect Transactions.....	10-26
10.4	Securing Financial Service Providers.....	10-27
10.5	Investing in the Workforce	10-28
10.6	Regional Solutions.....	10-28
11	Open-Source Cyber Risk Model Tool	11-29
12	Avenues for Future Research.....	12-1
13	Conclusion.....	13-1
14	References	14-1

List of Figures

Figure 1: Mobile Device Ownership in Africa	2-2
Figure 2: Growth of Mobile Money	2-3
Figure 3: The Many Mobile Money Providers of Africa	2-5
Figure 4: The Costs of Cybercrime	3-1
Figure 5: Notional mDFS Ecosystem	3-1
Figure 6: Customer, Network Provider, and Operational Domains	3-2
Figure 7: Intersections of DFS Stakeholders (Actors) with DFS Security Categories (Factors)	3-4
Figure 8: Snapshot of "Actors and Factors" Evaluated in Developing the Engenuity mDFS Risk Model.....	6-2
Figure 9: HSEDI Financial Services Threat Model	6-3
Figure 10: AT&CK for Mobile Threat Model.....	6-3
Figure 11: MITRE's International Cyber Capacity Building Model	6-4
Figure 12: Model Fusion Process Flow	6-5
Figure 13: MITRE's International Cyber Security Framework Development Approach.....	6-5
Figure 14: mDFS Threat Map	6-7
Figure 15: Snapshot of Threat Model on Which the Simplified Visual Representation Is Based	6-9
Figure 16: Process for Developing the Compound and Extended mDFS Threat Model	6-11
Figure 17: Example of Threats, Filtered by Domain.....	6-12
Figure 18: Notional Mapping of Countries against Technical Ecosystem Contextual Factors.....	6-13
Figure 19: Using the Country Mapping to Identify Proximate Threats	6-14
Figure 20: Policy and Governance Opportunities Mapped against National Context	6-15
Figure 21: Filtering Non-Technical Factors by Policy Domain	6-16
Figure 22: Mapping Countries by Policy/Governance Characteristics	6-17
Figure 23: Combining the Technical and Policy/Governance Lenses to Identify Countries' mDFS Risk Mitigation Opportunity Space.....	6-18
Figure 24: GSMA Mobile Money Certification Principles	10-23
Figure 25: GSMA Mobile Money Regulatory Index Showing Degrees to Which Countries' Regulatory Frameworks Support Mobile Money Development	10-25
Figure 26: Cybersecurity Gaps in Africa (Serianu).....	10-28

This page intentionally left blank

Abstract

The explosive growth in mobile digital financial services (mDFS) technologies in emerging markets and developing economies, along with an ever-expanding array of attack methodologies aimed at stealing or compromising financial and personal data, a variety of governance and policy approaches, and continuing challenges in equitable access to both broadband internet and banking-related services, is resulting in significant variations in individuals' and businesses' ability to securely access those services. At the same time, the dynamism and variability in this sector complicates decisions by governments, non-governmental organizations (NGOs), the international development community, and other potential investors about how and where to focus money and effort in improving mDFS security and accessibility, and in expanding banking services to underserved communities. MITRE Engenuity, a 501(c) (3) affiliate of the MITRE Corporation,ⁱ built a comprehensive risk management framework that identifies appropriate leverage points for reducing risk, improving access, and establishing trust within the context of each country's unique technology and policy environment. The team pursued a unique approach to this problem, utilizing its deep expertise across both technical and policy disciplines to combine several cyber threat models with the methodology behind MITRE's internationally recognized national cyber capacity building framework. In this approach, we examine the intersection of local technology contexts—what levels and kinds of connectivity, devices, and applications are in use in a particular country—with non-technical factors like national policy and governance to identify the predominant barriers to access and threats to secure financial transactions, in order to identify the range of effective actions countries, NGOs, and other stakeholders may take to improve secure access to mobile digital financial services in emerging economies. This research will benefit organizations seeking to quickly identify cyber-defensive gaps, manage long-term strategic cyber-risks, and prioritize security investments or resources.

ⁱ MITRE Engenuity received gracious financial support for this project from the Bill and Melinda Gates Foundation.

Executive Summary

Overview and Key Findings

The explosive growth in mobile digital financial services (mDFS) technologies in emerging markets and developing economies, along with the ever-expanding array of attack methodologies aimed at stealing or compromising financial and personal data, and continuing challenges in equitable access to both broadband internet and banking-related services, results in significant variations in the ability of both individuals and businesses to securely access mDFS. These issues are often exacerbated in markets in the early stages of digital development, where cybersecurity risk awareness and cyber protections typically lag demand for digital financial services. Moreover, the dynamism and variability in this sector complicates decisions by governments, non-governmental organizations (NGOs), the international development community, and other potential investors about how and where to focus money and effort in improving mDFS security and accessibility, and in expanding banking services to underserved communities. In short, mDFS play a vital role in helping developing economies bring people out of poverty, but with the proliferation of mDFS comes a wide array of cyber insecurities and vulnerabilities that look dramatically different from country to country, and thus lend themselves to different technical and policy approaches to risk mitigation.

To address the multi-dimensional technical risk and governance challenges presented by the Mobile Digital Financial Services ecosystem, the team developed a strategic system-of-systems threat model, which combines:

- A financial services cyber threat-model previously delivered to the Homeland Security Systems Engineering and Development Institute (HSSEDI),
- An internationally recognized National Cyber Strategy Development and Implementation model focused on cyber risk management, resourcing, policy, and governance and
- The expertise of a unique multi-disciplinary team of subject matter experts (SMEs) blending deep technical, policy, and international cyber development expertise in diverse fields such as international cyber capacity building, cybersecurity engineering, systems engineering, cyber threat intelligence, technology policy development, cybersecurity and technology law and policy development, and others.

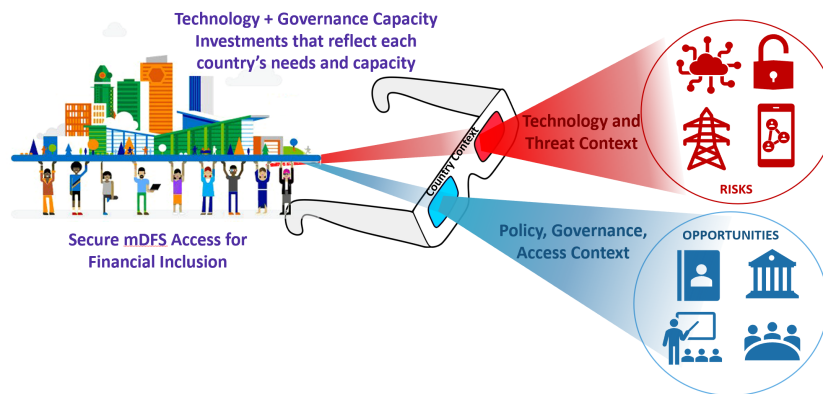
From this array of resources, the MITRE Engenuity team developed an mDFS extended risk model that is unique in its approach, as well as being among the most comprehensive ever developed for the mobile space. It incorporates:

- 680+ cyber-attack techniques,
- Ten threat domains,

- 54 correlated technical risk mitigating solutions, and
- 80+ recommended secure access policies in multiple legislative areas, e.g., Technical, Fiscal, Gender Policy, Education, etc.

This comprehensive risk management framework identifies leverage points for reducing risk, improving access, and establishing trust within the context of each country’s unique technology and policy environment. Risk mitigation in an arena as diverse and complex as mDFS is not solely a matter of the technology environment. Many non-technology factors centered around policy, governance, and user awareness can also have a significant effect on the types and magnitude of risks users experience in a given ecosystem, and an even greater effect on mitigating those risks. We believe this model will be a useful enabler to accelerating and broadening the adoption of secure financial services in the countries where it is applied as a guide to action and investment.

Figure 1: MITRE Engenuity's "Dual Lens" Risk Model



Drawing from MITRE’s deep cyber threat modeling expertise and its [International Cyber Capacity Building Framework](#), the MITRE Engenuity mobile Digital Financial Services (mDFS) Risk Management Model (RMM) uses a “dual lens” approach (Figure 1) that combines both technical and policy/governance risk factors and mitigants for a comprehensive view of the mDFS ecosystem in a specific country. Developed for government, business, NGO, and investment leaders and organizations that want to improve and expand secure access to mDFS in a particular community of interest, this model is designed to help narrow the cyber risk landscape to those areas most likely to apply within a specific technology ecosystem, and to provide recommendations for both technical and policy mitigations aimed at maximizing and optimizing impact. Our model is currently being integrated into an automated, dynamic software platform that will evolve with the changing landscape to provide a flexible yet consistent approach to evaluating specific national and local ecosystems in order to identify the most relevant **cybersecurity threats and obstacles to secure access**, and the **policy and technical approaches** most applicable to expanding and improving secure mDFS access in a given technology and governance context. It is intended to be used by governments and investors

seeking the best combination of technical and policy approaches for enhancing the secure mDFS ecosystem in a particular community of interest. This model can be used to:

- Identify **risks common to a specific country or local technology ecosystem**, to enable limited resources to be focused on relevant risks.
- Apply **threat domain filters** to isolate ecosystem segments (such as mobile device software or identity management systems), which may be best addressed by different stakeholders.
- Identify opportunities to **simultaneously reduce multiple risks** through public policy, industry standards, and governance approaches that correspond to country, government, or industry context and resources.
- Incorporate risk mitigation and opportunity-enhancing characteristics that **support countries' technology ecosystem evolution** toward high-bandwidth and internet-based digital financial services applications.
- Identify **risk mitigation strategies and policy opportunities** in various types of mDFS ecosystems and use cases, whether bank-centric, mobile money-centric, or hybrid.
- Help investors identify **the most effective partners** to engage with in a region and a country to improve security and access through targeted initiatives.

The MITRE Engenuity RMM for mDFS addresses the gap in stakeholder decision-making about where to focus resources to successfully evolve the digital financial services ecosystem by bringing together both the technical and governance aspects unique to each ecosystem to identify tailored, context-informed recommendations for making effective and lasting changes in mDFS access and security.

Real-World Application

As a companion to this model, MITRE Engenuity developed a dynamic software platform which automates and recreates the SME methodology; this enables non-cyber expert stakeholders quickly to select relevant ecosystem characteristics and assess what risks are most prominent. They also receive both technical and policy/governance recommendations to apply to their risk mitigation strategies. This platform is ready for pilot testing for a particular objective and application in any of the following use cases:

- Donor Nations or Assistance Organizations: Use the RMM to identify which of the prominent risk factors in a specific country or area best align with assistance goals and resources, as an aid to focusing resourcing efforts. Identify technology or governance approaches that are appropriate to a specific country as an aid to developing achievable goals and incentive initiatives.
- National Governments: Use the RMM to optimize limited resources by narrowing the risk landscape. Identify where policy/governance approaches can mitigate risks, even in a diverse technical ecosystem. Identify incentives or disincentives that may affect the

mDFS access and security, such as specific policies toward licensing, fees, taxation, etc. Identify less obvious contributing factors to mDFS adoption and security, such as gender policies, education curricula, the presence of a national digital identification program, or the availability and security of agent networks, that could be modified through policy.

- **Technology (including Fintech) Companies and Regulatory entities:** Identify approaches such as specific technology features and standards that can provide widescale improvements in ecosystem security. Identify national or regional trade and cooperation approaches that could help or hinder adoption of mDFS technologies, applications, etc.

Application Use Cases

Every year there are numerous news headlines related to major data breaches, financial fraud cases, and other cyber crimes. Using our comprehensive catalogue of contextual risks, stakeholders could leverage real-world news stories, along with the threat model's knowledge framework, to quickly evaluate their security posture and proactively find opportunities to enhance their overall defense-in-depth strategy.

Other real-world use cases include:

- **National Governments:** Major changes in technology ecosystems are invariably accompanied by shifts in the cyber risk landscape. For example, as legacy cellular protocols become obsolete—as in the shift from 3G to 5G—or as different protocols proliferate across an ecosystem, different vulnerabilities will emerge or be resolved, often dramatically affect the system-of-systems risk landscape. This extended risk model is expected to help governments and NGOs tailor approaches to helping countries anticipate and address their evolving ecosystem risks. The knowledge framework can also be used to proactively identify various regulatory or technology policies (e.g., government regulations surrounding digital financial services, licensing, technical standards, etc.) to help mitigate anticipated risks on a broad scale.
- **Financial Organizations:** Real-world attacks often highlight vulnerabilities that could have been identified beforehand, and which often could be affordably and effectively addressed. For example, in 2016 the BBC reported an attack on the Bangladesh Central Bank in which hackers managed to steal \$81M US dollars. Although this complex hack was accomplished after delivering a custom software exploit to affect the bank's database and SWIFT transactions, a forensic investigator reported the bank didn't have a firewall and was using obsolete routers that cost on average \$10 USD on sensitive financial networks. Thus though the malware itself was sophisticated, the delivery method was not, and the Central Bank could have significantly improved its risk profile with relatively minor investments in updated hardware and software. Engenuity's threat model could be used to identify risks from end-of-life technologies and accompanying risk mitigating actions (e.g., patching, hardening) to reduce the probability of a similar software exploitation.

- **FinTech Users:** Many financial service providers offer customer training to help prevent fraud. M-Pesa, a major mobile banking service in Africa, provides their customers with fraud awareness tips, focused primarily on social engineering, on their website. The comprehensive set of security provisions available at the mobile user level that is included in Engenuity’s model provides opportunities for extensive security awareness training in other areas, such as:
 - a. Avoiding poor encryption protocols for multi-factor authentication (e.g., SMS messaging);
 - b. Risks from connecting to untrusted networks or charging stations; and
 - c. Cyber supply chain risks that can affect mobile users (e.g., pre-loaded device backdoors or spoofed mobile applications, etc.).

1 Project Purpose and Goals

The purpose of this work is to apply MITRE’s deep cybersecurity threat modeling and international capacity building expertise and create an application that non-cyber experts can use to accelerate mDFS safely and securely in developing countries. After assessing several mDFS ecosystems, applications, and related policy environments, we share the following insights:

- Safe and secure mDFS ecosystems in developing economies are possible by considering the cyber threat landscape and risk mitigation strategies up front, and by deliberately instituting policies and governance mechanisms that foster secure technologies and equitable access.
- Policy can never anticipate the technical weaknesses that will emerge in this dynamic ecosystem, but governments can improve policy and outcomes through a dynamic understanding of the emerging threat landscape, and deliberate development of governance mechanisms and policy of various types (e.g., regulatory, technology, fiscal, trade, and national monetary policy).
- Taking a proactive stance against cyber threats and vulnerabilities and for expanded, equitable, and secure access will pay off over time—it will grow the mDFS ecosystem, strengthen governments, attract industry, and expand opportunities for individuals through access to financial services traditionally available only to “banked” consumers.

1.1 Cyber Risk Frameworks and Technical Trends

By leveraging MITRE’s ongoing work with international partners in cybersecurity awareness, defense, and incident response, MITRE Engenuity developed a technical cyber threat model that can support a comprehensive understanding of attack vectors, systemic behaviors, impacts, and counter measures relative to the mDFS environments and deployed technology levels. This

model is informed by MITRE technical efforts in cyber incident forensic reverse engineering, Cellular 5G cyber threats, and adversary behavioral-based machine learning detection techniques,ⁱⁱ including, but not limited to, MITRE’s internationally recognized [ATT&CK™](#) framework. It also incorporates ongoing analytic work with US Financial Services entities and global payment system firms in areas of blockchain, digital currency, payment system cyber and operational resilience, and cyber practitioner education. Foundational elements of this model draw on MITRE’s previous work to strengthen US Critical Infrastructure Protection programs through improvements in risk management against advanced threats as part of its support to the Treasury’s Financial Crimes Enforcement Network and the Department of Homeland Security.ⁱⁱⁱ

1.2 International Technical Strategy, Policy, and Governance

In addition to this cyber threat modeling expertise, Engenuity drew upon MITRE’s internationally recognized [cyber capacity building framework](#)—the National Cyber Strategy Development and Implementation (NCSDI) framework—which is used to help countries identify, prioritize, and implement strategies to expand their capacity to apply digital technologies to meet their national security and economic development needs. It has been highlighted as a global exemplar by the Global Forum for Cyber Excellence and Oxford’s Global Cyber Security Capacity Centre for its comprehensive focus not only on technology but also on the economic, social, and political policy and governance environment that shapes digital economies. MITRE is routinely invited to present its framework at the Global Forum for Cyber Expertise (where it has been added to the Cybil Library of international best practices) and international cyber capacity building conferences. To date, MITRE engagements at the national policy assistance level have included Botswana, Ecuador, Ghana, Georgia, Mexico, Moldova, Panama, Republic of the Marshall Islands, Singapore, Thailand, and Ukraine, with additional engagements at the regional level through the African Union, the Organization of American States (OAS), and the Economic Council of West African States focused on governance foundations for a digital economy.

While MITRE’s partner nation engagements are usually prompted by a desire for cyber capacity building, in most cases engagements are focused on pre-cursor enablers such as national and international law; governance structures and approaches; regulatory mechanisms and policies; workforce and education programs and incentives; and partnership opportunities across government, civil, private sector, and international organizations such as the World Bank. Drawing on its deep bench of government and private sector national policy and law experts; enterprise risk management specialists; strategic communications practitioners; social-behavioral scientists; cyber threat intelligence analysts; and experts in organizational change, human capital

ⁱⁱ MITRE ATT&CK, Adversary Tactics, Techniques & Common Knowledge, Online <https://attack.mitre.org>.

ⁱⁱⁱ MITRE FFRDCs include National Security Engineering Center (DoD), National Cybersecurity Center of Excellence (NIST), Homeland Security Systems Engineering and Development Institute (DHS), and the Center for Enterprise Modernization (Treasury), Online [https:// We Operate FFRDCs | The MITRE Corporation](https://WeOperateFFRDCs|TheMITRECorporation).

planning, and enterprise transformation, MITRE has developed and adapted an extensive suite of international comparative analyses, best practices, and legislative and policy approaches related to creating and sustaining effective national policy related to all aspects of digital economies and national security, with particular focus on identity, privacy, transparency, safety, affordability, and equitable accessibility to digital technologies spanning every industry sector from finance to healthcare and transportation.

The MITRE International Cyber Capacity Building team has also developed a national digital workforce development framework to help countries attract, develop, and retain a workforce with the digital skills needed for a modern economy, which is being introduced in several South and Central American and East Asian countries. MITRE is also in the process of developing a Critical Infrastructure Identification and Protection for Emerging Economies framework.

1.3 Technical Risk and Policy/Governance Opportunities Synthesis

Applied together, these technical risk and policy/governance opportunity perspectives produce a flexible yet consistent approach to evaluating specific national and local ecosystems in order to identify the most relevant cyber threats and obstacles to mDFS access, as well as the policy and technical approaches most applicable to expanding and improving secure mDFS access in a given technology and governance context. It is intended to be used by public, private, and NGO sector organizations that want to secure the mDFS ecosystem in a particular community of interest.

2 Background

The World Bank estimates that 1.7 billion people around the world today, mostly in emerging markets and developing economies in Africa and Asia, do not have access to financial services such as those typically provided by banks (deposits, savings, payments, funds transfers, loans, and so on).¹ The reasons for this vary—from difficulty in accessing a financial service provider (FSP) access point (such as a bank or ATM), to lack of identity documentation required for banking, distrust in banks, lack of sufficient funds, the cost of banking (minimum balances, fees, etc.), cultural prohibitions, and other reasons²—but the cost to individuals and national economies of having large segments of their populations unbanked is significant, because unbanked persons are cut off from many credit, investment, and commerce opportunities, and are less likely to be able to save for major expenditures like starting a business or recovering from crisis. It is more difficult for them to pay for necessary services like utilities, or to receive employer or government payments such as pensions, benefits, or assistance programs—a situation that can create a vicious cycle, given that poorer people are 13%^{iv} less likely to have access to precisely the kinds of financial services that could improve their situation.

Broadening financial inclusion has been a major goal of many countries, and of development entities like the World Bank and many non-governmental organizations (NGOs) for more than a decade, but many obstacles remain, particularly for women, who are over-represented among the unbanked in most economies. While in most cases the gap hasn't significantly widened, in most cases it also has not narrowed, leaving an average of a 9- to 11-point difference in developing nations. The World Bank noted in its Findex 2017 report that “this is true even in economies that have successfully increased account ownership and have a relatively small share of adults who are unbanked. In Kenya, where only about a fifth of adults are unbanked, about two-thirds of them are women.”³ Women's relative lack of access to financial services not only limits their own opportunities for self-determination by preventing them from accumulating savings, getting loans for small businesses, paying their own bills, accepting remittances, receiving government benefits, etc., but also hampers economic development by effectively precluding the full participation of more than half of the potential workforce and consumer base by limiting their access to capital. Again, there are many reasons: cultural and mobility impediments, less likelihood of controlling money or property, greater obstacles to acquiring identification,^v less representation in the formal workforce, and less access to education,⁴ with implications for

^{iv} According to the World Bank Findex 2017 report, among adults of the poorest 40% of households in developing nations, 39% have no account, whereas in the richest 60% of households, the number without an account is 26%—a ratio that as of that report had not meaningfully changed since at least 2014.

^v Inequalities in access to acceptable identification are a key contributor to gender inequities in many countries. In 2014, men in India were 20 percentage points more likely than women to have an account. By 2017, India's gender gap had shrunk to 6 points as a result of a strong government push to provide universal biometric identification cards (World Bank Findex 2017).

literacy/numeracy and employment prospects—less money and no employer relationship likely makes getting a bank account less clearly advantageous.

