Cybersecurity Risks and National Policy Implications - East African Experiences

Case 2

The Research Team

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Organization</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prof. Francis Wambalaba</td>
<td>Principal Investigator and Economist</td>
<td>United States International University (USIU)</td>
<td>Kenya</td>
</tr>
<tr>
<td>Dr. Paula Musuva</td>
<td>Co-PI and Cyber Security Researcher</td>
<td>United States International University (USIU)</td>
<td>Kenya</td>
</tr>
<tr>
<td>Student Interns</td>
<td>Literature Review and Research Support</td>
<td>United States International University (USIU)</td>
<td>Kenya</td>
</tr>
<tr>
<td>Ms. Judy Ouma</td>
<td>Data Analyst</td>
<td>Technical University of Kenya</td>
<td>Kenya</td>
</tr>
<tr>
<td>William Makatiani</td>
<td>Cyber Security Expert</td>
<td>Serianu Limited</td>
<td>Kenya</td>
</tr>
<tr>
<td>Brencil Kaimba</td>
<td>Cyber Security Analyst</td>
<td>Serianu Limited</td>
<td>Kenya</td>
</tr>
<tr>
<td>Dr. Koussis Nicos</td>
<td>Banking and Finance Expert</td>
<td>Fredrick University</td>
<td>Cyprus</td>
</tr>
</tbody>
</table>

Sponsor

The Global Business School Network (GBSN)

Funder

The SWIFT Institute

Report Date

November 2021

The views and opinions expressed in this paper are those of the authors. SWIFT and the SWIFT Institute have not made any editorial review of this paper, therefore the views and opinions do not necessarily reflect those of either SWIFT or the SWIFT Institute.
Abstract:

While innovative technologies are key in a competitive market, there also needs to be a corresponding investment in the development and enforcement of policy guidelines to safeguard operational environments. The main objective of this case study is to assess the lags between advancements in technology and their associated policy guidelines and the impact this has on cybersecurity risk. There is a notable dissonance between the elements of material culture such as technology and the elements of nonmaterial culture such as policies because they do not change at the same rate. It is important for policy makers and governance professionals within the banking industry to understand the impact this lag between technology and policy has on cyber security.

This case study reviewed past trends, current practices and, informed by both advanced practices and anticipated future practices elsewhere, projects future developments in the adoption of innovative technologies within the banking sector. The research used the cultural lag theory to explain respective lags between these technological advances and policy development in the East African context. Other pertinent concepts applied in the analysis included the theories of disruptive innovation and that of progress trap. Based on these findings, this research investigated potential pre-emptive, mitigation and adaptive strategies for policy and governance of regional banks practices.

This research found that USD $722 million was invested into FinTech in East Africa between 2010 and 2017 with Kenya receiving the largest investment. The top five technology advancements are: mobile banking, online banking, open banking, bank assurance and cloud computing. However, East African banks have not operationalized artificial intelligence and have a negative perception of blockchain technologies. Also, least implemented are data classification, digital forensics and security operation centers. In addition, banks are facing huge risks relating to financial fraud, data theft and malware attacks. The greatest risks are malicious insiders and organized crime syndicates, especially because of homegrown organized criminal actors such as SilentCards that have successfully stolen billions of Kenyan shillings using customized malware on ATMs and infiltrating financial systems with the help of accomplice insiders.

On one hand, there have been commendable advancements in cybercrime and data protection legislation by East African countries since the 2014 African Union Convention on Cyber Security and Personal Data Protection, making it possible to prosecute cybercriminals. On the other hand, given that a number of technology innovations such as artificial intelligence, blockchain and cryptocurrencies are yet to have policy guidance, this has resulted in a cultural lag. This lag can be explained by a notable shortage of skilled and experienced professionals needed in the formulation,
implementation and enforcement of cybersecurity best practices and policies. Policy makers, law enforcement and the judicial officers lack requisite cybersecurity training and expertise to guide the changing face of technology innovation and to avert potential cybersecurity risks.

To minimize this lag, the research recommends enhancement of the current model where these emerging FinTech innovations are first observed in a controlled sandbox environment before being allowed into the market, since regulators are keen not to stifle innovation while ensuring their policy guidelines are well informed. To mitigate skilled labor shortage, more investments in human resource development are needed. In addition, a lot more co-operation needs to take place between FinTech innovators and regulatory bodies to ensure technology innovation delivers desired benefits while avoiding pitfalls and cybersecurity risks.

This case study report is suitable for multi-audiences including practitioners, policy makers and academicians/researchers.