These dynamics have been changing, however, with increasingly widespread availability of mobile phones and internet access (the *Harvard Business Review* found that 1 billion of the world’s 1.7 billion unbanked own or have access to a mobile device⁵), which promise to eliminate barriers such as distance or inaccessibility, and lower the cost of providing financial services by reducing the “brick and mortar” and human resources footprint.⁶ Even without internet access, 2G and 3G cellular networks can support long-distance transactions through USSD or SMS text protocols, although some countries and providers levy taxes on such transactions. As with bank accounts, there is a gender divide in mobile device ownership,

with men in the six countries surveyed being significantly more likely to have a phone. Pew noted that “among countries with significant gender differences, the gaps between men and women in smartphone ownership range from 6 points in Tanzania to 15 points in Ghana.”⁷

The advent of smartphones offers even greater opportunities than basic mobile phones, and smartphone penetration in emerging economies has been growing steadily (Figure 2). Worldwide, Sub-Saharan Africa has the lowest rate of smartphone ownership of any geographic region, yet a 2018 Pew Research study found that in countries surveyed (Ghana, Senegal, Nigeria, Kenya, and Tanzania), approximately one-third of adults had a smartphone (compared to 77% in the US in that year). Of the countries Pew surveyed, Tanzania had the lowest penetration, at just 13% smartphone ownership, and its adoption curve has been flatter.⁸ As mobile devices—and particularly smartphones—proliferate, the opportunities to use them for accessing remote services such as digital financial services also grow.

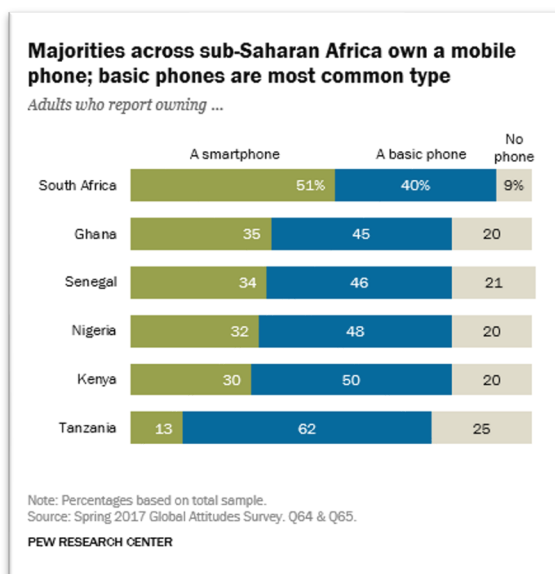


Figure 2: Mobile Device Ownership in Africa

2.1 From Mobile Phones to Mobile Money

Mobile networks and devices—particularly with internet access—have become a major force in the provision of DFS. While they can, as discussed above, help overcome accessibility barriers such as distance for people with existing but difficult to reach financial institution accounts, banks have not been the biggest winners in the explosion of mDFS—that award goes to mobile network operators (MNOs) and telecommunications companies (telcos), which typically started out allowing customers to buy additional airtime minutes directly via their devices, without a bank account.

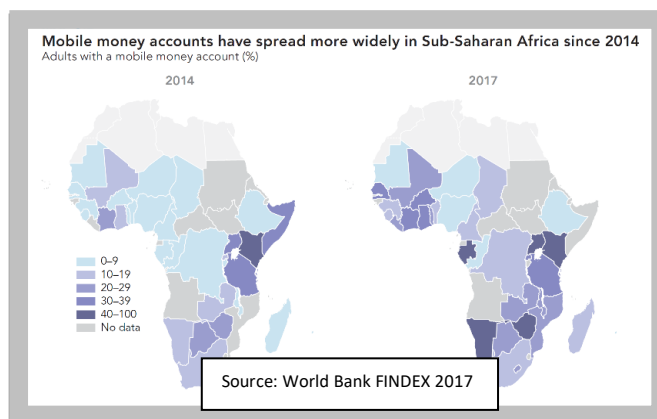


Figure 3: Growth of Mobile Money

Over time and through partnerships with entities like WorldRemit, PayPal, credit cards, banks, and businesses, MNO services expanded to allow the payment of other utilities and services from a “mobile wallet” that allowed users to deposit or disburse cash via local agents while storing the balance on their phones. These “mobile money” applications have continued to expand and mature to the point that the largest and best known constitute de facto national currencies in some places. Perhaps the best known of these, M-Pesa, was launched in Kenya in 2007 by Safaricom, the largest mobile network operator in Kenya. It has since expanded to Tanzania (via Vodaphone), Mozambique, DRC, Lesotho, Ghana, Egypt, Afghanistan, South Africa, and Ethiopia, and was briefly in India before being displaced. Other well-known mobile money applications associated with MNOs include MTN Mobile Money, Airtel Money, and Orange Money.⁹

Of the top 20 countries in the world in mobile money usage, 15 are in Africa, where the use of mobile money now far outstrips traditional bank accounts.¹⁰ In Kenya, the birthplace of M-Pesa, even a large majority of basic phone owners (79%) and 88% of smartphone owners report using their device to send or receive money. As of 2017, M-Pesa had about 20 million registered users in Kenya, and its transactions amounted to almost half of Kenya’s gross domestic product.¹¹ mobile money applications are not limited to MNO-provided options, but also include digital stand-alone applications such as PayPal, GooglePay, etc., that can be download from app stores (Africa in particular is known as a hub for DFS application start-ups), social media-provided apps such as Facebook Libra or China’s WeChat mobile money app, and an emerging slate of cryptocurrency applications. These are discussed in greater depth in Section 5.

Unfortunately, this explosion in mobile money services has largely not been accompanied by an equal emphasis on even the most basic cybersecurity protections, such as data encryption, which is not available for basic phones.¹² These and other cybersecurity concerns are addressed in

greater detail below. In addition, the proliferation of mDFS is raising related political and economic concerns among some governments and other observers, including:

- The acceptable role of mDFS that are based on cryptocurrencies not controlled by government, are often associated with cyber and cyber-enabled crimes, and have so far tended to fluctuate quite wildly in value
- Threats to national economic or fiscal policy created by mDFS applications that do not rely on national currency¹³
- The increasing reliance on social media applications, many of which have fraught relationships with national governments, and that offer mDFS applications that further enhance their popularity
- The impact of a growing tendency on the part of some national governments to shut off the internet or particular applications—particularly social media^{vi}—on people in the country who rely on mobile money
- The greater appeal of some mobile money applications that use a “basket of currencies” or are pegged to specific strong currencies, over that of the national currency when that currency is weak or unstable
- The potential volatility of funds for national bank-sponsored mDFS—digital runs on banks, for instance, in response to real political events or online rumors, can happen much more quickly than physical ones, and are less easily subject to control

Zimbabwe: A Cautionary Tale

Cybercrime is not the only threat to mDFS economies. Quartz Africa reported in June 2020 that Zimbabwe’s government banned all mobile money apps, claiming they had “impeccable intelligence [showing that] mobile money systems of Zimbabwe are conspiring, with the help of the Zimbabwe Stock Exchange, either deliberately or inadvertently, in illicit activities that are sabotaging the economy.” As Zimbabwe’s economy worsened over the preceding years, with little foreign exchange, a plummeting Zimdollar, and frequent long-term cash shortages at banks, citizens overwhelmingly turned to mobile money, with mobile wallets accounting for 84.8% of all transactions, representing 22.6% of the total value of financial transactions during the last quarter of 2019, according to the country’s central bank. The government had blamed EcoCash in particular, the country’s dominant mobile money service provider, for accelerating the decline in the street value of the Zimdollar. The ban frustrated Zimbabweans, who have increasingly relied on mobile transactions for remittances and bill payments during the COVID-19 pandemic lockdowns.

^{vi} Quartz Africa reports that politically motivated internet shut-downs in Africa increased 32% between 2018 and 2019, with 35 incidents across 19 countries lasting longer than a week. Source: Quartz Africa, “Internet shut-downs in Africa were more frequent and lasted longer in 2019,” reporting based on tracking by the Access Now, and internet freedom advocacy organization.

- Privacy and manipulation concerns arising from the use of digital currencies, such as the digital yuan, that allow the tracking of individual transactions
- Lack of visibility into and control over consumer protection, data privacy, and operational risk issues potentially associated with high-volume cashless apps like Venmo, WeChat, and M-Pesa
- The intersection of mDFS, national identity programs, gender inclusion policy, privacy policy, and other governance issues with economic growth and investment incentives and disincentives
- The potential that customers may choose to keep their funds in a mobile wallet rather than transfer them to a traditional bank account, depriving banks of working capital for investment
- The ease and speed with which mDFS transactions can occur, creating the possibility of a virtual “run” on the banks, for instance in response to some crisis, more widely and quickly than banks can “shut the door”

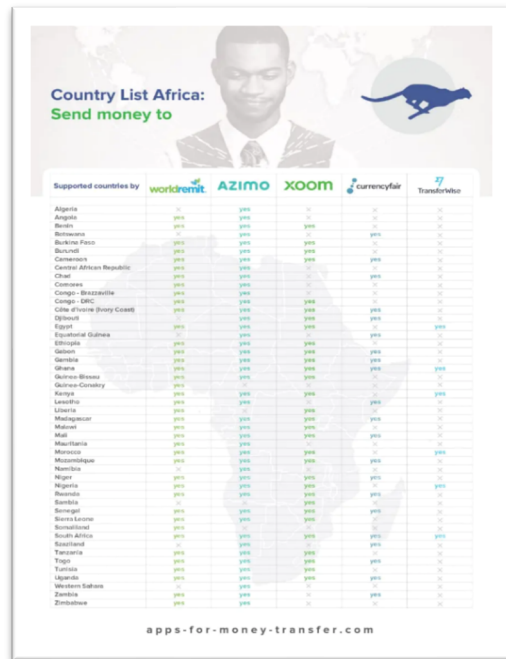


Figure 4: The Many Mobile Money Providers of Africa

These political and economic considerations suggest the need for countries to deliberately address the implications of the evolving mDFS ecosystem in policy. The Atlantic Council, a well-known American think tank focused on international cooperation, global security, and economic prosperity, points out that effectively removing banks as the intermediary between customers and the market requires new regulatory and oversight mechanisms in order not to undermine national monetary policy (such as the ability to invest, provide loans, manage currency reserves, etc.).

Despite these uncertainties, mobile money accounts play an important part in increasing financial inclusion overall and have had particular impact in some fragile and crisis-affected economies, such as Ebola-affected West Africa and earthquake-stricken Haiti, and in many countries where COVID-19 restrictions affected people’s ability to make transactions in cash.¹⁴ Mobile money accounts might also be helping to close the gender gap. The World Bank Findex 2017 examined eight African economies (Burkina Faso, Côte d’Ivoire, Gabon, Kenya, Senegal, Tanzania, Uganda, and Zimbabwe) where 20% or more of adults had a mobile money account in 2017. All of these had significant gender gaps for overall account ownership (financial institution accounts and mobile money accounts), but only Burkina Faso and Tanzania had a significant gender gap in the share owning only a mobile money account.¹⁵

Properly regulated, mobile money can also have a significant positive effect on national and local economies. Governments that establish mDFS-enabling regulatory structures have seen significant economic gains and wider access to banking services in general. Between 2014 and 2017, mDFS access doubled in much of the Sub-Saharan region. It increased even more in Togo, which went from 18% to 45% of adults with an account, with more than half of that growth attributable to mobile money.¹⁶ E-Payments for utilities and other services also tripled during that time. According to GSMA, markets in which regulatory barriers do not allow mobile money businesses to set up effective distribution networks or to register, identify, and activate clients are constricting business, creating major disincentives to investments, and delaying the generation of positive cash flow.¹⁷

2.2 Mobile Agents

According to research by the World Bank and Mastercard, more than 90% of transactions in the developing world are executed with cash. The 1.7 billion adults (35% of the world's adult population) without bank accounts nevertheless need a way to interact with the financial system to pay bills, purchase services, and so on. Accordingly, they need a way to safely move physical cash into and out of the financial system, which largely operates electronically. As the Boston Consulting Group has noted, banks have traditionally offered these cash-in/cash-out (CICO) services via ATMs and bank branches—solutions that are too expensive to make economic sense in markets that have low-income, low-density populations, or other prohibitive factors.¹⁸ Further, those solutions serve people who already have bank accounts, and are not typically available to mobile money users. This is where mobile agents—individuals who essentially act as human ATMs—come into play, providing points of access in otherwise difficult-to-access localities, often in the form of kiosks or as secondary functions in storefronts, where customers can deposit and withdraw cash, and, in the case of storefront agents, typically purchase goods such as groceries.

Mobile agents come in two flavors: mobile bank agents, who operate as a sort of franchise of an established financial institution and offer similar services (including loans), and mobile money agents, who contract with mobile money providers for licenses to act primarily as a CICO point of presence. Agents may also be either dedicated (serving a particular financial service provider (FSP)—whether bank or company—as their primary role) or non-dedicated, meaning they perform their agent function as an additional service associated with some other role, such as store owner. In all of these cases, the agent serves the dual functions of providing a vital CICO capability and creating additional jobs/income, as well as offering the less tangible benefits of in-person assistance for customers who may have limited literacy, numeracy, or digital savvy.¹⁹

Based on an analysis of data from the Reserve Bank of India, the Boston Consulting Group estimates that from 2012 through 2016, the number of mobile bank agents in the country grew 40% annually, significantly outpacing the growth of ATMs and brick-and-mortar bank branches (which grew 8% and 20%, respectively, during the same period).²⁰ Bank agents can offer the full

array of services a branch bank typically would, and in markets with high levels of deposits and demand for loans, banking agents can generate earnings for the parent bank through earned interest. In low-income communities where most transactions are CICO or purchases, however, agents tend to be more of a cost center than a profit center for the bank—they cost more than they earn. In many countries, consumer protection laws mandate that a certain number of CICO transactions must be free of charge to the account holder, so the bank is paying the agent a commission or fee on each transaction but earns nothing in interest.²¹ Nevertheless, bank agents can act as a “foot in the door” for extending banks’ customer bases into underserved communities. In addition, governments increasingly use banking agents as a distribution channel for public programs such as social cash transfers and commodity subsidies (this trend accelerated and expanded during COVID-19 lockdowns).

Mobile money agents act as the retail representative for the mobile money provider (typically an MNO, although some fintech start-ups and social media companies also operate in this space, as described above)—mPesa agents in Kenya (mPesa is described in greater detail in Section 5.1) are a fairly well-known example of this model. They typically do not offer banking services such as credit or loans, but do support other functions besides CICO, like person-to-person fund transfers, mobile phone airtime purchases, and utility bill payments. Some also have partnerships with other entities that allow them to facilitate insurance and tuition payments. Unlike banks, mobile money providers earn money from agents through fees charged to the user for each transaction, which vary by market and may be based on transaction volume, frequency, or size (each approach has advantages and disadvantages in terms of ease of execution/oversight and agent incentives).²² In the Boston Consulting Group’s study, the average agent commission rate was 0.7%, or approximately \$0.20 for a \$30 transaction. The agent’s main challenge²³ is to balance their liquidity so that they have enough cash on hand and reserve in their own mobile money account to cover cash-out requests and facilitate transfers and payments (to support a cash-in or deposit request, an agent accepts cash, and then transfers that amount from their own mobile money account to that of the depositor; cash-out transactions require the agent to receive money from the customer’s mobile money account into their own, and give them cash in return).

In both models, agents can make a decent living if they can sustain enough transactions. The Boston Consulting Group found that urban dedicated agents have a break-even point of about 26 transactions a day; urban, non-dedicated agents (agents who offer services as just one aspect of another operation, such as operating a store) need just 13 transactions per day because their operating costs (lease, equipment, etc.) are spread costs across multiple businesses that are also providing revenue. Dedicated and non-dedicated rural agents with lower operating costs require 10 and 9 transactions per day, respectively, to break even. In that study, the majority of agents conducted 30 to 50 transactions per day, earning an average of \$150 in profits per month. Non-exclusive agents, who represent multiple providers (many consumers in countries such as Kenya and Bangladesh, where mobile money is well established, maintain multiple SIM cards from various providers based on different deals or incentive packages, and may have multiple mobile money accounts), can earn up to 40% more.²⁴

Clearly, mobile agents not only extend financial inclusion opportunities to people who would otherwise be unbanked, but also offer economic benefits that extend beyond the account holder. Indeed, mobile agent networks (both bank and mobile money) are an ecosystem unto themselves, providing jobs and connecting people and businesses. The Boston Consulting Group study found that these ecosystems can be characterized as falling into one of three categories: dense urban locations, rural oases, or frontiers. In “dense urban” locations, agents tend to congregate near areas of high economic activity, like mosques or markets, where there may be several other agents with whom they compete through fees, customer service, and liquidity (ability to satisfy high volume or high value transactions). “Rural oases” describe locations such as highway intersections, fuel stations, or rural markets that represent isolated concentrations of activity far from any other significant economic hubs. Approximately 85% of successful agents operate here, because transaction volume is high and competition and operating costs are low. The challenges for agents operating in “frontier” locations, where a large proportion of the unbanked reside (in India’s Uttar Pradesh alone, 65 million people live more than 5 kilometers from the nearest highway, much less an ATM or bank), are much greater thanks to low transaction volumes (as few as one a day), prohibitive start-up costs relative to incomes in the area (agents must lease office space, equipment, an internet connection, etc.), and higher costs and complexity for liquidity management due to the remote location (the time, distance, fuel, absence from another business, etc., required for the agent to access a bank for cash).²⁵

While the most consistent challenge to the mobile agent ecosystem may be the frontier ecosystem segment, other obstacles also affect the transformative potential of the agent model. Regulatory requirements may make it difficult to recruit and train agents cost effectively. The lack of banking infrastructure, for which mobile agents compensate, may still be insufficient even to support them. And insufficient or unreliable telecommunications networks or power grids may undermine agents’ ability to conduct digital transactions. In addition, while mobile agents essentially extend mDFS access, they can also introduce security vulnerabilities and threats, not only through their own usage, devices, and applications if not properly secured, but also through unsecure Wi-Fi connections at the point of service, or even through deliberate misuse or compromise of customers’ data, such as account numbers, personal information, and access PINs.

2.3 Digital Currencies

Mobile money applications are not the only manifestation of mDFS. Another is the rise of digital currencies. “Right now, more than 70% of the world’s central banks are exploring the merits of central bank digital currencies (CBDCs)—electronic versions of their national fiat.”²⁶ Unlike mobile money that requires the ability of senders and receivers to be using the same app, sometimes on the same platform, a digital national currency functions just like cash, only as an electronic token. Its value and fungibility is the same as coins, and any open, interoperable payment or banking app on any mobile device could send, receive, or save money seamlessly. Also, unlike mobile money, which ultimately relies on private sector banks and their reserves,

digital currencies would have to be backed by a nation’s central bank and national treasury. This poses a risk for countries interested in adopting CBDCs, but as researchers from the Harvard Kennedy School’s Belfer Center observe, “As users demand the convenience and low-cost of digital payments, governments may be asking the question, ‘if not us, then who?’”²⁷ If governments do not get on-board with DFS, they are likely to find that other providers that do not necessarily operate within the national bank or fiat currency systems will fill the void, effectively cutting the national government out of a significant segment of the international economy.

Aside from the fear of being cut out of a large portion of global financial transactions, nations are also considering some economists’ arguments that CBDCs can improve market functioning by allowing faster transaction speeds while lowering transaction costs. In addition, “in many emerging economies, national digital currencies are being considered as a means to increase financial inclusion, by allowing governments to include unbanked populations in the digital economy” through government payments of pensions, benefits, assistance programs, and so on,²⁸ and to provide a single interoperable mobile money currency that, once in circulation, can be used without need of a bank account (though it will not solve problems associated with lack of identification, which is a major contributor to financial inclusion barriers, as discussed elsewhere in this paper).

The rise of CBDCs, epitomized and energized by China’s digital yuan, raises concerns about government tracking of financial transactions and the ability of central banks to “ramp up their operational capabilities to manage a digital currency, from managing reserves and deposits, to protecting user privacy, preventing digital counterfeiting, and mitigating cyber attacks.” CBDCs could also complicate international criminal prosecutions in that investigators would have to coordinate with every country managing any currency implicated in the crime to gain access to transaction records.²⁹ In addition, some American economists are concerned that China’s early dominance and aggressive pressure to utilize the digital yuan anywhere China is paying workers (including many large infrastructure investment areas in Africa) could allow China to dictate the future evolution of the global payment infrastructure, including cross-border trade and remittances.³⁰

Digital currencies can also be issued by private institutions. These may be centralized—that is, issued and regulated by a single authority (but not the government), such as Facebook’s stablecoin “Diem” (formerly Libra)—or decentralized like Bitcoin. At the time of writing this report, Coinmarketcap.com estimates the total digital currency market value at approximately \$2 trillion, comprising of about 3,000 privately issued digital currencies.³¹ The largest United States-based crypto-exchange, Coinbase, identifies the three largest cryptocurrencies as Bitcoin (\$1 trillion), Ethereum (\$426 billion), and Cardano (\$71 billion).³² At least 11 governments, including Nigeria and Bangladesh, have banned cryptocurrencies for stated reasons ranging from investor risk arising from lack of regulation to lack of consumer protections, concern over threats to the national currency, fears that cryptocurrencies support illegal activities including

ransomware and money laundering, perceived potential damage to national economic security, and legitimate concerns about the global and national impacts of a data security breach. In contrast, El Salvador adopted Bitcoin as legal tender, which President Nayib Bukele estimates will save citizens hundreds of millions of dollars in commissions to service providers such as Western Union by allowing direct remittances transactions, which total \$6 billion per year and represent approximately 23% of El Salvador's GDP.³³ One risk to adopting market cryptocurrencies as legal tender is the volatility of that market—El Salvador almost immediately lost the equivalent of several million US dollars to significant market fluctuations.³⁴ Other countries are considering various stablecoin approaches, in part to avoid such volatility, though questions of consumer protection, financial system stability, and appropriate regulatory mechanisms remain.

The *Harvard Business Review*'s Dante Duarte argues that open-source development platforms and “strong governance principles, such as those espoused by the World Economic Forum’s newly-released Presidio Principles, can make a difference in digitizing payments, without imperiling users to fraud, hyper-volatility and lax levels of risk management and compliance, which have plagued many blockchain-based financial services in the past.”³⁵ He notes that, to date, “innovation of low-cost, user-directed internet-ready payments has mostly come from Asia, and these innovations are quickly becoming mainstream.”³⁶ A related blockchain concept, “stablecoins”^{vii} (Facebook’s Diem, mentioned above, is a stablecoin), is being examined by the Financial Stability Board, an international body that monitors the global financial system.