**Introduction:**

Technological advancement and adoption of innovation by organizations tends to increase the cyber threat attack surfaces, cyber risk and consequently the number of cyber incidents. In 2013, Symantec Corporation reported that the rate of cybercrime increase in Africa was higher than any other region in the world. This is thought to be possibly due to weak cybersecurity controls despite there being very high rates of internet penetration (UNECA, 2014). In 2018, global losses resulting from cybercrime were approximated to have cost at least $45 billion (Online Trust Alliance, 2019) with a projected rise to $6 trillion annually by 2021 (Cybersecurity Ventures, 2019). The largest data breach in 2018 involved the compromise of 1.1 billion records from India’s integrated national biometric identification register named Aadhaar. Accenture & Ponemon Institute (2019) estimated an average loss of $13 million for each company they surveyed with banking firms experiencing the greatest losses with an average of $18 million per company. Kenya is estimated to have lost a total of $88.5 million due to direct costs of cybercrime, with banks and other financial service providers having been hit hardest with losses of about $28 million (Serianu, 2018). According to Van Niekerk (2017) South Africa reported that financial attacks were one of the most common type of attacks between the years 2011-2016 under a backdrop of global loses.

To effectively mitigate cybercrime risks that come with innovative technology adoption, emphasis needs to be placed on not only the significance of technological innovation but also corresponding protective controls particularly policy development to guide innovation (Schneier, 2019a). Policymakers can no longer afford to be ignorant about disruptive technologies, but rather must work
hand in hand with technologists to develop and implement policies that will effectively govern technological advancement and innovation (Christiansen, 2001; Schneier, 2019a).

**Aims:**

The main objective of this study is to assess the cybersecurity risks stemming from lags between policy development and technological advances in the banking industry with particular focus on the East African Region.

The specific research objectives are:

1. to review past trends, current practices, and anticipated future practices in development of innovative banking technologies with relation to cyber security risk;
2. to establish existing regulatory policy instruments guiding technology innovation in the banking sector within the East African Context;
3. to examine models and theories that explain the divergence between technological innovations and applicable regulatory policies;
4. to recommend potential regulatory strategies for addressing cyber security risk stemming from technological innovations in the banking industry.

1) **Literature Review:**

The United Nations (2018) Technology and Innovation Report notes that we are living at a time of unprecedented and exponential technological change. There are multiple innovative digital platforms interconnected in various combinations changing economies and societies at unprecedented levels. These new technologies are expected to automate and simplify human processes and can be seen as essential tools for delivering on the United Nations 2030 Agenda for Sustainable Development for more inclusive and thriving societies. Some of the technologies identified to have the ability to transform society include: Artificial Intelligence (AI), Big Data, Internet of Things (IoT), Blockchain, Satellites, Drones, Renewable Energy Technologies (RET), Advanced Materials and Nanotechnology, Biotechnology and Health Tech, and 3D Printing.

The banking sector is more specifically affected by technological innovations relating to delivery of financial services commonly referred to as Financial Technology or FinTech. FinTech has revolutionized the delivery of financial services in ways that have supported traditional banking but also in ways that have disrupted the traditional banking model. Banks are investing heavily to digitize their business model in order to meet customer demands for convenient and personalized services and to be more
efficient in their operations. There is a clear value proposition from FinTech which relates to economic
growth by opening up untapped geographic and customer segments, increased innovation that
improves customer experiences, reduces costs while increasing revenue (EAVCA et al., 2018).

While it was estimated 2018 that there are over 4,000 FinTech companies around the world, by
February 2021 the estimates stood at 26,045 worldwide (UKaid 2018 and Statisca, 2021). They operate
across different services such as payments, lending, banking infrastructure, markets, investments and
savings, and insurance (UKaid, 2018). The Global FinTech Report by PwC (2019) shows that 84% of
financial firms around the world have embedded FinTech in their operational models to some extent.
The report lists the top 9 technology game changers in the financial services sector as: Artificial
Intelligence (AI), Big Data, Cloud, Blockchain, 5G, Internet of Things (IoT), Robotic Process Automation
(RPA), Voice Technologies including those utilizing Natural Language Processing and Digital Identity
Management. Its 2017 report featured data analytics in first place followed by mobile services (PwC,
2017).