As with the introduction of any new technology, the addition of digital assets has increased the complexities in the attack surface across the system-of-systems that comprises the digital finance ecosystem. The Cloud Security Alliance (CSA) recently developed Blockchain/Distributed Ledger Technology Framework for Financial Institutes to provide stakeholders with security guidance to address the concerns from emerging threats in this new space. The examples below are among the CSA’s top 10 blockchain cyber-attacks:

- **Exchange Hack:**³⁷ On August 18th, 2021, cybercriminals attacked a Japanese crypto exchange’s multi-party computation (MPC) wallet, which deals with the warehousing and delivery of crypto assets, through a subsidiary in Singapore and successfully stole over ~\$90 million USD worth of Bitcoin, Ethereum, and other coins from customers’ “warm” (internet-connected) wallets.³⁸ The exchange assured customers they wouldn’t suffer losses, nor would their balances be impacted.
- **DeFi Hack:** More than \$600 million USD was stolen when hackers exploited a vulnerability in the decentralized finance platform Poly Network.³⁹ To prevent the criminals from laundering the stolen funds, Poly Network acted and urged fellow crypto exchanges to “blacklist tokens” coming from the hacker’s wallet addresses. In an

^{vii} Stablecoins are cryptocurrency pegged to the value of some other asset reserve, such as a fiat currency, a “basket” of currencies, or an investment commodity like precious metals, in order to stabilize its value and reduce volatility and speculation.

unexpected turn of events, the hacker returned all \$610 million worth of digital assets, so customers were ultimately not impacted. Researchers worry of both the lack of security by design and verified source code for a financial application being entrusted by investors with hundreds of millions of dollars.⁴⁰

- **Ransomware** is a type of malicious software that criminals use to deny the victim access to the information system by encrypting the data until a payment is made in the form of cryptocurrency. If the “ransom” isn’t paid, the victim’s risk permanently losing any data on the affected device or network. According to an affidavit,⁴¹ the FBI was able to recover the funds related to the colonial pipeline cyber-attack after using the public ledger and blockchain explorer to track 63.7 Bitcoins to a single address. This affidavit reports the FBI gained access to the private key after receiving approval for a seizure warrant from federal court.

2.4 The Complex mDFS Risk Landscape

While some risks associated with particular aspects of mDFS have been discussed above, the overall risk landscape varies widely across the ecosystem. This is the result of two main continuums. The first is the underlying network technologies that range from low-bandwidth 2G/3G cellular networks that primarily support SIM card-enabled “feature” or flip phones using USSD or SMS text protocols, to high-bandwidth internet architectures that provide multi-feature, graphical user interface web-based mDFS via smartphone apps or computers. The second is the type of “back-end” system supporting the mDFS application, which may be a well-regulated, proprietary banking system, a new fintech start-up’s basement servers, an international telecommunications provider, or something in between.

This array of “starting conditions” means that there is no single descriptor of mDFS risk, and no single solution for remediating that risk. Cyber risks can arise via the telecommunications provider, financial service provider, application developer, service host, user, or mobile devices themselves. Even modern solutions intended to apply to complex systems do not cover all the bases in this arena. For example, end-to-end encryption or zero-trust architectures may be widely touted as global solutions, but those are not implementable on a 2G cellular network or by understaffed administrative offices with limited cybersecurity skills or resources to buy them. Meanwhile, it is cheap and easy to procure fake mobile telecommunications base stations to intercept unencrypted transactions, capture customer data such as usernames and passwords, or send out counterfeit SMS messages asking for users’ private data and credentials. In 2017, reporting on several attacks in Africa indicated that hackers were using dormant accounts and the “no limit” vulnerability in many DFS systems to funnel huge amounts of money out of banking accounts. Even without sophisticated hacks, criminals routinely target less digitally literate mobile money users through phishing and social engineering attacks that drain attacks through various fraudulent schemes.⁴²

Some other threats and vulnerabilities that apply unevenly across the ecosystem include:

- Some regional banks and Savings and Credit Cooperatives (SACCOs) may rely on legacy systems with unsupported and vulnerable operating systems, like Microsoft XP, that they cannot afford to replace.
- Most mobile networks have systemic design flaws because of the 1970s-era communications design—still the current “DNA” of global telecommunications and mobile networks—that makes it easy for bad actors to gain access and intercept private data, steal customers’ funds, or obtain customers’ credentials.
- SIM swaps—a form of identity theft often enabled by telecommunications company insiders in which a criminal steals a person’s mobile phone number by assigning it to a new SIM card in a different phone—are an increasingly common practice. SIM swaps allow hackers to intercept one-time passwords sent to mobile phones as part of Two Factor Authentication, enabling them to hijack DFS and bank accounts.
- In markets where legitimate devices and licensed software are unaffordable for many, black market or “repaired” mobile devices may be loaded with malware and resold as “new” to unsuspecting customers.
- Public Wi-Fi access points may offer locals their only reliable connectivity, yet are generally operated by individuals with no cybersecurity expertise at best and malicious intent at worst. These networks offer hackers opportunities to “eavesdrop” on unsecured connections to steal credentials.
- “Free” phone charging stations may feed malware into a mobile phone.
- Customer information transmitted using near-field communications like Bluetooth can be easily intercepted—many users are not aware of how Bluetooth works or how to turn it off.⁴³
- Unbanked and underbanked customers are less likely to have financial and digital literacy, and may therefore use weaker security procedures, preferring convenience over security (as just one example, mobile devices and even PIN numbers are often shared in communities).
- The mobile agent-facilitated CICO environment produces many opportunities for the unscrupulous to skim money or credentials from customers who may be illiterate or innumerate.
- Many users, particularly women, do not have control over the mobile devices or even accounts that they use, and may be forced to provide account information, PINs, or other credentials to others.
- Many governments view internet connectivity as a risk to their power or social stability and may cut off citizen access to particular applications (especially social media, some of which are mDFS providers) or the entire internet for periods ranging from hours to months, threatening users’ access to mobile money wallets.

2.5 The Impact of Cybercrime

With the expansion of mobile money and other mDFS comes expanded opportunities for cybercrime targeting those services. Figure 5 shows estimates from 2017 on the impact of

cybercrime in Africa. While the amounts many users have in financial accounts, whether at banks or in mobile wallets, is often relatively small, some estimates suggest that two-thirds of all people online (more than 2 billion individuals) have had their personal information stolen or compromised,⁴⁴ so cumulative losses in both money and personal data are significant. More than half a billion US dollars are lost in cybercrimes targeting financial transactions of one kind or another (banking, mobile wallets, and e-commerce, some portion of which is credit card fraud).⁴⁵ Moreover, governments and organizations incur substantial additional costs in after-the-fact remediation, restitution, and reputational/trust losses. The Center for Strategic and International Studies (CSIS), based in Washington, DC, estimates that cybercrime currently costs the world as much a \$600 billion, or 0.8% of global GDP—“more than the income of all but a handful of countries, making cybercrime a very lucrative occupation.”⁴⁶ CSIS notes that, while the wealthiest and most developed countries are targeted most often, it is countries that have enough digital development to provide opportunities but insufficient maturity in cybersecurity to protect their burgeoning systems that lose the most, proportionally, to cybercrime.⁴⁷

As the mDFS environment changes in terms of technologies and providers, cybercriminals adapt. For example, Bitcoin, a digital cryptocurrency discussed in greater detail below, has been popularized in part as a secure and transparent digital option, and countries looking to establish digital versions of their fiat currency usually focus on related technologies. However, sophisticated cybercriminals have quickly adapted, targeting institutions using Bitcoin for theft, and also using Bitcoin as the currency of choice for ransomware pay-outs and other cyber or cyber-enabled crimes. North Korea in particular is known for targeting financial institutions in general and Bitcoin-based national banks in particular.⁴⁸

And as Interpol notes in its 2020 report on mobile money and organized crime, “Whilst acquisitive crimes significantly impact the lives of victims, criminals have also identified further opportunities to exploit mobile money services to assist other criminal activities. These ‘mobile money enabled crimes’ include illicit commodities purchases and terrorism financing. Such significant crimes pose a threat to stability and security across Africa if not addressed by member countries.”⁴⁹

3 Challenge Description

Despite the cautionary notes described above, it must be recognized that mobile DFS in general and mobile money in particular have been a boon to developing economies, connecting people with banking-like services where such services were inaccessible in the past. The mobile money ecosystem also creates jobs in the form of agent networks, fosters commerce, enables people to more easily pay for essential services, and facilitates government and international payments.

MITRE Engenuity’s interest in this lies in ensuring that this burgeoning ecosystem continues to foster greater economic power and financial inclusion in developing economies by helping governments and FSPs build trust in mDFS through the application of a risk management framework of technical protections and policy/governance best practices for creating the most secure and effective mDFS ecosystem for each context. To do so requires a model that accounts for the complexity of this ever-evolving system-of-systems in which governments, corporations, and individuals are all in constant interaction with ever-evolving technologies.

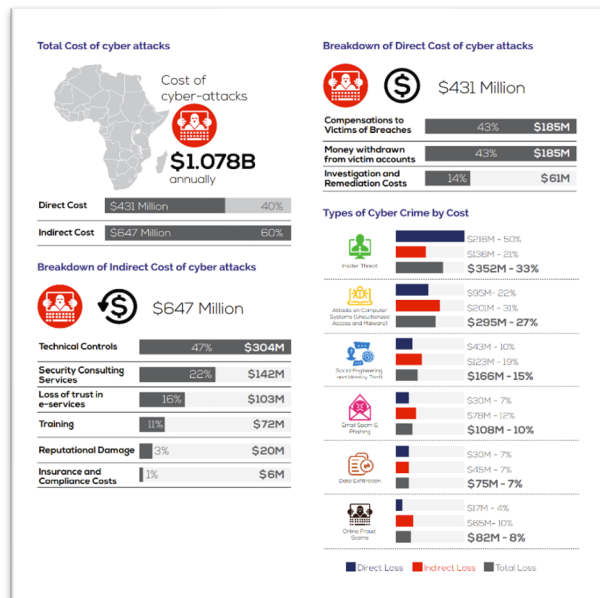


Figure 5: The Costs of Cybercrime

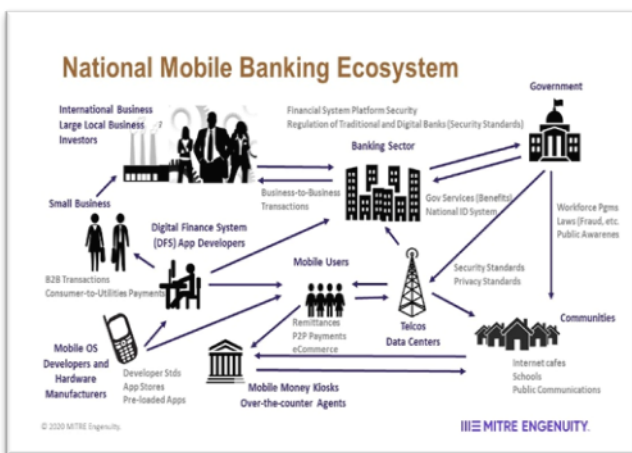


Figure 6: Notional mDFS Ecosystem

As described above, delivery of mobile mDFS to the underserved leverages a host of technologies that span several disparate, interconnected systems owned, operated, and regulated by multiple stakeholders, including governments, financial institutions, mobile device providers, telecommunications companies, mobile money payment processors, and application developers. Analyzing the roles of these stakeholders involves consideration of payment infrastructures (financial institutions, small over-the-counter kiosks, and purely digital banks), government policies, national laws, regulations, technical standards, economic incentives and barriers, and user behaviors and use cases (including first-time digital consumers).

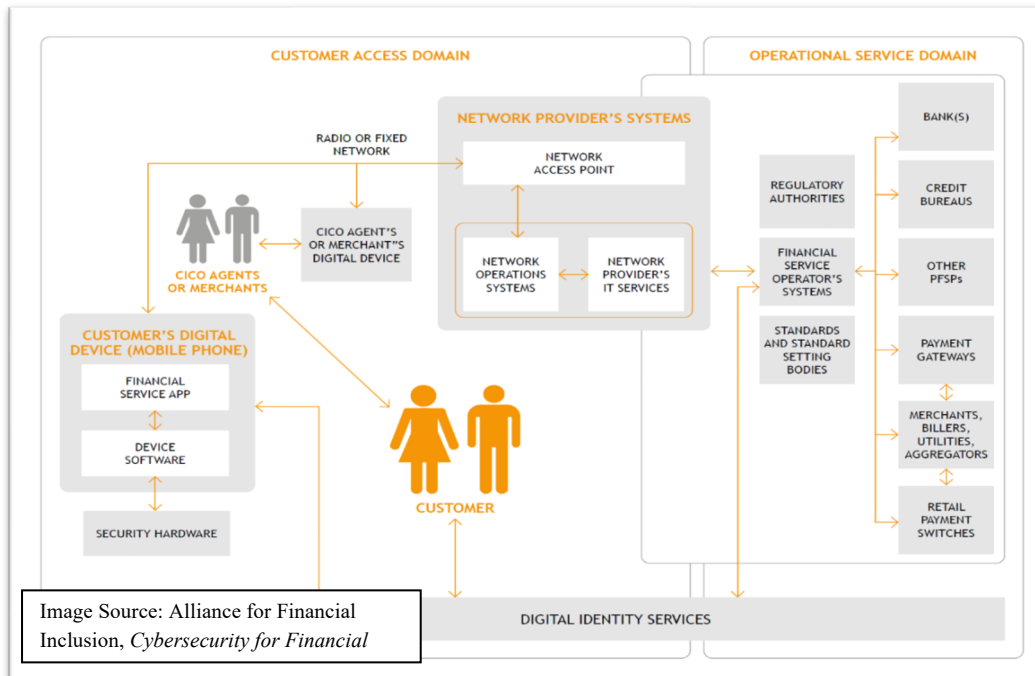


Image Source: Alliance for Financial Inclusion, *Cybersecurity for Financial*

Figure 7: Customer, Network Provider, and Operational Domains

A final consideration is the human element. Human behaviors and the factors driving those behaviors—like incentives, culture, religion, and education—must be addressed in any examination of the security of DFS. These factors are important in understanding the nature of the challenge as well as the feasibility of potential solutions. For example, it is necessary to understand how illiteracy affects cyber risk as well as potential risk mitigations, and how the ways in which people use mDFS shape provider offerings and security decisions. As previously mentioned and described more fully by the Alliance for Financial Inclusion (AFI), a significant proportion of mDFS users are low-income customers with limited digital or financial literacy,⁵⁰ and the World Bank Findex 2017 observes that the two-thirds of adults in the developing world who are unbanked—a major user demographic for mobile money applications, as noted—are “more likely to have low educational attainment... [A]bout half ... have a primary education or less.”⁵¹ This increases the risk of both cyber-attacks and fraud at the personal level. Yet because transactions are typically both of low monetary value and low volume, risks may be seen as acceptable at the provider level, disincentivizing providers from seeking comprehensive security solutions even as they increase service volume (and sometimes usage fees) to compensate for the low values in individual transactions.

Gender is another important human element consideration in increasing secure access to DFS, as there are profound gender inequalities in education, literacy, and access to both technology and financial services. Women are much more likely to be outside the formal labor force, and individuals outside the formal labor force are less likely to have a phone, internet access, or any kind of financial account. Further, in many communities, mobile devices that do exist are controlled by men, and accounts in women’s names are also effectively controlled by their male

relatives, forcing them share their online identify credentials (if any) with the men they rely on to perform financial transactions on their behalf. These disparities have further hindered women’s ability to contribute to their communities and to earn/control their own money—a key enabler of personal autonomy.

To the technology, policy/governance, and human aspects of the mDFS challenge, add the kinds of major contingencies, such as the on-going COVID-19 pandemic and other national and global events, that can also affect the security and availability of such services.

There is no simple solution for addressing this multi-dimensional technical and governance challenge, but MITRE Engenuity is able to draw on deep subject matter expertise in [cybersecurity](#) and cyber threat modeling; [international cyber capacity building](#) across eight policy/governance capability areas; [national policy analysis and advice in multiple national sectors](#), including financial services; and [the development of systems and services designed to address public needs, including inclusion, data privacy and protection, and stakeholder coordination](#).

To conduct a multi-factor mDFS risk assessment model that can be applied to any national context, MITRE Engenuity leveraged its expertise in several areas that have not previously been combined (the following contributing products are discussed in greater detail in Section 3):

- The Homeland Security Systems Engineering and Development Institute (HSSEDI)^{viii} [Financial Services Sector Threat Model](#) and other financial services risk frameworks
- [MITRE’s ATT&CK for Mobile](#) framework, highlighting cyber threats specific to mobile devices and users
- MITRE’s internationally recognized [Cyber Strategy Development and Implementation Framework](#)
- Relevant use cases, best practices, and community expertise identified through research and interviews

The desired output was an mDFS Risk Model that considers technology risks in the context of factors such as laws and policies, technology, literacy, and gender that can be applied at the regional, national, or local (state) level to produce a set of tailored, actionable recommendations focused on the risks most relevant to the specific risk landscape in order to inform return-on-investment decisions on the part of governments, NGOs, and other investors interested in improving the accessibility and security of the mDFS ecosystem.

^{viii} MITRE operates and contributes to the HSSEDI Research and Development Center, which is funded by the US Department of Homeland Security. This threat model was developed by MITRE researchers.

3.1 Actors and Factors

One major step in developing a risk model for a system-of-systems is identifying entities that have control or influence over significant aspects of the ecosystem. For this project, some of these stakeholders include:

- Governments and regional organizations
- Payment processors
- Application developers
- ICT sector
- Mobile network operators
- Banking sector
- Industry/businesses
- Regulatory agencies
- Mobile agents
- Individual users



Figure 8: Intersections of DFS Stakeholders (Actors) with DFS Security Categories (Factors)

Some of the technology-related aspects the team considered, in addition to the two technology continuums described above, included mobile device network

characteristics (type, operating system [OS], adoption/penetration, bandwidth, access), typical attack techniques, requirements/standards for platform onboarding, government-established security standards for DFS providers, the software/OS/app development environment, and the security strengths/weaknesses of existing mobile money apps.

In examining the kinds of solutions that should emerge from this model, we considered:

- What’s already been done? By whom? How well did that work?
- Who else is looking at this problem, and what partial solutions can they bring?
- From the ATT&CK for Mobile framework, what is most common that can be cost-effectively remediated?
- From the HSSEDI FS Cyber Threat Model, what general practices could be applied in this environment with broad effect?
- From the international cyber capacity building perspective, how can policy and governance approaches be used to create ecosystem-wide improvements in both equitable access and security?

4 Target mDFS Use Cases

In examining the way mDFS are used in emerging economies, we identified several key use cases that any effective model must address.

4.1 Cash In/Cash Out

CICO functions have already been discussed at length above. As previously noted, this is one of the most prevalent use cases for all DFS, whether through a mobile device, an agent, or both. It carries particular risks in that training and accountability of agents vary widely, and opportunities for point-of-service fraud abound.

4.2 Remittances

Domestic remittances, in which people working abroad send money home, are an important part of many developing economies. In developing economies on average, 27% of adults reported having either sent or receiving domestic remittances in the past year. Domestic remittances are particularly important in Sub-Saharan Africa, where 45% on average reported having sent or received such payments. According to the World Bank’s 2017 Global Findex Database, Gabon, Ghana, Kenya, Namibia, and Uganda have the highest shares of adults using domestic remittances (60–70%).⁵² In Kenya, 89% reported having used an account (as opposed to an over-the-counter wire transfer or similar) to do so—in most cases a mobile money account. As the Findex authors note:

“This should come as no surprise—because when the mobile money operator M-PESA launched its business in Kenya in 2007, it specifically targeted the domestic remittances market, promoting its services with the slogan ‘send money home.’ Indeed, among those sending or receiving at least one domestic remittance payment in Sub-Saharan Africa, most reported having done so through a mobile phone—through either a mobile money account or an OTC service. But in some economies, including Ethiopia, Namibia, Nigeria, and South Africa, people sending domestic remittances through an account are most likely to do so using an account at a bank or another type of financial institution.”⁵³

4.3 Utilities/Pay as You Go

“Pay-as-you-go” (PAYG) services allow low-income customers to make small incremental payments toward otherwise unaffordable goods and services. They originated in MNO packages that allowed users to buy airtime for their mobile devices and expanded into other areas. As GSMA observes in its *Digital Solutions for the Urban Poor* report, PAYG services have “demonstrated great results when applied to rural electrification, are now also unlocking a range of urban services such as water, clean cooking gas, and sanitation.”⁵⁴

4.4 Payments for Goods/Services

Many people can use their mobile money accounts to buy routine goods and services, particularly where the supplier is also a mobile money agent, such as a grocer who provides mobile money agent services as an additional product from their storefront.

4.5 Person-to-Person (P2P)

P2P transfers allow people to provide loans to friends and family members, pay for goods and services from personal businesses, accept/send remittances, and so on. This function is sometimes referred to as wallet-to-wallet transfer, and except for digital currencies that are fungible across platforms and some bank-centric apps, typically requires that both parties be subscribers to the same network or mobile money provider.

4.6 Business-to-Person (B2P)

The B2P use case primarily focuses on employer payments to employees, although the reverse case allows customers to send money to a business account. B2P functionality can reduce payday crimes in which predators wait outside of businesses to extort or simply rob employees of their cash on regular paydays, particularly in rural areas such as some agricultural communities.

4.7 Government-to-Person (G2P)

This is an important, if underutilized, use case in which government payments of all kinds—such as pensions, benefits, and assistance (as during the COVID-19 pandemic or a natural disaster)—are sent straight to recipients. It allows faster, more secure payments, but is typically reliant on a national identity system to which all people (particularly women and ethnic minorities) may not have equitable access, and on reliable connectivity. Because one reason for not having an account is that one's daily life doesn't involve financial transactions of significant value, the addition of G2P functionality can have a significant effect on mDFS adoption, assuming the underlying enablers (such as a digital ID) are in place.

5 Research Observations

This section offers some further, more specific, insights into the mDFS ecosystem, beginning with the key characteristics of some representative and prominent mDFS models that epitomize various approaches to digital financial services. It is intended to provide an overview of some key aspects that may not be familiar to many readers but are important in both the ecosystem analyses for a given country and for understanding some of the technical and policy challenges and recommendations that the model will highlight for specific contexts.

5.1 Characteristics of Prominent Mobile Money Models

Bangladesh: bKash is a mobile financial service (MFS) provider in Bangladesh that Fortune magazine ranked among the top 50 companies in its 2017 Change the World list in 2017, noting that 22% of Bangladeshi adults use bKash for approximately 4.5 million transactions per day. Asiamoney Magazine declared bKash the Best **Digital Bank** in 2018, and World HRD Congress declared it as one of Asia’s best employees in 2017.⁵⁵ Through bKash, users can deposit money into their mobile accounts; withdraw, transfer, and receive money domestically, including from overseas (bKash partners with the China’s Ant Group—formerly Alipay); make payments and recharge prepaid mobile device airtime; and pay postpaid bills.

China: China licenses its DCEP (electronic version of yuan) as a **digital legal tender** through licensed affiliates of the Peoples Bank of China (PBC). DCEP can reportedly be transferred directly wallet-to-wallet, which suggests commercial banks are not necessarily tracking every transaction, but the PBoC certainly can. This has raised concerns about government surveillance and the addition of financial transaction tracking to the Social Credit Score China uses to evaluate and influence citizen behavior. The DCEP does not appear to use public-private keys for digital tokens—users can reportedly scan QR codes within apps like AliPay and WeChatPay to transfer funds P2P.⁵⁶ In areas abroad in which China pays workers, such as those associated with Belt and Road projects around Africa, companies are encouraged to use digital yuan, which can be used directly, including sending to China or elsewhere, without the intermediation of PBC branches, expanding China’s awareness of individual transactions overseas while accelerating DCEP adoption.

Facebook Diem: Facebook plans to release its Diem online currency as a scalable **stablecoin** cryptocurrency and blockchain contract service accessible to the global mass-market worldwide, including to users of low-cost feature phones. Backed by a funds reserve and governed by an international and independent governance body called the Libra Association (composed of geographically distributed business, nonprofit, multilateral, and academic organizations), it is intended to improve financial inclusion by providing a secure, private, no-fee platform for global financial transactions that are “as easy and cost effective as sending a text,” and more secure.⁵⁷

M-Pesa: M-Pesa (*M* stands for mobile, *pesa* is Swahili for money) was launched in 2007 by the Vodaphone Group and Safaricom, the largest MNO in Kenya. It is a **mobile phone-based**

money provider styled as a “branchless banking” service that allows users to deposit, withdraw, and transfer money; make payments; pay for goods and services; and access micro-financing services using PIN-secured SMS text messages or a network of agents and retail outlets, in return for a small transaction fee. It has since expanded to Tanzania, Mozambique, the DRC, Lesotho, Ghana, Egypt, Afghanistan, South Africa, and Ethiopia.⁵⁸ It is the most successful mobile phone-based financial service in the developing world, lauded for giving millions of people access to the formal financial system and for reducing crime in otherwise largely cash-based societies.

Mobile Payment Forum of India: The offshoot of an Indian government policy launched in 2014 to boost account ownership among unbanked adults through biometric identification cards, this **bank-centric program** benefited traditionally excluded groups and helped ensure financial inclusion, raising account ownership by more than 30 percentage points between 2014 and 2017 among women and adults in the poorest 40% of households.⁵⁹

5.2 The Role of Telcos

In many ways, telecommunications companies (telcos) are leading the way on mDFS adoption and use cases through their mobile money applications, particularly in African countries where broadband internet connectivity has not caught up to cellular service penetration. Several have actively engaged with national governments and local MNOs to establish “rules of the road” that have expanded the reach and reliability of mDFS in countries like Kenya, Tanzania, and others. One key framework used by several of these entities is the Global Service Mobile Association (GSMA) Mobile Money Certification framework, which establishes principles for secure mobile money platform and service development, including a five-step certification process and online toolkit. Some entities prevalent in Sub-Saharan Africa and Southeast Asia that have embraced the GSMA Mobile Money Certification approach include MTN, Orange, Safaricom, Telenor Microfinance Bank, Tigo Tanzania, and Vodacom.⁶⁰

5.3 The Role of Government

Governments have several roles in the mDFS ecosystem, and how they execute those roles can have profound effects on the robustness and security of the landscape. The most obvious role governments fulfill is that of policy and governance, where decisions can create either incentives or barriers to mDFS development. And indeed, countries have taken a variety of approaches to mDFS. Some, like Kenya, Rwanda, and Tanzania, have actively embraced it, proactively creating a favorable regulatory environment, national standards, and public-private partnerships that have allowed the dominance and broad adoption of major mobile money currencies like M-Pesa.

Others, like Nigeria and Zimbabwe, have found the tendency of mDFS to expand beyond or circumvent national monetary policies and institutions alarming, and have just as actively put policies in place that have the effect of throttling its use, such as banning cryptocurrencies (this

effects only some providers); requiring transactions to be in their sovereign currency, which may be unstable or devalued, and which can hinder use cases like remittances; monitoring and/or taxing transactions; and clamping down on e-commerce where payments can occur online without visibility or taxation.

Still others, like India and Bangladesh, have strived to expand access to bank-based DFS, in part through the dramatic expansion of a national biometric identification program that is compatible with financial services sector know-your-customer (KYC) requirements. Bangladesh also planned to increase rural access to high-speed internet for 100 million citizens in 2020.⁶¹ Once achieved, this should have a significant impact on the availability of mobile money in Bangladesh, particularly since that country has fostered a partnership between its major banks and mDFS provider bKash, for which it has also established security and privacy requirements.

Another way governments can affect the mDFS landscape is through their payer role. Many people cite the small amounts of money they typically handle as a reason not to get a financial account, but by using digital money to pay government salaries, pensions, benefits, and assistance programs (several digital money distribution programs arose during COVID-19 lockdowns when the ability to travel or visit a bank was constrained), governments can incentivize (and assist) people to acquire accounts in order to receive these payments, as Tanzania has done with Tigo Pesa. Uruguay is another country that requires all government agencies to make payments via e-money—in Uruguay’s case, the law mandates these e-money accounts be free to open, include no maintenance fees, and have no minimum balance requirements. Colombia goes further and covers accounts under its national deposit insurance scheme (like the US’s FDIC).⁶²

In addition to fostering or hindering mDFS development directly through policy and governance, or the power of the purse, governments also play a significant role in facilitating key enabling conditions such as national identify programs. There is a strong relationship between formal government identity documentation and the ability to access financial services in general, since KYC anti-money laundering standards and normal banking processes require it for everything from establishing an account to transferring or withdrawing funds or accessing credit. The World Bank Findex 2017 notes that “in Sub-Saharan Africa, where those without a financial institution account were especially likely to cite documentation requirements as a barrier, only 56% of adults reported having government- issued identification.”⁶³ Women may find getting government identity documents particularly prohibitive, since in many countries the process is highly centralized (requiring travel), expensive, rife with corruption, or not available to them without a male relative accompanying and/or vouching for them. Women may have trouble getting secondary identify documents, such as utility bills or property verification, because they do not control family finances or property.

Another key enabler with a great deal of government input is infrastructure. Though many people will immediately think of ICT and broadband connectivity in this context, other infrastructure, such as stable electric grids that support mobile money equipment and the

financial sector infrastructure itself, are also essential factors. The fact that projects like rural electrification have an impact on digital development and financial inclusion makes national prioritization of limited fiscal resources even more complicated for policymakers.

5.4 The Role of Regional Organizations

Regional organizations can have an impact on the mDFS ecosystem if they have the member commitment to do so. Their most powerful levers are cybersecurity and app development standards for any products marketed in the region, shared regulatory practices, and cooperation in countering cybercrime.⁶⁴

5.5 The Role of Cybersecurity Experts and App Developers

Because mDFS are fundamentally software, cybersecurity experts and app developers have—or should have—significant roles in helping to define standards, assess product security, create development platforms, provide user digital awareness training, guide investments in security provisions, and so forth. For example, CREST, a nonprofit based in the United Kingdom, seeks to increase financial regulator capacity to measure and manage cybersecurity risk through accredited pen testing, standards, and local workforce training and accreditation.⁶⁵

The GSM Association (GSMA) has played a major role in mDFS development through its Mobile Money Regulatory Index, its Mobile Money Certification, and its principles for mobile money app development. Several major mobile money offerings, including M-Pesa and those from MTN and Orange, pride themselves on complying with GSMA standards.

The role of open-source software is another consideration. Open-source mDFS software provides a common platform for transactions, which is an affordable solution in the development world. However, one challenge with using open-source software for such focused applications is that much of it has not benefited from the kind of crowdsourced scrutiny that identifies and remediates vulnerabilities in more widely used code, increasing the likelihood that cyber vulnerabilities are not identified until after they are exploited. Moreover, liability for such vulnerabilities is difficult to attribute, since responsibility for development resides in a community rather than any individual or other defined entity.

6 Model Development Methodology

The Engenuity mDFS RMM was built on the foundation of the research briefly summarized above, and on the synthesis of several threat and capacity building frameworks, as detailed in this chapter. The team took this unique parallel approach, which merges technical threat analyses with policy and governance assessments, to create a more complete contextual understanding of the DFS ecosystem than has previously been modeled, in order to support the development of recommendations for all affected stakeholders that address the specific needs in their environment. As described below, many of the opportunities to address mDFS access and cybersecurity challenges can best be addressed through a combination of technical and non-technical approaches that reflect the specific mix of technologies, stakeholder programs, and national policies that pertain in a given country. This approach reflects best practices drawn from MITRE Engenuity's deep research experience in both cybersecurity threat modeling and national cyber capacity building more focused on economic and policy development.

6.1 Assumptions

The model was developed using assumptions drawn from MITRE's experience in both the technical and policy/governance environments as they relate to improving secure outcomes in the adoption of digital technologies, particularly in the developing world:

- Technology environments supporting mDFS vary widely, from 2G flip/feature phones with primarily SMS/USSD service to 4G (and soon some 5G) smartphone-centric areas where services are accessed through web-pages and on-board applications.
- These distribution technologies are rapidly evolving through the relatively rapid deployment of 5G infrastructure, bringing 5G threats to existing 4G devices, especially in network-based attack scenarios.
- DFS technology environments also range from bank-centric to mobile network operator and/or social media application-centric, with different implications for systemic vulnerabilities.
- In addition to technical ecosystem variations, the threats and barriers to secure access pertaining to mDFS vary according to the local policy/governance context of each country or community.
- Given the assumptions above, there is no one-size-fits-all solution to improving secure access to mDFS—in every locality, a different combination of factors will determine top risks and appropriate/feasible mitigations. These risk factors will continue to shift over time.
- Different stakeholders will have different policy tools and technical/fiscal resources at their disposal to affect the mDFS cybersecurity ecosystem.

6.2 MITRE Engenuity's System-of-Systems Approach

MITRE Engenuity takes a “system-of-systems” approach to addressing complex technology and policy problems. In the case of improving and expanding secure access to mDFS, this system-of-systems is composed of an interlocking set of technology systems and standards operating within a particular policy/regulatory/ governance and threat context, typically in a severely resource-constrained environment (where “resources” comprise money, trained workforce, broadband connectivity, depth and power of the policy/legal framework, educated users, and the ready availability of the technologies themselves).

To develop this model, MITRE Engenuity considered more than 100 factors (some of which have been discussed above), including:

- Variations among technology landscapes that suggest different threat/opportunity profiles
- Known security and accessibility issues in both mobile device and financial services ecosystems
- The intersection of mDFS with national ID systems (governments)
- Roles and characteristics of payment processors (banks, savings and credit cooperatives [SACCOs], mobile money providers and agents, application developers, e-commerce services)
- Various models of mDFS currently in use (such as M-Pesa) or in development (such as Facebook Libra)
- Standards for application developers (including for financial platforms, mobile devices, and operating systems [OS])
- Infrastructure (mobile network operators/providers, internet connectivity availability, cloud/data center availability and security)
- Mobile Device OS and hardware (IT developers and OEMs)
- End user needs and concerns (consumers, commercial businesses)
- Barriers associated with the inclusion of people without ready access to mobile technologies and/or financial services, particularly women
- Disparities among countries intended to benefit from these services in adoption, national policy, internet connectivity, access to mobile technologies, and other factors that affect the universality of certain “best practices”

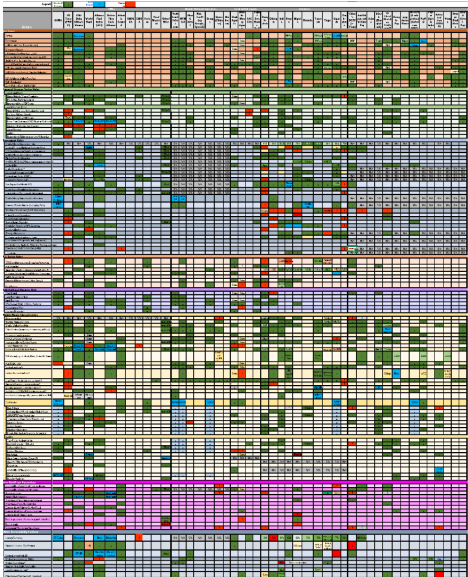


Figure 9: Snapshot of "Actors and Factors" Evaluated in Developing the Engenuity mDFS Risk Model

The fourth framework used drew on MITRE’s extensive experience in international cyber capacity building^{ix} in the developing world to incorporate factors specific to that context. Without considering the unique resourcing, governance, and implementation capacity challenges presented by this environment, it would be easy to create a tool that is useful on paper but ineffective when applied to the circumstances found in the countries of interest to NGOs, donors, and investors. Engenuity applied the MITRE National Cyber Strategy Development and Implementation Framework and the research approaches that went into developing that framework to bring in the policy and governance factors that are instrumental in facilitating or hindering risk mitigation implementation efforts on a national scale. This framework has gained international attention and recognition; is used extensively by several bureaus within the US Department of State; and has been shared with government leaders from nearly 100 nations in Africa, Asia, the Americas, and Eastern Europe through workshops, toolkits, and other offerings aimed at improving national cybersecurity.

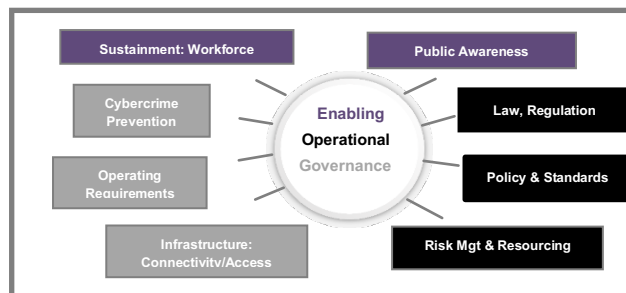


Figure 12: MITRE's International Cyber Capacity Building Model

The different models were fused using the process depicted in Figure 13.

^{ix} “Cyber capacity building” is a term commonly used by the US State Department, the international development and assistance community, other governments, and numerous NGOs to refer to a process of assisting countries to grow and mature their national capacity in any of several capability areas (MITRE’s approach considers eight areas, plus two overarching enabler functions) deemed essential to a strong digital economy.

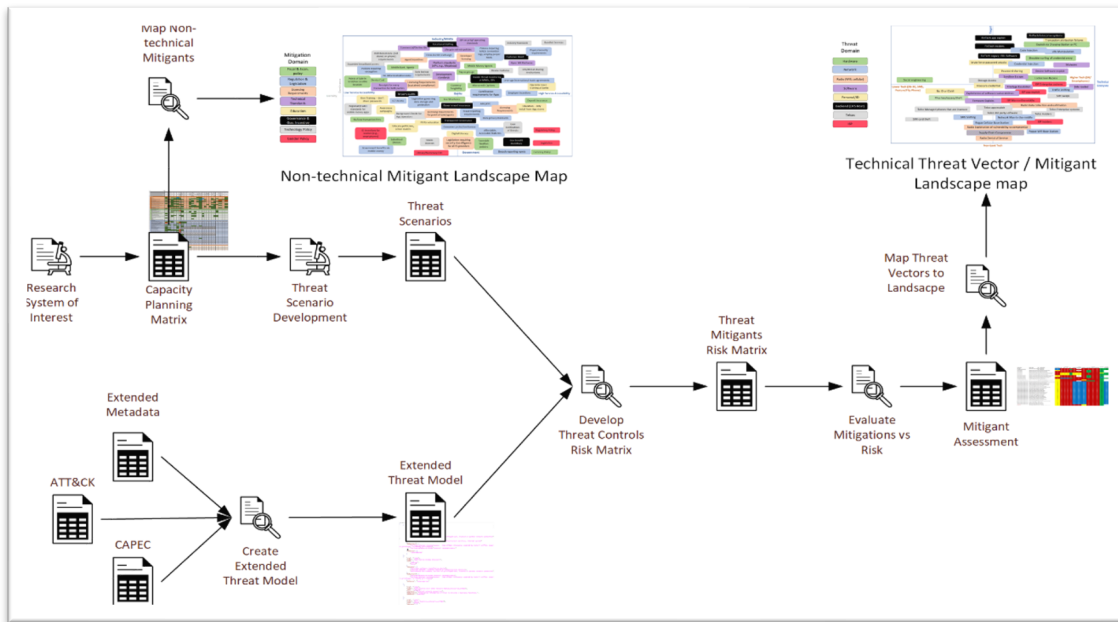


Figure 13: Model Fusion Process Flow

Details on the development of the extended technical threat model and the capacity building model can be found in the following subsections.

MITRE’s experience in cybersecurity framework development has led us to a process that starts with a *tabula rasa* overview of relevant contextual factors, including technology, local/regional governance and norms, culture, infrastructure, human and fiscal resources, and legal/policy factors. This broad research, which includes interviews with subject matter experts and users, is used to identify a weighted matrix of applicable factors pertaining to a problem, which in turn illuminates “pivot points” where stakeholders can apply technology, process, or policy controls to influence security and effectiveness outcomes. For example, particular combinations of technologies like 5G cellular or encryption, and policies such as licensing frameworks or national identification programs, can combine to affect the risk environment. Once these are well understood, we apply our threat models to determine the most likely methods of compromise and evaluate the most feasible and effective mitigation approaches for addressing the identified threats.

Figure 14: MITRE's International Cyber Security Framework Development Approach

For this project, the team studied the following:

- Characteristics and security provisions of existing mobile finance apps (e.g., M-Pesa, bKash, MTN, Tigo, DCEP, PayPal, GooglePay, Zelle, Venmo, MobileMoney)
- Case studies of Africa's mDFS experience to date
- Reports by and interviews with digital banking and cybersecurity experts
- Reports by and interviews with funders and implementers of mobile payment systems
- Mobile and financial security threat models and protection frameworks
- Connectivity and access
 - Is there nationwide connectivity? Are existing networks 2G/3G/higher?
 - What kinds of mobile devices/networks are common?
 - Who has phones? Women? Small businesses (farmers, rideshare providers)?
 - Are there other access points (internet cafés, community centers, workplaces)?
 - What is typical security at those locations?
- Stakeholder roles
 - Who are the typical government, banking, business, and developer stakeholders?
 - Who can develop and market digital finance apps? How is this decided/enforced?
 - How involved should government be, and how will it engage?
 - What are law enforcement's roles and constraints (privacy vs. fraud, money laundering)
 - Who develops standards, and how are they adopted/enforced?

6.3.1 Threat Identification and Mitigation (Technical Ecosystem)

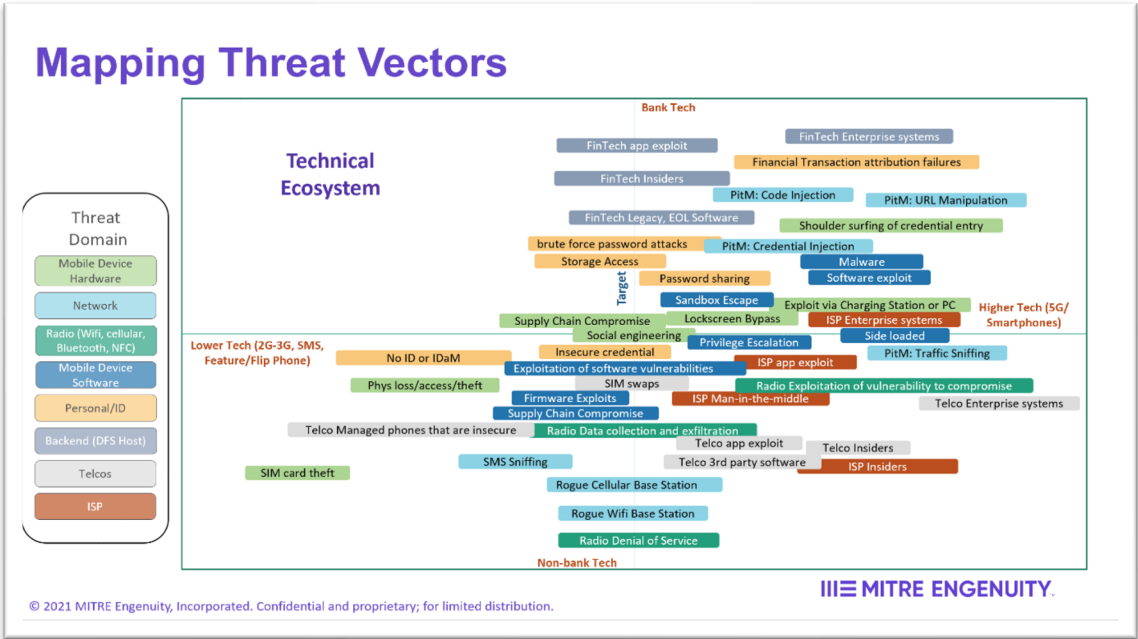


Figure 15: mDFS Threat Map

The first and most commonly examined aspect of any digital ecosystem is the array of technical threats and vulnerabilities it must address. For this model, these technical attacker methods are drawn from MITRE and cyber defense community sources including Adversary Tactics Techniques and Common Knowledge (ATT&CK), ATT&CK for Mobile, HSSEDI Financial Services Sector Threat Model, and the Common Attack Pattern Enumeration and Classification (CAPEC). This array of sources produced a technical threat dataset that is extraordinarily complex (i.e., over 680 cyber-attack techniques) in its full rendering—a simplified subset is depicted in Figure 15. Not surprisingly, most policymakers, assistance organizations or NGOs, and investors will find this full array too complex to be useful for decision-making. To address this problem, MITRE Engenuity’s mDFS Risk Management Model developers examined a notional mDFS ecosystem along two sliding scales intended to help “locate” those threats most applicable to a particular environment. In researching a variety of ecosystems and subject matter expert treatments, the team identified the network/device infrastructure and the primary technologies likely to be targeted by attackers as key “sliding scale” determinants. Accordingly, in this model, the X-axis ranges from ecosystems dominated by low-bandwidth 2G or 3G networks supporting flip phone or basic feature phones and mDFS applications utilizing USSD or SMS text communications, to broadband 4G (some soon to be 5G) networks with a significant proportion of users able to access mDFS services over the internet through a web site, cloud app, or on-board app using computers or smartphones.