The Atos (2018) report examines how ten key technologies illustrated in

Figure 1 are transforming the present and future of the banking and financial services ecosystem.
Hybrid cloud technologies are currently considered widely adopted and are classified as mainstream.
API platforms, Robotic Process Automation and Instant Payments are classified to be in an early trial
adoption phase within the industry. Artificial Intelligence, Blockchain, Prescriptive Security and
Augmented Reality are at an adolescent stage while Quantum Computing and Smart Machines are
classified at an emerging stage.
The investment in FinTech companies all over the world since 2010 is estimated to be more than $24B. Unfortunately, FinTech regulatory policies may not exist or may be weak as regards data protection and cyber security. In many cases fraudsters, hackers and malevolent actors take advantage of weaknesses in FinTech development, implementation and use and thereby lead to substantial financial, data and privacy exposures. Ng & Kwok (2017) urge for the scrutiny of FinTech against best practices and applicable policies, regulations and legislation. IMF (2019) issues caution pointing out that as much as FinTech has been highly adopted in sub-Saharan Africa and has brought great gains, it is a double-edged sword. These new technologies could introduce new risks and unintended negative consequences. It is important to have relevant policy guidance and regulatory oversight to ensure that FinTech delivers intended benefits while mitigating against associated risks and unintended negative consequences.

2) Methodology:

This case study research took up a descriptive research design utilizing a concurrent mixed method data analysis approach to establish practices relating to FinTech innovation and regulatory policy
guidance aimed at addressing cybersecurity risk in the East African Banking context. The research questions were answered by examining secondary data captured in various reports published by East African Banks, Bankers Associations, Central Banks and other financial industry stakeholders who contribute to FinTech research, innovation, cybersecurity risk mitigation and cybersecurity policy.

The secondary data was enriched through primary data surveys completed by representatives of 27 banks located in Kenya, Uganda, Tanzania and South Sudan. Further interviews were conducted with representatives from the Kenya Bankers Association, Uganda Bankers Association, Communications Authority of Kenya, ICT Authority of Kenya and the Kenya Capital Markets Authority that runs a regulatory sandbox for FinTech.

Primary data collection took place over a period of 5 months from May to September 2020. Due to the COVID-19 pandemic, the research team had to observe restrictions relating to travel, physical meetings and group gatherings. All surveys and interviews took place virtually using email and online collaboration platforms.

The analysis of collected data allowed an identification of key emerging issues from a theoretical but also practice-based approach relating to the development of appropriate recommendations for strategies for addressing cybersecurity risks arising from FinTech adoption.

Finally, the draft recommendations were shared with stakeholders for review and feedback allowing for transparency in outcome report content, additional input for more enriched recommendations, and also room to correct any misrepresentations. These have been incorporated in the report.

3) Findings:

This section presents the research findings. It begins by examining past trends, current technology innovation practices and anticipated future trends influencing banking practices and their effect on cybersecurity risk in the East African Region. It then establishes existing regulatory policies within the East African context that are governing technology innovation in the banking sector. Thereafter, the cultural lag theory and disruptive innovation and progress trap of innovation theories are used to explain the dissonance between technological innovations and applicable policies. Finally, recommendations are given with regard to regulatory strategies for addressing cybersecurity risk stemming from technological innovations in the banking industry.

3.1 Past Trends, Current Practices and Anticipated Future Practices in Financial Technology Innovation:

Technology innovation in the East African region is thought to have begun with the introduction of the
pre-computing devices such as the Electrical Accounting Equipment (usually called EAM) that used punched cards and electro-mechanical parts for mathematical computation. Couperus (2011) notes that these EAM machines were replaced by the ICT 1500 in the 1960s. Kenya got two ICT 1500 machines after independence around 1964; one was installed at the East African Railways & Harbours (EAR&H) and the other at the East African Power & Light (EAP&L). The first financial organization to make use of the ICT 1500 was the Post Office Savings Bank which used it to keep financial records for its savings accounts. Subsequent technology adoption in the banking sector saw the adoption of credit and debit cards, ATM machines, electronic funds transfer, internet and online banking. By the year 2000 online banking and money transfer services such as PayPal become mainstream, thereby supporting the burgeoning e-commerce industry. Many banks would later innovate by making it easy for customers to access funds and carry out transactions online. The next technology innovation that would be a game changer is mobile money services where people could carry out financial transactions using their mobile device instead of using cash or cards. More importantly, this innovation increased the reach into the population of the unbanked.

The East African banking sector space has been greatly transformed by FinTech with Kenya standing out as the regional leader in financial innovation (FSD, 2015). Research by East Africa Venture Capital Association (EAVCA), Intellecap, Financial Sector Deepening-Africa, FMO, and UKAid shows that USD $722 million has been invested into FinTech in East Africa during the period 2010 to 2017 with Kenya receiving the largest investment. Of this amount 72% was invested externally by foreign investors while 28% of the financing came from within East Africa as illustrated in Figure 2 (EAVCA et al., 2018).