At one end of the Y-axis, the primary targets of would-be attackers are bank-centric financial systems, which may be proprietary, and which likely have certain common interfaces and other

characteristics—including platforms, software, and security controls—with those of other banks across the national or international financial services sector. At the other end are systems and services controlled by non-financial sector entities such as MNOs, social media companies, start-ups, or mobile device families (such as the Google App Store or Alibaba ecosystem).

The model developers then identified which common technical attack methods or risks pertain to each of the quadrants formed by these axes, grouping them into eight threat domains (a threat domain in this model is a segment of the ecosystem with particular technical characteristics): mobile device hardware; mobile device software; the host network; radio transmissions (Wi-Fi, cellular, Bluetooth, etc.); personal identity; backend systems (the mDFS application host); telecommunications providers (“telcos”); and internet service providers. It is important to note that this depiction is simplified for legibility—each attack method appears only once, even though it may manifest in several areas. Accordingly, in this portrayal, the location of each threat should be regarded more as the “center of mass” of that threat than a precise characterization. Though each threat is placed on the quad chart where it is most prominent, it likely applies somewhat more broadly. For example, mobile device malware (dark blue) is shown in the center of the lower half of the upper-right quadrant. This should communicate to viewers that it is an attack method much more prominent in a smartphone than a flip or feature phone environment (X-axis) and that it is slightly more common in ecosystems with dominant DFS applications, such as those offered by banks with a website presence that can be spoofed to inject malware, than in those characterized by a wide variety of non-bank mobile money apps. Clearly, however, malware on user devices can be and is used in other conditions as well, so viewers should imagine each threat depiction as being the center of a “probability cloud” rather than a highly localized phenomenon.

A more representative depiction of the underlying data representing the major risks associated with an ecosystem of various characteristics is shown in Figure 16. This dataset was built from the extended, compound technical threat model. The team’s cyber subject matter experts expanded the data in the model with custom fields to provide context behind cyber-attacks relevant to the financial technology sector. The extended threat model was developed to enrich the framework’s dataset and inform decision makers of potential impacts, and addresses various categories, including threat domains, adversary characteristics, attack vectors, cyber adversary lifecycle, and threat events. These enhancements are expected to allow analysts to categorize multiple attacks based on cybercriminal behaviors, adversary objectives, or attack paths.

Threat domains refers to the different ecosystems of technology, organizations, and people that collectively compose the relevant technical spheres within the broader mDFS ecosystem and geographic regions of interest. The following provides a brief description of the combination of components and related factors that create system vulnerabilities—the “attack surface”—which varies by on impacted asset and/or exploitation target.

- **Hardware:** This domain covers electronic devices that form part of the organization’s information technology infrastructure.

- **Enterprise Computing Resources:** Enterprise computing resources are the sum of components that make up an organization’s total business network (e.g., web servers, routers, wireless access points, storage devices, laptops). Because of the commonality among IT components for multiple organizations, this domain will apply to multiple sectors: telecommunication providers, internet service providers, and financial industry stakeholders.

- **Mobile:** This subdomain refers to mobile devices used to access the DFS infrastructure. There is a wide range of mobile device hardware present in emerging ecosystems, including legacy flip phones with talk and text capabilities, mobile devices with rudimentary internet access operating on 3G/4G (often referred to as “feature phones”), and smartphone devices with modern compute operating systems and software applications that operate on 4G/5G. Because of limited cellular and internet infrastructure in many emerging economies, along with issues of affordability for the latest mobile devices, there is a wide range of mobile device hardware that may be present in various ecosystems. Each variation potentially creates different attack surface characteristics.

- **Other:** This subdomain includes non-conventional enterprise technology interfaces including printers, IOT devices (smart TVs, Wi-Fi security cameras, etc.), and USB/USB-C ports. These should all be contemplated as attack vectors that require protections to mitigate cybercriminals’ ability to access internal networks, spread malware, and/or exfiltrate sensitive data.

- **Network:** This domain covers network appliances that enable internet connectivity (e.g., routers, switches, wireless access points) and protect data-in-transit at the network layer of the OSI model. (e.g., firewalls, intrusion detection systems, intrusion prevention systems, virtual private networks, etc.).

- **Radio (Cellular, Bluetooth, Wi-Fi, NFC):** This domain covers wireless technology standards or protocols for interconnection of computing devices at short range or long range. These vary from cellular signal services (e.g., 3G, 4G, 5G), short-range data

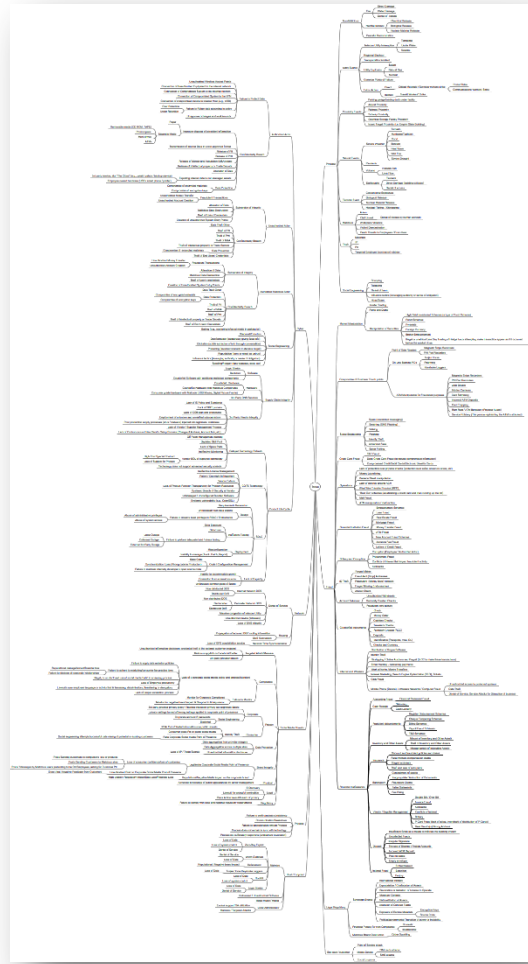


Figure 16: Snapshot of Threat Model on Which the Simplified Visual Representation Is Based

transfer with near-field communications (NFC), or internet connectivity wireless local area networks.

- **Mobile Device Software:** This domain applies to the operating systems and applications needed for mobile devices, including feature phones and smart devices.
- **Personal/Identity:** The user layer is one of the most vulnerable to attacks aimed at bypassing access controls and gaining unauthorized access to the information system. These attacks attempt to exploit illicitly acquired credentials to compromise the victim's digital identity. Examples include insider threat attacks, social engineering, shoulder surfing, etc.
- **Backend (DFS/Fintech Hosts):** This domain encompasses the host enterprise resources (e.g., application and platform developers, computing resources, third-party software, mobile applications, etc.) that enable the secure exchange of mobile money.
- **Telco:** This domain applies to the provider of cellular communication and spectrum services in a predefined region or country. Examples of these mobile providers include SafariCom, Airtel, MTNL, MTN Nigeria, etc.
- **ISPs (Non-traditional; e.g., Facebook, Google, SpaceX):** Due to the limited technical infrastructure, the users of many emerging countries rely on alternative types of internet service providers that are considered non-traditional.

To provide the end user with further context behind each cyber-attack, an extended threat model was developed and enhanced with metadata fields added to each baseline ATT&CK and CAPEC framework element. In ATT&CK, these additional fields were used to extend each Technique and sub-technique, while for CAPEC they were applied to each of the framework's attack patterns.

Adversary characteristics are identifiers generated to profile different attackers' objectives and associated effects on cyber resources. These characteristics help analysts assess the probability an attacker will target a key resource and cause a threat event. The identification of adversary characteristics enables the profiling of different types of threat actors and techniques for use in threat models, cyber tabletop and wargaming exercises, and other similar assessments. During this research, different identifiers were generated to effectively profile various attackers' motives, techniques, and capabilities.

Attack vectors can be thought of as information exchange paths or avenues of attack that cybercriminals may target to generate an effect on part of the system and/or infiltrate the network. Over a dozen different attack vectors were identified for this framework—examples include internal and external networks, email, malicious software installed on devices, actions from users, immediate physical proximity, and supply-chain attacks.

Threat events are observed adversary behaviors that are used to categorize objectives and/or end goals during the cyber-attack lifecycle. There are 37 distinct adversary behaviors classified; examples of these include the following: obfuscate adversary actions, perform malware directed

internal reconnaissance, stage data for exfiltration, exploit recently discovered vulnerabilities, and obtain unauthorized access.

The cyber-adversary lifecycle describes the multiple stages of an attack: Recon, Weaponize, Control, Execute, Exploit, and Maintain.

Cyber effects refer to either the interception, exfiltration, corruption, modification, degradation, insertion, or unauthorized use of computers, networks, or communication systems by hackers, cybercriminals, or nation state-sponsored actors.

To build the extended, compound threat model incorporating both the extensions of ATT&CK and CAPEC as described above, as well as the HSSEDI Financial Services Threat Model, the research team used the process depicted in Figure 17.

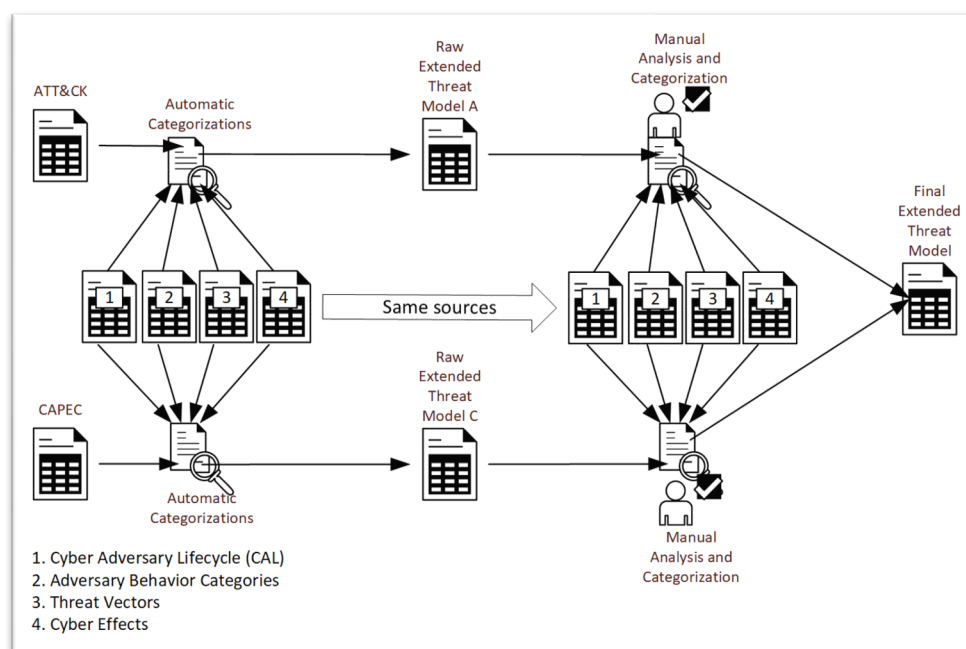


Figure 17: Process for Developing the Compound and Extended mDFS Threat Model

To automate the categorizations for ATT&CK, the four metadata fields were applied across each tactic (in ATT&CK, each technique and sub-technique is a member of at least one tactic). After the automated mapping was accomplished, cybersecurity SMEs reviewed the results, correcting as necessary. The same SMEs then performed a manual mapping process, assessing every technique and sub-technique from ATT&CK and each attack pattern from CAPECT to assign the appropriate values for each of the five metadata fields of the extended, compound threat model.

This process is an enhancement of the one described in the HSSEDI Enhanced Cyber Threat Model for Financial Institutions, leveraging some initial automation to achieve the first pass at mapping. It should be noted that in the future, this process will need to be repeated as the ATT&CK and CAPEC models respectively evolve to reflect changes in the threat environment.

At the time of this document’s writing, ATT&CK is updated on a semi-annual basis—this effort utilized v9.^x

To apply this extended, compound threat model to the threat scenarios produced by the capacity planning process, cybersecurity SMEs reviewed the research and developed threat vectors based on the various domains (see above). These threat domains were then mapped to specific ATT&CK and CAPEC elements (see Appendix B).

The cybersecurity SMEs then assessed the relative risk of the threat vectors in the context of their respective threat domains, with evaluation of the component ATT&CK and CAPEC elements, to determine meaningful mitigants. The mitigations already listed respectively in ATT&CK and CAPEC for each element were consulted, as was the CTID mappings for NIST-800-53 mitigations to ATT&CK.^{xi} These, in combination with domain experience of the cybersecurity SMEs, were used to construct composite mitigations that reflect considerations of each of these models for the threat vectors in the respective domains. These mitigants can also be found in Appendix B.

6.3.1.1 Opportunities to Improve Ecosystem Security and Access (Technical)

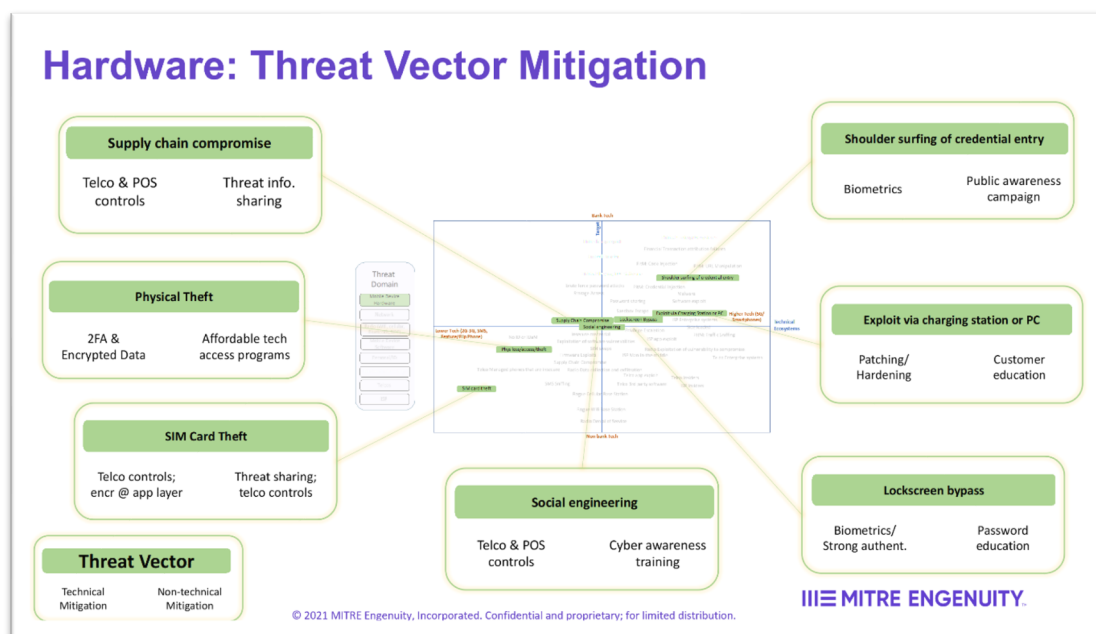


Figure 18: Example of Threats, Filtered by Domain

The next step in the model development process was to identify mitigations associated with each type of attack method. The technical threat dataset included the proposed defense-in-depth

^x See <https://github.com/mitre/cti/releases/tag/ATT%26CK-v9.0> for details, specifically the enterprise-attack.json and mobile-attack.json files within the Source code archives.

^{xi} See ATT&CK-v9.0 Update (#71) · center-for-threat-informed-defense/attack-control-framework-mappings@2a2fb4a · GitHub

strategy to counter each risk with technical and non-technical mitigations. The various options associated with each risk allow practitioners to identify security posture gaps (defensive approaches not currently in place) or find alternative cost-effective mitigants.

During development of this model, the team used a simplified visualization approach to filter the threat map by domain for manageability. Figure 18: Example of Threats, Filtered by Domain shows one example of this simplified visualization, using the mobile device hardware domain as the filter. Entities interested in investing in risk mitigation approaches in a particular domain (for instance, telco operators or mobile device manufacturers) can use this view to identify risks most relevant to their areas of interest or influence. Equally important, they can use this filter to identify commonly recurring mitigations—those that can create improvement in multiple risk categories. In the example shown, for instance, the addition of biometric authentication can help mitigate lock-screen bypass attacks, as well as less sophisticated “shoulder surfing” aimed at stealing credentials. Awareness campaigns or training are non-technical approaches that also apply to both of those attacks, as well as charging station-enabled attacks and social engineering attacks such as phishing. Such recurring mitigation options can help identify approaches with the most “bang for the buck,” which is not always apparent in other models.

6.3.1.2 Mapping Countries on the Technical Ecosystem Quad

Applying the technical ecosystem lens to a country is a matter of characterizing its dominant technical ecosystem: what kind of network/devices are in use, and what kind of fintech is dominant (bank or non-bank oriented). Of course, countries are constantly in development and transition, so it is common that a country will be predominantly 2G/3G, and people rely on flip or feature phones for USSD or SMS text-based transactions, for instance, and yet have some areas and populations with access to 4G networks and smartphones, where mobile money or bank-offered DFS are available. Thus, placing a country in its tech ecosystem is somewhat subjective, and some users of this model may focus more on one part of the ecosystem than another, depending on what they are trying to accomplish. **Figure 19: Notional Mapping of Countries against Technical Ecosystem Contextual Factors** shows a notional mapping of several countries with varying technology ecosystems.

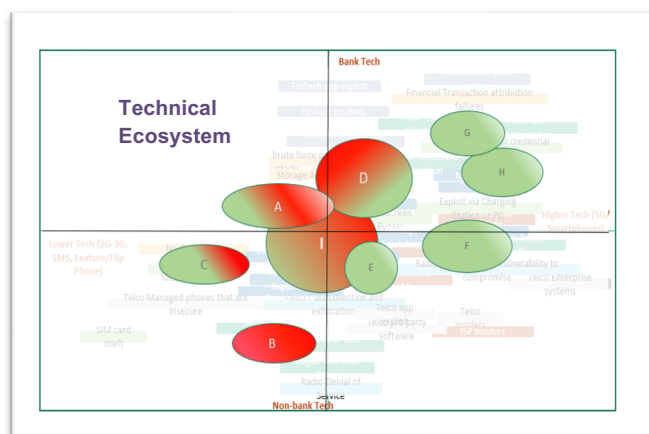


Figure 19: Notional Mapping of Countries against Technical Ecosystem Contextual Factors

In this depiction, it is important not to confuse the size of a country “bubble” with the size of the country. The bubbles represent what portions of the technology ranges the country covers. For example, in this figure, Country I has an ecosystem that is composed almost equally of low- and high-bandwidth networks and is balanced between mobile money or non-bank fintech and bank-centric DFS. The red/green coloration is intended to indicate the degree to which the country may be able to absorb or implement technology-focused mitigations—a somewhat subjective determination by the researchers generated through consultation with SMEs on various aspects of the technology environment. Difficulties (a higher proportion of red) can

result from various factors, such as a lack of standards or a highly complex blend of technologies and actors that makes addressing particular security or access issues on a meaningful scale difficult. In the case of Country B, which is a low-tech country with little banking service penetration, such difficulties may represent the sheer variety of device types and mobile money applications that may spring up in such an environment. Country H, by contrast, is one that has a fairly homogenous tech ecosystem that can be quite concisely represented (smaller bubble). It is more bank DFS-focused than not, and primarily operates 4G networks that support smartphone or web-enabled DFS applications. Perhaps because of this uniformity, it appears to present little anticipated logistical difficulty in applying technical solutions to common risks.

6.3.1.3 Applying the Technical Lens to a Country

Once a country has been approximately located against the X- and Y-axes of the ecosystem quad, users can identify the risk factors associated with the characteristics of that ecosystem by looking at the threats in proximity to the country's bubble. Again, it is important to note that both the bubble and the risk factors are “fuzzy” in the sense that they do not have defined

borders. As just discussed, the country bubble is an approximation that depicts predominant ecosystem characteristics. And as described above, the location of each threat depicted on the map is more like the center of a probability distribution than a specific point—each can and probably does apply somewhat more broadly than the discrete graphical location would suggest. Nevertheless, by locating the country within the risk map, users are able to identify threats that are very likely to apply to that environment and eliminate from consideration or lower the prioritization of distant, less likely threats. This allows investors in government, NGOs, or international assistance entities to make better use of constrained fiscal and personnel resources by offering a first-order prioritization when considering technology-based approaches to lowering risk.

Note that in Figure 18: Example of Threats, Filtered by Domain above, mitigations associated with a handful of proximate threats are listed. This representation is an extreme simplification of the “behind the scenes” association of risk mitigation controls with particular threats the model supports (Figure 16), described in the sections above.

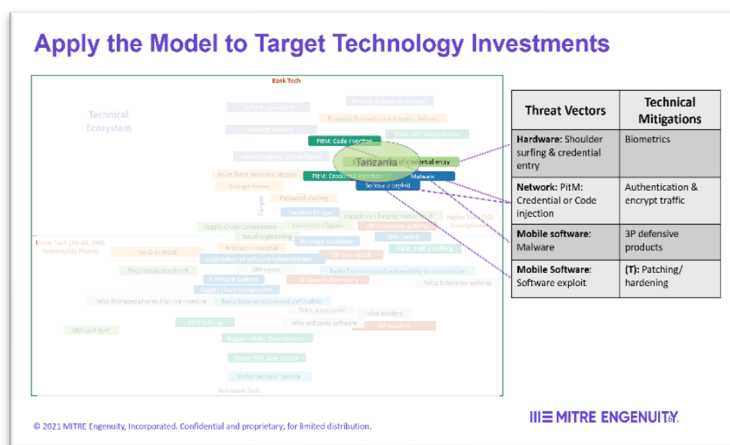


Figure 20: Using the Country Mapping to Identify Proximate Threats

6.3.2 Non-Technical Ecosystem Factors

Risk mitigation in an arena as diverse and complex as mDFS is not solely a matter of the technology environment. Many non-technology factors centered around policy and governance can also have a significant effect on the types and magnitude of risks users experience in each ecosystem, and an even greater effect on mitigating those risks.

The model’s developers took a similar approach to the technology-focused one described above in identifying non-technical ecosystem factors. In Figure 21, the X- and Y-axes represent ease of access to DFS and the relative dominance of influencers in the governance of the ecosystem, respectively.

Along the X-axis, low accessibility reflects any of a variety of conditions that could make it prohibitively difficult to access a DFS point of service, from location in an isolated rural area with little or no ICT connectivity to the hyper-congested conditions that pertain in some urban areas. In both cases, customers may have to spend hours reaching a point of service, and in some cases hours or days longer to actually receive that service, whether because of lines, service shut-downs, unavailability of agents, or other reasons. Other barriers to access, which disproportionately affect women and other disenfranchised groups, may include an inability to travel, hold, or access accounts in their own names, or easily/affordably obtain needed

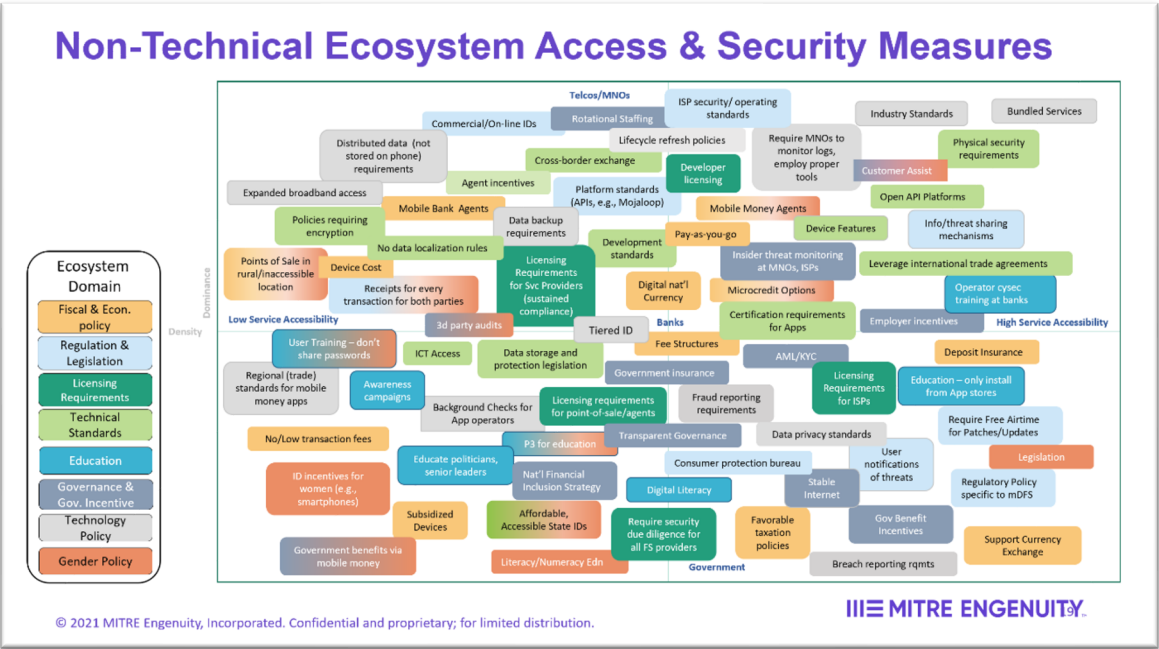


Figure 21: Policy and Governance Opportunities Mapped against National Context

identification credentials. The high service accessibility end of the axis represents a well-connected ecosystem plentifully supplied with points of service, whether in the form of bank or mobile money agents, on-device applications and the infrastructure to access them,

kiosks/ATMs, etc. Such environments also tend to offer fewer structural or policy barriers to women, although no country the team examined appears to offer truly equitable access.

The Y-axis represents a continuity of ecosystem influencers. One end of the axis is labeled “Government.” Ecosystems dominated by government typically have strong regulation, licensing regimens, taxation, or other policies that can incentivize or disincentivize mDFS services and associated security measures. The other end is labeled “MNOs/Telcos” and represents those ecosystems in which how mDFS services are offered and controlled is generally determined by non-government industry actors—typically MNOs, telcos, or in some cases social media entities or even small start-ups. Banks are situated in the middle of this continuum, as their role varies in different countries, where a strong national banking system may act as a de facto extension of government or where private or international banks function primarily as part of the commercial/investment landscape, governed by international banking sector guidelines more than national ones.

Each country—or in the case of very large, complex countries like India, each locality—comprises some blend of these factors: a subset of the range of service accessibility and a combination of ecosystem stakeholders with various levels and types of influence over the characteristics of the ecosystem, typically categorizable as one of the domains listed: fiscal and economic policy, legislation and regulation, licensing requirements, technical standards, education, governance incentives/disincentives, or technology policy. Gender policy is something of a special case, as it rarely stands alone but often manifests as an emergent quality of other domain cases. For example, a national identity system may function in such a way as to disproportionately exclude women; education and training systems may be oriented more toward men and boys; and/or laws or customs determining who may control money can drive women

toward certain kinds of financial services (e.g., unregulated mobile money apps/agents) over others (e.g., banks and SACCOs), where they have access to them at all.

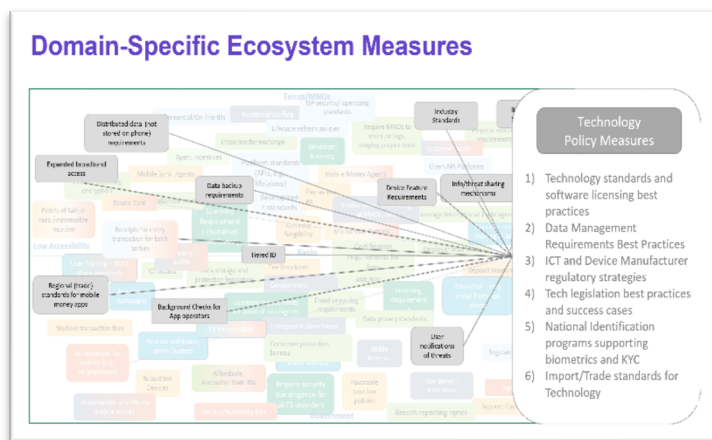


Figure 22: Filtering Non-Technical Factors by Policy Domain

6.3.2.1 Opportunities to Improve Ecosystem Security and Access (Governance/Policy)

As with the technical lens, non-technical policy/governance opportunities can be filtered by domain—Figure 22: Filtering Non-Technical Factors by Policy Domain shows a gender filter—this is the only

filter that combines with other factors, as seen in the color gradations, because although some countries may have gender-specific policies in some areas, it is more common that other types of policies have disparate effects on or outcomes for women, or offer opportunities to specifically address gender inequalities in how they are framed or implemented.

6.3.2.2 Applying the Policy/Governance Lens to a Country

As with the technical lens, the next step is to overlay a country on the policy/governance map. This can look quite different from the country mapping through the technical lens, because whereas a technical ecosystem tends to be relatively easy to characterize, a policy/governance landscape is less precise. As noted in some of the government examples earlier in this paper, countries frequently have broadly disparate access (a combination of isolated rural areas and densely packed urban areas), and their policies may be narrow and restrictive, broad and encompassing, or some of both. Similarly, their ecosystem may be strongly government-centric, dominated by industry in the form of telcos and social media platforms, or a volatile combination in which a many providers vie for control of users and policy with government regulators and/or banking sectors. Accordingly, on this map, each country bubble is centered approximately where its service accessibility “score” intersects with the relative dominance of particular actors in the ecosystem.

For example, in Figure 23: Mapping Countries by Policy/Governance Characteristics, the long, gray horizontal oblong notionally represents a country like India. It is centered in the “government-dominant” lower half of the chart, with just a little extension into the telco/MNO-dominated area. India’s government has taken an active role in mDFS, and entities interested in trying to further improve mDFS access and security there will need to work with them as the primary influencer in that ecosystem. On the “access” slider, it spans almost the whole spectrum, representing India’s mix of large rural areas with poor connectivity (though mobile device ownership is high) and its dense, sprawling cities. In the governance sphere, relatively few policies will work in both of those contexts. Nevertheless, because of its strong legal and policy foundation and its ability to directly influence major stakeholders such as banks and MNOs, India has a wide range of policy opportunities to draw from.

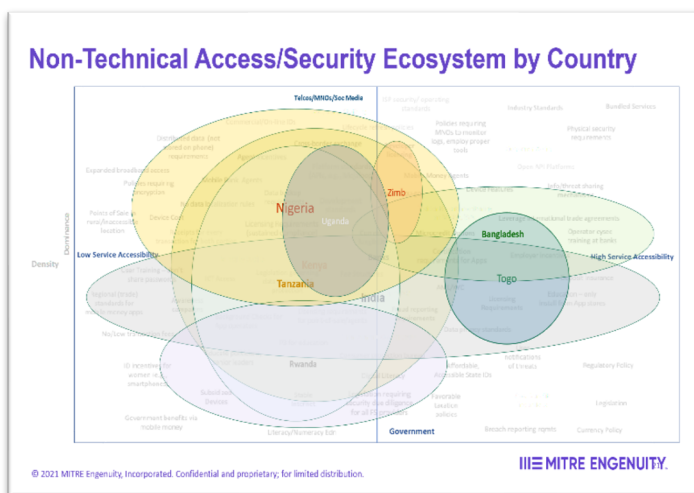


Figure 23: Mapping Countries by Policy/Governance Characteristics

Zimbabwe (the narrow orange vertical oblong), in contrast, has a narrow “service accessibility” range—indicating that most of the country falls in this range—centered in the high-access half of the map, thanks to having implemented an extensive fiber infrastructure more than a decade ago. Nevertheless, it has a very narrow policy opportunity coverage area because, although the ingredients for success are available, its government has clamped down on virtually all mobile money, accusing providers of undermining the national

currency and economy. That leaves very little maneuvering room for developing conducive policies or incentives, and suggests that would-be investors in the mDFS ecosystem would do better looking for non-government partners, such as telcos, to work with.

Finally, Togo is represented by a bubble that is disproportionately large, given the size of the economy. Considered a low-income country, its government has nevertheless actively pursued digitization, with mobile access of nearly 80% and a dominant MNO provider, Togocell. Among other efforts, Togo has deliberately incentivized the adoption of mDFS through government payments, and during COVID-19 lockdowns, it eliminated all mobile money fees in a push to get citizens to use mDFS. Though its record on internet freedoms is not stellar, it has consciously fostered a very large policy opportunity area through the establishment of mDFS-friendly laws and consumer protection regulations, which is reflected in the size of its bubble.

6.3.3 Combining the Technical and Non-Technical Lenses

As should be clear by now, neither the technical nor the policy/governance lens provides the whole picture of cyber risk and access equality with regard to mDFS. Rather, like a pair of 3D glasses, both lenses must be used together to get a clear picture.

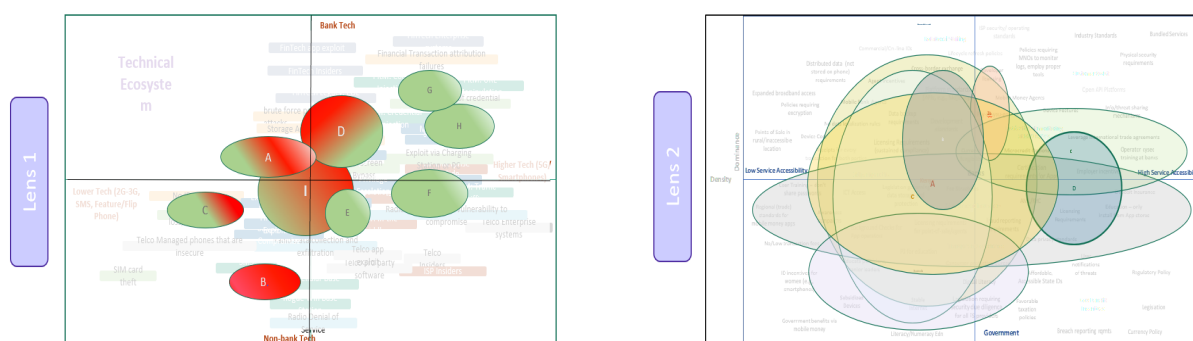


Figure 24: Combining the Technical and Policy/Governance Lenses to Identify Countries' mDFS Risk Mitigation Opportunity Space

Users of the mDFS Risk Model can use both lenses by mapping the country under consideration on both maps and then considering them together. Every country's technology-driven risk picture will present a certain subset of likely threats and associated technical mitigations. However, many countries will find that some of those mitigations are beyond their reach for various reasons—cost, complexity, expertise, etc. At the same time, their policy/governance opportunity space will suggest approaches that can make some mitigations more achievable, for instance by establishing standards, or provide ecosystem-wide security improvements that can obviate or substantially reduce whole categories of risks—for instance, a government-wide software purchase could bring several legacy systems up to date and ensure they are patchable—a top control for a myriad of risks. Other options in the policy space, such as user training or public awareness, can also help mitigate a wide number of threats, such as the many associated with phishing, fraud, identity theft, and so on.

Together, these two lenses provide a more complete picture of the “universe of solutions” to the problems of cybersecurity threats and insufficient or unequitable digital inclusion in the context of mDFS. It is hoped that users of the model will employ it to make wise, context-informed investment decisions aimed at improving the economic situation of the poor and financially underserved.

7 Framework Validation and Key Stakeholder Interviews

To validate its approach, MITRE Engenuity is conducting open-source research on several countries representative of various aspects of the framework (various governance approaches, fiscal/economic policies, technology landscapes, experience with mobile money or digital currencies, use cases, etc.). This step will provide insights to further refine the model, in addition to identifying high-level recommendations for improving the security and access to these countries’ mDFS ecosystems. Each of the countries is representative of a unique set of factors that make it an interesting test case. Recommendations suggested by the model will be presented in a separate report.

- **Bangladesh** provides an Asian example with low governance capacity, a tendency toward restrictive regulation, and a predominantly rural problem set. It also offers the example of bKash, a bank-centric, government-licensed mobile money that has reportedly been very successful in increasing financial inclusion.
- **Kenya** was selected because it has long been the most successful of Africa’s mobile money adopters—it provides an opportunity to identify success factors and lessons learned. It is also at the higher end of the technology spectrum, with a rapidly growing number of 4G/smartphone users and a very broad array of use cases.
- **Nigeria** is an important African case, with its exploding population and large urban centers. It is a hotbed of fintech start-ups and investments, and is also a hub of cybercrime in Africa.⁶⁷ It has basic technology and regulatory/policy capacity in place, but is still in transition with significant room for both technological and governance improvements. Its government has pursued policies that are both positive and negative for the development of a strong mDFS ecosystem, establishing policies that aim to promote a vigorous tech start-up environment while at the same time attempting to block technologies of which the government does not approve, including cryptocurrencies. Women entrepreneurs play a particularly strong role in Nigeria—an opportunity to examine the role mobile money can play in increasing financial inclusion and security. Finally, in 2021, Nigeria became the first country in Africa to go public with plans for a blockchain-based central bank digital currency (CBDC), the eNaira,⁶⁸ which aims to improve financial inclusion but which has also raised concerns about privacy, the future of other popular decentralized mobile currencies and of the brick-and-mortar banking industry in the country, and the possibility of introducing additional cyber vulnerabilities into Nigeria’s central bank system.⁶⁹ Nigeria’s technology and policy choices will determine the success of this effort, making it a good case study for this model.
- **Rwanda** has the highest GSMA Mobile Money Regulatory Index score of any country we researched, and a mobile phone and smartphone penetration similar to that of Kenya.

It offers an example of a country with a very high demonstrated commitment to an mDFS ecosystem but relatively low capacity overall. It also offers unique use cases, such as a government-endorsed mobile money system (Tigo-Pay) that it has extended to SACCOs. During the COVID-19 pandemic, the government incentivized mobile money usage by eliminating fees, providing an opportunity to examine the impact of such policy options.

- **Tanzania** was selected because, like Kenya, it has a strong M-Pesa presence and supportive government policies, with an even higher GSMA Mobile Money Regulatory Index score (indicating favorable policies) than Kenya's. It has only a fraction of the mobile phone penetration that Kenya does, however, and different use cases predominate. Its mobile money adoption curve has been flatter than any other country in M-Pesa's sphere, providing an opportunity to examine what factors made the difference.
- **Uganda** has an MTN-based GSMA-compliant national mDFS solution in place, a moderate Mobile Money Regulatory Index, a good underlying regulatory regime, and moderate literacy. But though its government has expressed strong interest in a digital economy and financial inclusion, it has put policies in place that seem to work against a vibrant system, including internet shut-downs, surveillance, and punitive tax policies.

The results of this effort will be presented in a separate paper upon completion of the pilot phase, which will apply the model to each country and explain where each fell on the 2x2 threat and opportunity quad charts, the specific threats and technical mitigations their positions suggest, and recommendations for improvements that reflect their policy/governance context.

8 Recommendations for Stakeholder Engagement

Interested entities such as NGOs or international development advisors might use this model to assess and engage a particular nation of interest in the following areas:

- **Risk Landscape Description:** The model can be used to describe those aspects of the pilot country's ecosystem that locate it in a particular quadrant of the mDFS Risk Management Model quadrant visualization—its network/device technology landscape and primary attack targets—and its service accessibility and dominant stakeholder context. As described above, these factors are used together to help governments, NGOs, and other investors interested in expanding/improving secure access to mDFS determine what efforts are likely to produce the greatest impact—by threat domain/ecosystem segment if desired—in both the technology and the policy/governance arenas.
- **Key Stakeholder Identification:** For entities outside the country, application of the model can also help identify which stakeholders it may be most effective to work with—government, MNOs/telcos, social media or other mobile money providers, device manufacturers, banks, etc.
- **Technical Risk Mitigation Recommendations:** Recommendations for technical risk mitigations for specific components of a particular technical ecosystem can be presented through threat domain filters—that is, recommendations focused on host networks, device hardware/software, ISPs, etc. These recommendation will typically be most pertinent to the stakeholders responsible for those network segments (such as device

manufacturers, app developers, network operators, etc.), or those that oversee/support/regulate them (licensing and standards bodies, certification entities, etc.).

- **Policy/Governance Recommendations for Risk Mitigation:** Non-technical recommendations can be presented by stakeholder (e.g., financial services regulators, telco regulators, appropriate ministries, legislators, regional trade or standards organizations, etc.) and/or through the ecosystem domain categories in the model: fiscal policy, technical policy, regulation and legislation, licensing, inclusion policy/impacts, education, and governance/incentives.

9 General Recommendations for Improving National mDFS Ecosystem Access and Security

Security and access are closely related concepts in any digital undertaking—identity and access management is one of the most fundamental cybersecurity tenets, and the ability to ensure that data and services are available to those who need them (and only those who need them) is one-third of the confidentiality/integrity/availability cybersecurity triad. Addressing both aspects effectively requires a focus on both technical and governance measures that, as noted above, vary by context. Nevertheless, certain foundational approaches are broadly applicable. Accordingly, in researching this very complex arena, the MITRE Engenuity team identified a number of best practices from various technical sources and our own experience in international cyber capacity building that can be offered to countries as a generic list of approaches for improving both security and access for mDFS in emerging economies. This list emerged from observations about how the technology and policy/governance aspects of national ecosystems relate, as described in the model, and will grow as the model is validated and used.

9.1.1 Improving Cybersecurity of mDFS

As noted in Serianu’s Africa Cyber Security Report 2017, no investment in high-tech security controls will improve the cybersecurity posture of a weak security architecture. For example, the authors of that report noted that successful ransomware attacks in that year were mostly the result of failure to patch known vulnerabilities.⁷⁰ Similarly, in the first quarter of 2017, Kaspersky Labs blocked 51 million user attempts to open a phishing website, 20% of which targeted banks or other financial services organizations—a user awareness weakness in these users’ organizational security postures.⁷¹ Improving the cybersecurity of mDFS is a core objective of the MITRE Engenuity model. Recommendations (some of which are already in work in various programs) for improving mDFS security architectures across the board include:

- Require bank and mobile money agents to receive cybersecurity awareness training and be periodically audited—a cost that providers should be able to easily bear, according to the Boston Consulting Group’s study, which found that providers typically make a 12% profit from each agent, with a return on adding a new agent (including any training, monitoring, marketing materials, etc.) in nine months.⁷²

- Implement a security standard, such as the GSMA certification, and require mDFS providers to comply.
- Implement end-to-end encryption where networks will support it.
- Implement laws banning SIM card swapping, along with procedures to identify and prosecute it when it occurs.

9.1.2 Improving mDFS Usage through Trust

Several factors affecting the relative trustworthiness of mDFS in various contexts arose in Engenuity’s research. These factors are identified below, with associated best practice recommendations.