![Figure 2: FinTech Financing in East Africa (EADB, 2019)](image)

Current trends in technology advancements show that FinTech innovation is and will continue changing the face of banking services. This section explores some of these technology trends namely mobile banking, online banking, open banking (web services and APIs) digital lending, cloud
computing, artificial intelligence, machine learning, blockchain and cryptocurrencies. Figure 3 illustrates the innovation trends expressed by banks during the data collection process. Participants in this study shared the extent to which their organization had embraced eight listed technology advances in their operations. Results indicate that mobile banking is the most adopted technology, followed by online banking and open banking through web services and APIs, bank assurance, cloud computing, social media and robotics. What may not be widely known are the Bank Assurance (sometimes called bancassurance) technologies which enable banks to partner with insurance companies to sell insurance products to bank customers seamlessly (Deloitte, 2019b; McKinsey, 2019). The majority stated that they were not using artificial intelligence but it was a desirable target in the near future. However, blockchain technology was yet to receive positive consideration and adoption.

These emerging and future technologies that are revolutionizing East Africa’s banking industry are examined in more detail in the following sections.

3.1.1 Mobile Money:

Mobile money technology is a digital wallet operated using a mobile phone to send, receive and store
money during transactions. It is considered by some to be the most revolutionary innovation to transform the financial services industry (Cytonn Investment, 2019). The East African region is considered as the heart of mobile money in not only Africa but also the world. This is because it has the highest per capita number of registered and active mobile money accounts and this number has actually surpassed that of bank accounts (Groothuizen, 2019).

The use of mobile phones to carry out financial transactions using mobile money began in Kenya in 2007 through Safaricom’s M-PESA service. In 2008, Vodafone launched M-PESA in Tanzania; in 2009, MTN launched MTN mobile money in both Rwanda and Uganda (EADB, 2019). The introduction of mobile money in East Africa has been key in increasing financial inclusion and consequently poverty reduction a key Sustainable Development Goal. The number of East Africans dependent on mobile money services continue to rise exponentially. Data examining financial inclusion in 2019 shows that 82.9% of adults in Kenya have access to formal financial services accounts, which is a substantial increase compared to 26.4% in 2006. This rise coincides with the introduction of M-PESA and associated services that provide access to the financial system (Ndung’u, 2019). Findex 2014 data illustrated in Figure 4 shows that Kenya outperformed other sub-Saharan countries in measures of financial inclusion.

As of December 2019, the Communications Authority of Kenya (CAK) reported that 28.9 million Kenyans actively used mobile money services with a 54.5 million active SIM card registrations implying a 114.8% mobile subscriber penetration rate due to multiple SIM card ownership. Safaricom’s M-PESA controls 98.8% of the mobile money market share (Communications Authority of Kenya, 2020). Rwanda’s financial inclusion statistics recorded an increase from 21% in 2006 to 68% in 2016, with 60% of the population using mobile money. Tanzania recorded an increase from 11% in 2006 to 65%
in 2017, with 60% of the population using mobile money services. Uganda’s increased from 21% in 2006 to 58% in 2008, with 56% of the population using mobile money (EADB, 2019). These statistics are illustrated in Figure 5.

These East African mobile money platforms are used largely for more than just person-to-person transactions and more for business-to-business transactions and in the purchase goods and services and to access short-term loans. In 2018 over 4 trillion Kenya shillings was exchanged through mobile money services as illustrated in Figure 6 which is equivalent to 45.3% of the country’s GDP. Mobile money platforms have challenged commercial banks to embrace these technological innovations in order to regain their market share.
3.1.2 **Online Banking:**

Traditional brick-and-mortar bank operations are increasingly being replaced by contactless online banking options and mobile phone apps that enable convenient and quick access to 24/7 financial services at low cost. Cytonn Investment (2019) reports that the top 3 Kenyan banks register 54% of their transaction volumes through internet and mobile banking with only 8.5% of their transaction volumes taking place at physical branch locations. This has led to branch closures and staff retrenchment with a negative impact on employment and calling for a more tech-savvy workforce.

3.1.3 **Open Banking and Application Programming Interfaces (APIs):**

Open banking is a technology initiative that facilitates the creation, access, distribution and sharing of data from financial institutions using secure application programming interfaces (APIs). This exchange of data fosters innovative packaging and delivery of financial services across different service providers and improves customer experience. It also protects intellectual property and fosters investment in innovation because developers do not have to share details regarding the internal workings of their software. Different service providers can open up APIs to their platforms and have consumers of their services (whether other businesses or customers) access these platforms. It also empowers users to manage their own data and flexibly access the financial providers of choice (Cytonn Investment, 2019; Deloitte, 2019a; Munyu, 2018). Examples within East Africa of this is the API interfaces opened up to the M-PESA mobile money service that allows integration of mobile money payments on various online businesses and e-commerce platforms.