- Trust factor: Reliable access to internet and mobile money transaction-related applications
 - Internet availability should not be subject to political control, particularly where people depend on it for essential services. Where internet shut-downs are likely, users cannot rely on being able to access mDFS. Some governments restrict access to particular applications that may support mobile money transactions—particularly social media applications—or disincentivize digital access in general, such as by taxing data packets.^{xii}
- Trust factor: Government surveillance and taxation
 - Thoughtful regulation of DFS to ensure transparency, access, affordability, and consumer protections can improve trust.
 - Over-regulation of mobile money can hinder DFS development efforts. Mobile money, though not necessarily under the control of a government, can have substantial positive impacts on economic development and expansion.
 - Mobile money transactions should have the same level of personal data protections afforded to other sensitive information, such as health records. The European Union’s GDPR is becoming an international standard for privacy protections.
- Trust factor: Cost
 - Eliminate user fees, at least at some (such as SACCO- or bank-operated) kiosks, or for some number of transactions per month. Because many users’ average transactions are low-value, fees can be prohibitive. A USAID study in Rwanda found that the elimination of fees on mobile money transactions during the COVID-19 pandemic dramatically increased usage, which dropped off again in favor of cash when the fees were re-instated.⁷³ When such fees are eliminated, MNOs will continue to make money on their airtime and other services, and on merchant/agent fees, and

^{xii} In 2018, Uganda established a daily tax of 200 shillings (established in 2018) on users of social media applications designed to reduce “rampant rumor-mongering.” Internet usage dropped 30%. In 2021, the government replaced that tax with a more general internet usage tax of 12% on data packets, on top of an 18% value added tax (VAT). SOURCE: Stephen Kafeero, “To Control Speech, Uganda is Taxing Internet Usage 30%,” *Quartz Africa*, July 3, 2021, online at: Uganda replaces OTT social media tax with tax on internet bundles — Quartz Africa (qz.com).

banks will continue to profit from interest and merchant charges, but mobile money itself will become a differentiator for attracting customers, rather than a profit center.

- Trust Factor: Security
 - Mobile Money applications should be certified and licensed. The GSMA Mobile Money Certification Model follows eight principles aligned with international best practices and provides a framework to guide new app developers.

10 Recommendations for Stakeholder Program Planning to Improve mDFS Security and Access

This section provides a set of recommendations that combine technical and non-technical best practices and security/access approaches that the MITRE Engenuity model suggests are general insights that are broadly applicable to developing economies and mDFS ecosystems, starting with a list of general “desirable” practices and system characteristics that can help establish the foundation for a more secure, accessible, and equitable mDFS ecosystem. The approaches listed here are representative of the kinds of recommendations this model will produce in contexts where the relevant factors apply (where they do not apply, it is likely either the technology base is not yet available—such as to support multi-factor authentication—or similar measures are already in place).

- Desirable financial inclusion policies
 - Promote policies to improve basic education—particularly for girls, in those areas where their participation in education is limited—focused on literacy/numeracy, but including basic digital skills such as protecting personal data. Such education enables users to more effectively understand and use mDFS security features such as transaction reports and receipts, strong passwords and PINs, etc.
 - Encourage youth interest in technical pursuits through information campaigns that show the role of digital technologies in “normal” economic activities such as retail, tourism, selling manufactured goods, paying bills, operating a personal business, etc.
 - Identify any government payments, such as salaries, benefits, assistance payments, etc., and offer a phone and a one-hour training session as incentive to receive those payments on a mobile device. This can also particularly expand women’s ownership of mobile devices by associating them with individuals’ paychecks, while providing an opportunity to deliver basic security awareness training verbally and in person.



Figure 25: GSMA Mobile Money Certification Principles

- Incentivize full participation in national identity programs (women in particular often have less access to such programs) through government initiatives, community programs, religious organizations, NGO programs, etc., and by removing barriers such as fees, travel restrictions, access to registration points during times working people can meet, etc. Apply Tiered Identity Verification approaches such as affidavits or sponsorship to help people without basic identity documents like birth certificates or proof of address. Identity verification is key to both security and access to digital financial services.
- Desirable mDFS app characteristics (may be required in licensing regimens)
 - Multi-factor authentication (reduces fraud)
 - Biometric ID (reduces chance of ID compromise—not compatible with flip phones)
 - Receipts (reduce point-of-service fraud)
 - One-time PINs for access without phone (shared phones)
 - SIM card based (allows one phone to access multiple accounts, expanding access and making it easier to protect individual PINs)
- Desirable mDFS system characteristics
 - Mobile money currencies available through applications that meet GSMA Mobile Money Certification requirements
 - Agent training and audits—for both security and transaction integrity
 - Distributed/cloud-based ledger
 - Objective/outside audits of business processes, including security
 - Encryption at rest
 - Receipts required to be available for both parties in a transaction
 - Government or provider insurance against fraud or service provider negligence
 - For CBDCs, data privacy guarantees in law
 - Strong anti-cybercrime and anti-fraud laws, and a sufficiently trained regulatory, law enforcement, and judiciary cadre to enforce them

Further recommendations in the sections below build on recommendations from the AFI Cybersecurity Guide for Financial Services and MITRE’s International Cyber Capacity Building Framework and experience.

10.1 Regulation, Compliance, and Reporting

This section describes best practices for improving compliance with cybersecurity and digital access/privacy regulations, policies, and laws.

- Regulators should require transaction quality oversight by FSPs and frequently assess factors such as security and availability, particularly for those that incur additional risk by relying on USSD/SMS for transactions.

- Apply data management and privacy requirements to any personal or confidential data shared by FSPs with regulators.
- Compare suspicious transaction reports among financial sector entities to identify significant patterns that could suggest systematic fraud.
- Require cybersecurity training for FSP staff, including authorized FSP agents, and for regulatory officials and auditors.
- Establish penalties in law for non-compliance by FSPs.
- Require FSP reporting of data breaches, and ensure appropriate entities (such as a national CSIRT or financial/retail CSIRT, or an international or private sector information sharing partner) publicize the information for the public and constituents, and warn other regulated entities of the attack.
- To incentivize better cybersecurity among FSPs, liability for losses should be assigned to the FSP, which must refund it promptly to the customer (if subsequent investigation indicates it was deliberately caused or facilitated by the customer, the refund can be reversed). This rule may require FSPs to hold a reserve of funds for the purpose of making timely refunds.
- FSPs and MNOs should have arrangements in place to restrict SIM card swaps to verifiable authorized users, and swaps should be disabled for SIMs that belong to prominent individuals whose phone numbers may be known, or for FSP agents and employees who may have privileged account access, unless approved and documented by FSP and MNO senior management. Multiple SIM swaps against a single account within a short period should be disabled.
- FSPs, including, but not limited to, MNOs, should be required to report incidents to any national Cybersecurity Operations Centre (CSOC), Computer Emergency Response Team (CERT), or Cyber Security Incident Response Team (CSIRT) that may be established with oversight of financial sector cybersecurity, and to participate in incident response activities.
- Additional specific controls recommended by the Alliance for Financial Inclusion for FSPs and MNOs, which could be addressed in regulation, can be found in the AFI's *2019 Cybersecurity for Financial Inclusion: Framework and Risk Guide*.⁷⁴

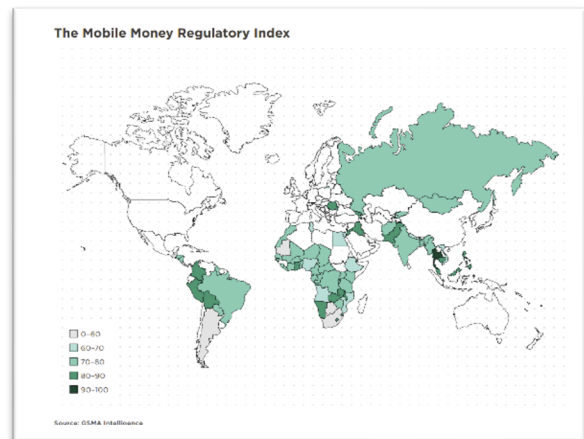


Figure 26: GSMA Mobile Money Regulatory Index Showing Degrees to Which Countries' Regulatory Frameworks Support Mobile Money Development

10.2 Customer Identity and Privacy

This section addresses general best practices in identity and data protection that apply to mDFS.

- FSPs should offer educational programming for customers with limited digital or financial literacy focused on steps they can take to protect their identity, personal data, and transactions.
- All FSPs should subject customers to a robust identification and verification process, understanding that not all customers will have access to the same levels of credentials. A tiered documentation system ranging from a single item, such as a voter ID card, up to full identification, such as a passport, biometric ID, proof of residency, and an established digital footprint, could enable individuals to participate in financial services at different trust levels, with different constraints regarding balance limits, number and size of transactions, creditworthiness, etc.
- The FSP should provide tools to the customer, such as PINs for low-value transactions or multi-factor authentication or biometric protocols for larger-volume or cumulative threshold-crossing transactions.
- FSP-collected data should be encrypted, and not disclosed to anyone but the customer and authorized FSP staff.
- In over-the-counter transactions, all parties—the sending and receiving customer, and the sending and receiving agents—must be properly identified, and receipts provided to the customers that those with limited financial literacy can verify with other trusted individuals.

The Alliance for Financial Inclusion (AFI) notes that where identity programs are weak, unaffordable, or inaccessible, FSPs could consider offering services to individuals without formal identification whose identities are vouched for by a customer who does have such credentials, with careful government oversight and the understanding that if the attesting customer should come under investigation for any criminal finance-related issue such as fraud, money laundering, or links to terrorism, the customer(s) for whom they vouched will have all accounts similarly suspended.

10.3 Technical and Policy Controls to Protect Transactions

This section addresses best practices toward mitigating common security threats to the integrity of mDFS systems and transactions.

- There is a high risk associated with USSD/SMS transactions, which is created by a lack of security protections from the user’s handset to the network provider that may allow hackers to eavesdrop on account transactions and PINs—including one-time PINs. FSPs should put active transaction monitoring capabilities in place to identify and stop fraudulent transactions. Such monitoring need not focus on individual transactions that could violate privacy protections, but rather on patterns of transaction activity known to be associated with fraud.
- Localities, in partnership with network operators, should actively work to accelerate migration away from USSD/SMS systems. Government incentives, removal of barriers such as fees, and investments in broadband connectivity can help.
- As smartphones and broadband networks come into broader use, FSPs should use appropriately secured apps, ideally with biometric or other non-PIN-based identify

verification, end-to-end encryption (including of the app itself, to prevent reverse-engineering), data obfuscation, and distributed cryptographic keys.

- The AFI recommends FSP smartphone apps be developed to operate in the smartphone's sandbox to make use of the device's Secure Execution Environment, and should not operate if the operating system does not support the required level of security or if the phone has been jailbroken.

10.4 Securing Financial Service Providers

Some best practices for general technical and process improvements to DFS security include the approaches listed here. Because many of the proposed mitigations are not technology specific, the costs and ROI for implementation will vary depending on the organization's budget, personnel skillset, capability available, and priorities for different cyber risks.

- **Technical mitigations (ATT&CK):** The dataset includes 54 technical mitigation recommendations for the different domains (41 in ATT&CK for Enterprise and 13 in ATT&CK for Mobile) that offers threat-informed technical guidance that is abstract and vendor agnostic, has little overlap, and in some instances provides specific safeguards.
- **Threat-informed cyber policy (security controls):** With collaboration from the Center for Internet Security and JP Morgan, MITRE's Center for Threat Informed Defense recently published a mapping of security controls from NIST's (SP) 800-53 to MITRE's ATTACK framework.⁷⁵ The guidance found in NIST's (SP) 800-53 establishes a comprehensive set of safeguarding measures that could be used to baseline the security posture of different types of computing platforms (e.g., cloud based, mobile device, communication systems, and system-of-systems). This research mapping provides organizations with the ability to prioritize security controls based on the perceived threat risk. When implemented appropriately, these security controls limit the damage and improve the overall system's cyber-resiliency from attackers.
- **Cyber exercises** allow organizations to assess in a tabletop format the operational impact and business consequences from simulated red-team scenarios against deployed technologies.⁷⁶ Similar to hands-on penetration testing reports, the benefits from these cyber exercises are used to identify gaps in compliance, improve intrusion detection, harden compute resources, optimize the security posture, and prioritize risk investments. Cyber exercises can also be used to practice and improve Incident Response and Disaster Recovery procedures, identify defensive gaps, etc.
- **Advanced security assessments** are designed for organizations that want to validate or further optimize their security posture beyond fundamental cybersecurity practices.
 - **Third-party security assessments:** As financial institutions attempt to reach a broader consumer base with websites or mobile applications, they increase their digital footprint while adding vectors to the attack surface. Bug bounty programs are examples of third-party independent assessments that crowdsource the discovery of critical security gaps in the organization's lines of code (e.g., mobile apps, website, smart contracts). The software vulnerabilities are often mapped to MITRE's

CWE/CVE knowledge base, and payment rates are proportionate with the impact from the discovered software vulnerability.

- **Automated security assessments:** MITRE’s Caldera⁷⁷ is an example of modern-day automated red-teaming tools that allow individuals with a limited cyber skillset to emulate advanced persistent threat techniques and discover security vulnerabilities in enterprise computing resources.

10.5 Investing in the Workforce

Many countries that might be interested in implementing the recommendations that may be suggested by the application of this framework will be unable to do so because of systemic shortfalls in trained cybersecurity workforce, to include tech-savvy policymakers and their advisors. A key component of any long-term cybersecurity capacity building approach is the expansion of a digitally literate workforce, both to enable implementation of such policies and approaches and to reduce the overall public risk through awareness and better practices. Such programs ideally start at the primary and secondary school levels, and build on strong literacy and numeracy education to focus on cyber fundamentals such as online safety and the protection of personal information, and also address new workers and re-skillers through affordable, accessible hands-on programs such as apprenticeships, accredited certification programs, etc., that address the specific skills needed (not that such skills do not typically require a four-year or other university degree) in the ecosystem. Public-private partnerships between government and industry can create programs tailored to particular economies and major industries, including financial services, and target historically underutilized but economically significant groups such as women and girls.

10.6 Regional Solutions

The AU Convention on Cyber Security and Data Protection, African Continental Free Trade Agreement, ASEAN, ECOWAS, and other regional organizations offer opportunities to standardize regulatory measures and cooperate on raising awareness and countering cybercrime.

Summarized Findings Report – What are Cybersecurity Gaps in Africa?
*Reporting approach adopted from cyberroad-project and survey




Theme	Scenario	Consequence(s)	Mitigation	Identified Gap(s)
 Database Security	Limited visibility on activities on the databases.	1. Fraudulent database postings! 2. Loss of sensitive information!	Continuous monitoring of activities within databases. Limit and monitor access to database. Audit and review privileged access to DB.	How can African companies improve visibility on DB activities at a cost effective and resource friendly manner?
 Privileged User Management	Compromised administrator accounts.	Unauthorized access to critical systems within the organizational	Audit the activities of privileged users within the network.	How can organisations implement segregation of duties when resources (staff) are limited?
 Patch Management	Missing patches contribute 70% of vulnerabilities identified. 60% of these are never mitigated. Employees are trained only after an incident.	Exploitation of missing patches to compromise confidentiality, integrity and availability of critical informational assets! Employees fall victims of social engineering attacks!	Remediation roadmaps that ensure that critical patches are applied while medium and low risk vulnerabilities are fixed within a stipulated agreed upon period. Regular employee training programs that have an effectiveness measuring metric.	How can African organisations maintain a patch management program without exhausting resources? How can organisations ensure employees understand the concepts taught during awareness workshops and trainings?
 Training and Awareness	IT Training is done on specific tools. Board members lack cyber security expertise and rely on standard audit reports to understand the security posture of organisations.	IT teams lack the expertise for defensive and offensive security! Lack of visibility on actual cyber security posture! No standard way of measuring progress and ROI on IT investments!	Regular training on both defensive and offensive cyber security concepts. Board training to involve reporting metrics for enhanced visibility that can provide a basis and guide on future decision-making.	How can IT teams transform from being "tool analysts" to network engineers and architects? How can Board members understand the concepts taught during awareness workshops and trainings?
 Network Security Engineering	Limited expertise in the country on Security Architecture/Engineering skill set.	Networks are misconfigured to allow easy manipulation and system sabotage!	Organisations to invest in or outsource security engineers/architects for network design purposes.	Where can organisations get specialised training on security architecture and engineering?

Figure 27: Cybersecurity Gaps in Africa (Serianu)

As the research section of this paper noted, while there are risks associated predominantly with banks—especially unregulated local banks and SACCOs—most of the security risks surrounding mDFS are the same as those surrounding digital services and mobile devices in general, and most could be remediated through basic cybersecurity best practices. Figure 27: Cybersecurity Gaps in Africa (Serianu) shows Serianu Ltd.’s assessment of the largest cybersecurity gaps in Africa in 2017 and their remediations. Together, they boil down to access management, secure configurations and patching, and awareness. But as that report also suggests, countries below the “cybersecurity poverty line” do not have enough cybersecurity professionals to implement even these foundational programs in their organizations. On the contrary, the overwhelming demand for digital services combined with the severe shortage of cyber professionals incentivizes poor practices and shortcuts such as cheap software products, common administrator accounts, and backdoors.⁷⁸

Regional organizations can improve risk management approaches by eliminating the need for individual countries to create and sustain their own stand-alone regulatory solutions. Regional technology standards can not only improve cross-border transaction ease and security by establishing operating and security requirements for licensing, but can help resource-constrained governments by pooling subject matter experts, including for combatting cybercrime. Common technology standards also ease the development of appropriate training programs and allow parts of governments, such as ministries of education, to share curricula and best practices. One interesting example of regional regulatory regimes is the West African Police and Security Chiefs Commission (WAPCCO), which has established a new type of oversight agency focused specifically on the digital economy, including mobile money regulation.⁷⁹

11 Open-Source Cyber Risk Model Tool

MITRE Engenuity is building an open-source interactive application that captures data and research from this mDFS cyber risk model. Users will be able to select key model inputs based on technology maturity and connectivity, as well as political/governance characteristics of specific countries. In response to these inputs, the software application will identify key technical threat vectors and associated technical mitigations, as well as non-technical opportunities to lower risk and improve overall ecosystem security. The application’s output is intended to empower stakeholders and aid in programming decisions by providing data-driven assessments of what technology and/or policy investments may be most effective and sustainable within an overall technology-governance context, or even within a particular ecosystem segment (such as platform development or network modernization), while also highlighting governance/policy approaches that may enhance or hinder programming sustainability.

12 Avenues for Future Research

This section lists ideas that were prompted by but not included in this model development effort, which may warrant further pursuit:

- Demand for fewer in-person interactions has opened up mDFS opportunities. Has it also opened new avenues of attack?
- Various contingencies will affect threat modeling—pandemics, conflict, natural disasters, etc. How might these be anticipated in ecosystem development?
- Onboarding of new technologies or platforms triggers regulators to think they are opening their door to money laundering and fraud. Is this an issue? If it's not where the threats really are, how do we convince regulators to be more open?
- There is room for large mega bodies to be running parts of the DFS ecosystem. What might those be, and how could they be established?
- How can we bring in basic tools to go along with transparency (i.e., “CISO In A Box” or “CSIRT In A Box” packages)?

13 Conclusion

The development of MITRE Engenuity's mDFS Dynamic Risk Management Model presented numerous challenges in technical and policy complexity, and in reconciling and combining several disparate threat, defense, and capacity building approaches into a single model. Our team can apply these recommendations to a specific use case or a broad set of use cases for any organizations interested in proposing pilot work to enact an applied set of recommendations.

With the development of the automated user tool, a wide variety of stakeholders can examine different aspects of the mDFS ecosystem through the lens of a particular national context to aid in investment and policymaking decisions. Some examples of the types and levels of planning this model can support include:

- **Tactical/Technical:** Financial technology stakeholders, engineers, and developers can apply this model to extract the technical risk and communicate impact of key cyber resources for secure and reliable operations.
- **Operational/Production:** The end user is often the least aware of cybercrime yet the most targeted in the ecosystem. This model can be used to help improve cyber risk awareness in the conduct of peer-to-peer or peer-to-business payment transactions for industry or government stakeholders.
- **Strategic:** Governments, NGOs, and investors are examples of stakeholders that could use this model to make decisions about how best to improve accessibility, reliability, equity, and security in the mDFS ecosystem, or to overcome the challenges of cybercrime through regulations and investment in key areas (e.g., CERT, law enforcement, etc.).

- **Business:** Industry can apply the model to ensure investments in digital development are wisely implemented with security integrated into the approach up front, or as a way to reconcile breaches and lost revenue where a system needs to be improved.

In addition, we believe examining cyber ecosystems through two context-sensitive lenses can be applied to assist decision-making in other cybersecurity-related sectors such as health services, maritime or other transportation sector security, and others. We look forward to demonstrating the effectiveness of this dynamic risk management approach in approaching other complex problems.

14 References

Aditi Kumar, Jeremy Ney, Eve Lee, Victor Ji, “National Digital Currencies: The Future of Money?” Harvard Kennedy School Belfer Center for Science and International Affairs, Updated September 2020.

Alex Scroxton, “Bill Gates Backs CREST FinTech Security Scheme for Africa and Asia,” ComputerWeekly.com, March 9, 2020.

Alliance for Financial Inclusion, *Cybersecurity for Financial Inclusion: Framework & Risk Guide*, Guideline Note No.37, October 2019.

Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar, Jake Hess, *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, World Bank, Washington, DC, 2018.

BBC News, “\$10 router blamed in Bangladesh bank hack”, April, 2016, <https://www.bbc.com/news/technology-36110421>

C. Diaw, “Gender and Education in Sub-Saharan Africa: The Women in Development (WID) Approach and Its Alternatives,” In: Abdi A.A., Cleghorn A. (eds), *Issues in African Education*. New York, Palgrave Macmillan, New York, 2005, https://doi.org/10.1057/9781403977199_10.

Center for Strategic and International Studies, “Economic Impact of Cybercrime – No Slowing Down,” McAfee, Washington, DC, 2018.

Dante Disparte, “Could Digital Currencies Make Being Poor Less Costly?” *Harvard Business Review*, August 5, 2020.

Darren Parkin, “Facebook’s Libra White Paper in Full,” Coin Rivet, Yahoo Finance, June 18, 2019.

David Fox, Catherine D. McCollum, Catherine D., Eric I. Arnoth, Darrell J. Mak, “Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context,” Homeland Security Systems Engineering and Development Institute, August 29, 2018.

David Fox, Eric I. Arnoth, Dr. Clement W. Skorupka, Catherine D. McCollum, Deborah J. Bodeau, et. al., “Next Generation Cyber Infrastructure APEX Program,” The MITRE Corporation, November 2018, <https://www.mitre.org/ngci>.

Fiacre Kakpo, “Togo: Mobile Money Drives Financial Inclusion, According to World Bank,” Mobile Money Africa, January 26, 2018, www.TogoFirst.com.

Global System for Mobile Association (GSMA), *GSMA Mobile Money Certification Guide*, Mobile for Development, GSM Association, August 2020.

GSMA, “Mobile Money Certification Principles,” *The Mobile Money Certification*, GSM Association, 2019.

Hung Tran, Barbara C. Matthews, “China’s Digital Currency Electronic Payment System Reveals the Good and the Bad in Central Bank Digital Currencies,” *The Atlantacist*, The Atlantic Council, August 24, 2020.

Ian Hall, “Nigeria Becomes First Country in Africa to Launch CBDC,” Global Government FinTech.com, October 25, 2021.

INTERPOL, “Mobile Money and Organized Crime in Africa,” INTERPOL, June 2020.

Isaac Dachen, “Nigeria Ranks 3rd in Cyber Crimes Rating Globally,” Pulse.ng, August 23, 2017.

J.V. Owens, “Digital Financial Services, Regulations, and Financial Inclusion: Where Are We Headed?” Digital Financial Services for Development, Alliance for Financial Inclusion, posted online October 30, 2014.

Laura Silver and Courtney Johnson, “Internet Connectivity Seen as Having Positive Impact in Sub-Saharan Africa,” Pew Research Center, October 9, 2018.

Mark Flaming, Claudia McKay, Mark Pickens, “Agent Management Toolkit: Building a Viable Network of Branchless Banking Agents Technical Guide,” Consultative Group to Assist the Poor (CGAP), Washington, DC, 2011.

Mercyline W. Kamande, Anna C.R. Kamanzi, Alice W. Kituyi, Farah Qureshi, “Exploring the Use of Mobile Money Services among Tea SACCOs in Rwanda,” *Rwanda Mobile Money Report: Challenges and Opportunities*, USAID, 2020.

Olumide Adesina, “Nigeria’s CBDC: The Good, the Bad, and the Ugly – The Possible Impacts of an eNaira on Financial Inclusion, Privacy, and Decentralized Crypto,” Coinspot.com, August 31, 2021.

Oscar Lopez and Ephrat Livni, “In Global First, El Salvador Adopts Bitcoin as Currency,” *New York Times*, September 7, 2021.

Quartz Africa, “Internet Shut-Downs in Africa Were More Frequent and Lasted Longer in 2019,” posted online January 9, 2021.

Serianu Ltd., “Africa Cyber Security Report 2017: Demystifying Africa’s Cyber Security Poverty Line,” The Africa Cyber Immersion Center, 2018.

Shalini Unnikrishnan, Jim Larson, Boriwat Pinpradab, Rachel Brown, “How Mobile Money Agents Can Improve Financial Inclusion,” Boston Consulting Group, February 2019.

Simone Di Capri, “Mobile Money for the Unbanked: Enabling Regulatory Solutions,” GSMA Mobile Money for the Unbanked, February 2013.

Stephen Kafeero, “To Control Speech, Uganda Is Taxing Internet Usage 30%,” Quartz Africa, July 3, 2021.

United Nations Secretary General Fintech Subgroup on Cyber Security (UNSGCS), “Briefing on Cybersecurity, UNSGSA Fintech Sub-Group on Cybersecurity,” United Nations, UNSGSA Queen Máxima, June 1, 2018.

Appendix A Other Frameworks and Guides Applicable to mDFS Cybersecurity

The Alliance for Financial Inclusion has compiled a list of existing frameworks that can be used to help develop and establish appropriate cybersecurity standards for financial service providers, briefly summarized here.

NIST

The NIST Cyber Security Framework (CSF) is often the starting place for organizations seeking to improve their cybersecurity. However, it is quite general, and must be significantly tailored to fit the needs of FSPs. NIST is developing sector-specific profiles, including for the financial services sector, which should be helpful.

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) developed a cybersecurity self-assessment tool in 2017 based on the NIST CSF, aimed at helping financial institutions identify their risks and to provide them with a repeatable, standardized process to measure cybersecurity improvements over time. The FFIEC approach has been widely influential, including on the European Central Bank's CROE (see below).

CPMI-IOSCO

The Committee on Payments and Market Infrastructures (CPMI) at the Bank for International Settlements (BIS) collaborated with the International Organization of Securities Commissions (IOSCO) to develop its "Guidance on Cyber Resilience for Financial Market Infrastructures" in 2016. Though focused on a nation's complete financial market infrastructure, it is based on a set of principles focused on addressing dynamic cybersecurity threats to critical systems and services, and is intended to supplement more IT-focused cybersecurity guidance with resiliency approaches that go beyond IT.

CREST

CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST provides internationally recognized accreditations for organizations and professional-level certifications for individuals providing penetration testing, cyber incident response, threat intelligence, and Security Operations Centre (SOC) services. Working alongside the UK central Bank, CREST has developed a framework to deliver controlled, intelligence-led cybersecurity tests that replicate the behaviors of threat actors assessed by government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions.

ECB CROE

The European Central Bank’s (ECB’s) 2018 “Cyber Resilience Oversight Expectations for Financial Market Infrastructures” (CROE) draws from several international approaches, including CPMI–IOSCO, NIST and FFIEC to assist supervisory/ oversight authorities. It provides assessment guidance that bridges security standards and the processes financial institutions must have in place to comply with them, in a way that is adaptable to the cybersecurity maturity of the institution being audited.

FSSCC Cybersecurity Profile

The US’s Financial Services Sector Coordinating Council works collaboratively with US government agencies to protect the US financial sector from cyber and physical incidents. Based heavily on the NIST CSF and the CPMI-IOSCO Guidance, and mapping to ISO/IEC 27001/2 controls, its 2018 Cybersecurity Profile (CSP) was developed in part to harmonize piecemeal regulations and frameworks that provided only partial or arbitrary guidance. It offers assessment questions that take a comprehensive pan-sector approach based on relevant supervisory guidance and frameworks. However, as the AFI notes, it was developed in and for the US financial sector, which is not necessarily representative of the capacity of smaller financial institutions or sectors, particularly those in emerging economies.

The Center for Internet Security “CIS 20” Controls

The CIS 20 is an IT cybersecurity, rather than a principles-based, framework. It takes a “bottom-up” approach to cybersecurity that many organizations find very useful. In its latest iteration, it includes implementation tiers, starting with the most foundational cybersecurity considerations, that can be applied as organizations mature. The guidance popularly known as the “CIS 20 Controls” (the most recent edition has 18) includes a set of cybersecurity controls and guidelines that together address the most foundational cybersecurity needs of the majority of organizations, including those in the financial sector. These are also mapped to the NIST CSF so that practitioners can cross-reference, tailor, and/or expand on them to meet their specific needs.

Other guides and frameworks relevant to the mDFS ecosystem include:

GSMA Mobile Money Certification Guide⁸⁰

Launched in 2018, the GSMA Mobile Money Certification is “a global initiative to bring safer, more transparent, and more resilient financial services to millions of mobile money users around the world.” It is the result of a three-year collaboration between the GSMA and the mobile money industry in Africa, Latin America, and Asia to understand best practices in these markets. The certification criteria were then developed and tested through self-assessments by 39 mobile money providers.

Homeland Security Systems Engineering and Development Institute (HSSEDI) Financial Services Cyber Threat Model

Published in November 2018, the Next Generation Cyber Infrastructure (NGCI) APEX project developed a detailed threat model, reflecting attacker methods at a level relevant to implementation with respect to a financial services institution intended both to support the NGCI APEX program use cases and to provide a common, consistent frame of reference for community interaction.

MITRE ATT&CK for Mobile

This MITRE-developed framework adapts the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) threat model to the specific threats, vulnerabilities, and remediations associated with mobile devices, and can be used as a way to further assess and address the user device-to-network segment of the mDFS ecosystem.

The Open Web Application Security Project Foundation for Mobile Security

The OWASP foundation has released a comprehensive manual to define the standard of mobile application security and enable testers to deliver consistent results for secure mobile app development and reverse engineering for IOS and Android.

Cyber Analytics Repository

The Cyber Analytics Repository (CAR) is a knowledge base that provides analysts with a catalog of intrusion detection analytics based on MITRE's ATT&CK adversarial model. These analytics improve the organization's ability to audit and respond to threats on the network and computing resources based on suspicious events that alert cyber defense personnel.

MITRE's D3FEND

This NSA-funded research was conducted with the objective to make it easier for cyber defenders to understand how countermeasures work in certain cyber technologies. For this effort, MITRE generated a knowledge graph to describe technical functions within technologies in a common language of "countermeasure techniques." Please visit the website for more information and other technical resources.

Common Weakness Enumeration (CWE™)

CWE is a community-developed list of hardware design- and software development-related weaknesses. Depending on the impact, many of these weaknesses could be considered dangerous, as they allow attackers to take over an information system or steal data.

Financial Services Information Sharing and Analysis Center (FS-ISAC)

The FS-ISAC is a cyber threat intelligence sharing membership program designed to bring awareness of ongoing attacks specific to the financial services sector (e.g., DDoS extortion, Ransomware, etc.).

National Institute of Standards and Technology Mobile Threat Catalog

NIST's mobile threat catalog contains a repository with threats specific to mobile information systems. These resources can be leveraged by security architects and application engineers to better understand threats and mitigate risks that impact either operating systems, mobile hardware, or applications.

Blockchain Security from Cloud Security Alliance

The Cloud Security Alliance recently published Blockchain Distributed Ledger Technologies (DLT) Attacks and Weaknesses Enumeration, which includes almost 200 blockchain and smart contract-related weaknesses, mapped where applicable to MITRE's Common Weakness Enumeration (CWE).

Appendix B Technical Threat Vector Mapping to the Extended, Compound Threat model

The following is a representative set of entries from the full JSON document of the technical threat model mappings of mDFS threat vectors to ATT&CK techniques and CAPEC attack patterns. The summary technical and non-technical mitigations are included, as are the relative positions on the Threat Vector map (see Section 6.3) A full version a full version will be available for download upon publication.

```
{
  "Physical Loss/Access/Theft": {
    "domain": "Hardware",
    "x": "20",
    "y": "35",
    "attack": [
      "T1213"
    ],
    "capec": [
      "CAPEC-507"
    ],
    "DFS Mitigants": {
      "Technical": [
        "authentication\u2013 complex passcodes, maximum access attempts, Two-Factor Authentication (2FA)":
        {
          "LevelOfEffort": "medium",
          "LevelOfImpact": "high"
        },
        "encryption of data at rest":
        {
          "LevelOfEffort": "medium",
          "LevelOfImpact": "high"
        }
      ],
      "NonTechnical": [
        "Policies and subsidies to provide affordable feature/Smart phones w/better access control to key populations",
        {
```

```

        "LevelOfEffort": "medium",
        "LevelOfImpact": "medium"
    }
]
}
},
"Exploit via Charging Station or PC": {
    "domain": "Hardware",
    "x": "70",
    "y": "83",
    "attack": [
        "T1458",
        "T1427"
    ],
    "capec": [],
    "DFS Migitants": {
        "Technical": [
            "patching / hardening",
            {
                "LevelOfEffort": "medium",
                "LevelOfImpact": "high"
            }
        ],
        "NonTechnical": [
            "Customer education on always plugging into untrusted sources, policy and legislation requiring operators to maintain regular reviews of equipment",
            {
                "LevelOfEffort": "medium",
                "LevelOfImpact": "medium"
            }
        ]
    }
},
}

```

Appendix C Extended Compound Threat Model Sample Entries

The following is a representative set of entries from the JSON document of the extended, compound threat model. A full version a full version will be available for download upon publication.

```
"T1003": {
  "cal": [
    "Control",
    "exploit"
  ],
  "behaviors": [
    "Acquire privileges associated with a user account, process, service, or domain. [See ATT&CK: Credential Access]",
    "Obtain unauthorized access."
  ],
  "vectors": [
    "Internal network, internal shared or infrastructure services",
    "External network"
  ],
  "cohort": "O",
  "effects": [
    "Unauthorized use",
    "unauthorized_use"
  ],
  "source": "ATT&CK"
},
"T1595": {
  "cal": [
    "recon"
  ],
  "behaviors": [
    "Perform perimeter network reconnaissance/scanning."
```

```

    ],
    "vectors": [
        "External network"
    ],
    "cohort": "P",
    "effects": [
        "(no immediate effects)"
    ],
    "source": "ATT&CK"
},
"173": {
    "cal": [
        "Control",
        "Maintain"
    ],
    "behaviors": [
        "Employ anti-forensics measures. [See CTF; see ATT&CK: Defense Evasion]",
        "Employ anti-IDS measures. [See CTF; see ATT&CK: Defense Evasion]",
        "Obfuscate adversary actions. [See ATT&CK: Defense Evasion]"
    ],
    "vectors": [
        "Internal network, internal shared or infrastructure services, internal system",
        "Internal network, internal shared or infrastructure services",
        "Internal network, internal shared or infrastructure services, authorized action of privileged user"
    ],
    "cohort": "O",
    "effects": [
        "Modification, Insertion",
        "Corruption, Modification"
    ],
    "source": "CAPEC"
},
"T1595": {
    "cal": [

```

```
    "recon"  
  ],  
  "behaviors": [  
    "Perform perimeter network reconnaissance/scanning."  
  ],  
  "vectors": [  
    "External network"  
  ],  
  "cohort": "P",  
  "effects": [  
    "(no immediate effects)"  
  ],  
  "source": "ATT&CK"  
},
```

Endnotes

¹ Demirgüç-Kunt, Asli, Klapper, Leora, Singer, Dorothe, Ansar, Saniya, and Hess, Jake, *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, World Bank, Washington, DC, 2018. p. 35.

² Ibid., p. 40.

³ Ibid., p. 54.

⁴ Diaw, C., “Gender and Education in Sub-Saharan Africa: The Women in Development (WID) Approach and Its Alternatives.” In: Abdi A.A., Cleghorn A. (eds), *Issues in African Education*. Palgrave Macmillan, New York, 2005, https://doi.org/10.1057/9781403977199_10.

⁵ Disparte, Dante, “Could Digital Currencies Make Being Poor Less Costly?” *Harvard Business Review*, August 5, 2020, p. 1.

⁶ Ibid., p. 91.

⁷ Ibid., p. 2.

⁸ Silver, Laura, and Johnson, Courtney, “Internet Connectivity Seen as Having Positive Impact in Sub-Saharan Africa,” Pew Research Center, October 9, 2018, p. 1.

⁹ Demirgüç-Kunt et al., p. 36.

¹⁰ Serianu Ltd., “Africa Cyber Security Report 2017: Demystifying Africa’s Cyber Security Poverty Line,” The Africa Cyber Immersion Center, 2018, p. 67.

¹¹ Ibid., p. 2.

¹² Ibid., p. 67.

¹³ Tran, Hung, and Matthews, Barbara, “China’s Digital Currency Electronic Payment Project Reveals the Good and the Bad of Central Bank Digital Currencies,” *The Atlanticist*, The Atlantic Council, August 24, 2020.

¹⁴ Demirgüç-Kunt et al., p. 40.

¹⁵ Demirgüç-Kunt et al., p. 43.

¹⁶ Kakpo, Fiacre, “Togo: Mobile Money Drives Financial Inclusion, According to World Bank,” *Mobile Money Africa*, January 26, 2018, www.TogoFirst.com.

¹⁷ DiCapri, Simone, “Mobile Money for the Unbanked: Enabling Regulatory Solutions,” *GSMA Mobile Money for the Unbanked*, February 2013, p. 18.

¹⁸ Unnikrishnan, Shalini, Larson, Jim, Pinpradab, Boriwat, and Brown, Rachel, “How Mobile Money Agents Can Improve Financial Inclusion,” Boston Consulting Group, February 2019, p. 2.

¹⁹ Ibid., p.4.

²⁰ Ibid.

²¹ Ibid., p. 6.

²² Ibid., p. 5.

²³ Ibid., p. 7.

²⁴ Ibid., p. 13.

²⁵ Ibid., p. 19.

²⁶ Disparte, p. 1.

²⁷ Kumar, Aditi, Ney, Jeremy, Lee, Eve, and Ji, Victor, “National Digital Currencies: The Future of Money?” Harvard Kennedy School Belfer Center for Science and International Affairs, Updated September 2020.

²⁸ Ibid.

²⁹ Ibid.

³⁰ Ibid.

³¹ CoinMarketCap, “Cryptocurrency Prices, Charts and Market Capitalizations,” October 6, 2021, <https://coinmarketcap.com/>.

³² Coinbase, “Cryptocurrency Prices, Market Cap, and Highlights,” 2021, <https://www.coinbase.com/price>.

³³ Sigalos, MacKenzie, “El Salvador Bitcoin Move Could Cost Western Union and Others \$400M a Year, Says President Bukele,” CSNBC Online, September 17, 2021, <https://www.cnbc.com/2021/09/09/el-salvador-bitcoin-move-could-cost-western-union-400-million-a-year.html>.

³⁴ Lopez, Oscar, and Livni, Ephrat, “In Global First, El Salvador Adopts Bitcoin as Currency,” *New York Times*, September 7, 2021.

³⁵ Disparte, p. 6.

³⁶ Ibid., p. 5.

³⁷ CNBC, “More than \$90 Million in Cryptocurrency Stolen after a Top Japanese Exchange Is Hacked,” August 19, 2021.

-
- ³⁸ Liquid Crypto Exchange, “Important Notice: About Hacking Damage and Suspension of Warehousing and Delivery of Crypto Assets,” August 19, 2021, <https://blog.liquid.com/ja/20210819-important-notice>.
- ³⁹ Locke, T., “Investors Must Be Vigilant and Cautious Following the Massive \$600 Million Defi Hack,” CNBC, August 11, 2021.
- ⁴⁰ Zhou, Y., “The Retrospection of the Poly Network Hack from a Security Researcher Perspective,” *Medium*, August 14, 2021.
- ⁴¹ The United States Department of Justice, “Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Dark Side,” DOJ Office of Public Affairs, June 8, 2021.
- ⁴² Serianu Ltd., p. 16.
- ⁴³ United Nations Secretary General Fintech Subgroup on Cyber Security (UNSGCS), “Briefing on Cybersecurity, UNSGSA Fintech Sub-Group on Cybersecurity,” United Nations, UNSGSA Queen Máxima, June 1, 2018. p. 2.
- ⁴⁴ Center for Strategic and International Studies (CSIS), “Economic Impact of Cybercrime – No Slowing Down,” McAfee, Washington, DC, 2018, p. 4.
- ⁴⁵ Serianu Ltd., pp. 59-60.
- ⁴⁶ CSIS, p. 4.
- ⁴⁷ *Ibid.*, p. 7.
- ⁴⁸ *Ibid.*, p. 5.
- ⁴⁹ INTERPOL, “Mobile Money and Organized Crime in Africa,” INTERPOL, June 2020.
- ⁵⁰ Alliance for Financial Inclusion, *Cybersecurity for Financial Inclusion: Framework & Risk Guide*, Guideline Note No.37, October 2019.
- ⁵¹ Demirgüç-Kunt et al., p. 38.
- ⁵² *Ibid.*, p. 68.
- ⁵³ *Ibid.*, p. 51.
- ⁵⁴ GSMA, “Digital Solutions for the Urban Poor,” GSM Association Report, 2020.
- ⁵⁵ Wikipedia, “bKash,” <https://en.wikipedia.org/wiki/bkash>.
- ⁵⁶ Tran et al., p. 2.

-
- ⁵⁷ Parkin, Darren, “Facebook’s Libra White Paper in Full,” Coin Rivet, Yahoo Finance, June 18, 2019.
- ⁵⁸ Wikipedia, “M-Pesa,” <https://en.wikipedia.org/wiki/m-pesa>.
- ⁵⁹ Disparte, p. 18.
- ⁶⁰ GSMA, “The Mobile Money Certification,” GSMA Mobile for Development, August 2020.
- ⁶¹ Dhaka Tribune, “100mn Rural People to Get High-Speed Internet Access within 2020, Dhaka Tribune online.
- ⁶² Owens, John, “Digital Financial Services, Regulations, and Financial Inclusion: Where Are We Headed?” Digital Financial Services for Development, Alliance for Financial Inclusion, posted online October 30, 2014.
- ⁶³ Demirgüç-Kunt et al., p. 109.
- ⁶⁴ Owens, p. 5.
- ⁶⁵ CREST “About Us” webpage, <https://www.crest-approved.org/about-us/what-we-do/>
- ⁶⁶ Fox, David B., Arnoth, Eric I., Skorupka, Clement W., McCollum, Catherine D., and Bodeau, Deborah J., “Enhanced Cyber Threat Model for Financial Services Sector Institutions,” Homeland Security Systems Engineering Institute, November 2018.
- ⁶⁷ United States Federal Bureau of Investigations, “Internet Crime Report 2020,” United States, March 2021.
- ⁶⁸ Hall, Ian, “Nigeria Becomes First Country in Africa to Launch CBDC,” Global Government FinTech.com, October 25, 2021.
- ⁶⁹ Adesina, Olumide, “Nigeria’s CBDC: The Good, the Bad, and the Ugly – The Possible Impacts of an eNaira on Financial Inclusion, Privacy, and Decentralized Crypto,” Coinspot.com, August 31, 2021.
- ⁷⁰ Serianu Ltd., p. 17.
- ⁷¹ Serianu Ltd., p. 17.
- ⁷² Unnikrishnan et al.
- ⁷³ Kamande et al, p. 52.
- ⁷⁴ Alliance for Financial Inclusion, p. 17.
- ⁷⁵ Bergeron, T., and Baker, J., “Security Control Mappings: A Bridge to Threat-Informed Defense,” *Medium*, December 15, 2020.

⁷⁶ Fox, David, McCollum, Catherine D., Arnoth, Eric I., Mak, Darrell J., “Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context,” Homeland Security Systems Engineering and Development Institute, August 29, 2018.

⁷⁷ The MITRE Corporation, “Caldera™,” 2021, <https://www.mitre.org/research/technology-transfer/open-source-software/caldera%E2%84%A2>.

⁷⁸ Serianu Ltd., p. 10.

⁷⁹ INTERPOL, p. 52.

⁸⁰ Global System for Mobile Association (GSMA), GSMA Mobile Money Certification Guide,” Mobile for Development, 2018, <https://gsmamobilemoneycertification.com/>.