3.1.4 **Digital Lending:**

In Kenya, Safaricom started operating in the digital lending space in November 2012 when it launched the M-Shwari platform. M-Shwari is a deposit savings account product backed by Commercial Bank of Africa (CBA) from which customers can get instant loans through their mobile phones. M-Shwari has over 23 million customers with over USD$140 million in customer savings while lending over USD$2.7 billion in loans. CBA Tanzania launched a similar digital lending platform dubbed M-Pawa in May 2014 which now has over 7 million customers with over USD$8 million in deposits and over USD$56 million in loans.

Safaricom subsequently launched the Fuliza service in 2019 to allow M-Pesa mobile money customers access overdrafts to facilitate transactions when they do not have sufficient funds. In the first week of Fuliza’s operations, customers had borrowed 1 billion Kenya shillings, and this had risen to over 6.2 billion shillings by the end of that month and to over 81 billion in 6 months (Cytonn Investment, 2019; Kamau, 2019).
These Telco-bank lenders, as they are referred to, have accounted for over 76% of the loan accounts in Kenya. However, since the amounts loaned out are often small, they only account for 4% of the loan values. Typically, the amount advanced to a mobile-bank account is approximately USD$25 compared to an average of USD$ 2,794 for a loan advanced to a bank account.

Kenya is reported to have over 150 FinTech companies operating with an increasing number of them offering quick unsecured loans using mobile apps to handle the entire process end-to-end. The mobile apps are able to register new customers, process their loan applications having done some form of credit assessment and even automate the collections for repayment. They manage risk by using big data from various sources and using artificial intelligence algorithms to assess risk of defaulting repayments. FinTech firms have innovated in this space by coming up with innovative risk assessment models that leverage the collection of vast credit scoring data (Collins, 2020; Cytonn Investment, 2019).

3.1.5 Cloud Computing:

Banks have increasingly adopted cloud technologies to reduce the complexities associated with running on premise infrastructure and services. Cloud setups have enabled banks to quickly rollout their services with requisite flexibility and capacity to scale as demand increases. Banks have been able to secure connectivity for their staff to work from home and various remote locations while ensuring business continuity during COVID-19 travel restrictions and lockdown periods. Cloud services, when structured right, have helped banks cut down on costs and have lowered risks associated with cyber incidences while providing for security and resilience.

3.1.6 Big Data, Analytics, Artificial Intelligence, Machine Learning and Robo-Advice:

Vast amounts of Big Data are being amassed across disparate platforms by firms and the corresponding strategic investments in analytics and use of artificial intelligence make this a top category to watch. One prominent application of these technologies is in being able to conduct risk assessments when deciding whether to advance loans based on computed credit scores and also when identifying and investigating fraud. Some FinTech platforms can examine customer behaviour and integrate this information on risk assessments. These technologies are also used to automate routine banking operations such as account opening. Banks are also using chat bots for customer service to deliver self-service options, answer simple queries from a Frequently Asked Question (FAQ) database and also to reduce volume of requests that reach human customer service agents thereby reducing their workload. Recent applications of these technologies is in robo-advice which automates personalized investment advice to customers based on their historical data, profile and investment goals (Crosman, 2019; PwC, 2019).
3.1.7 Blockchain and Cryptocurrencies:

Blockchain technology is considered to have great potential for securing transaction information, automating financial contracts and protecting data privacy in the financial sector. Through blockchain technology, new financial products and services might be developed to considerably increase operational efficiency (Ng & Kwok, 2017).

There have been mixed reactions within the banking industry regarding the adoption of blockchain technologies in financial services. Blockchain’s association with cryptocurrencies has drawn a negative backlash due to risks relating to fraud and association with anti-government, anti-regulation and criminal movements on the dark web. In 2018 Kenya’s Central Bank sent a circular to banks warning them against transacting trading in cryptocurrencies and, due to regulatory concerns, further speaking against the launch of Facebook’s Libra cryptocurrency which was expected to serve over 2.3 billion Facebook users (Mbogo, 2018; Michira, 2018; Munda, 2019).

The negative sentiments and resistance to cryptocurrencies may have overshadowed the positive transformation that could come with the underlying blockchain technology that promises a secure distributed and immutable platform for transactions with the capability of building in automated enforcement of agreements through smart contracts and strong cryptography when fighting fraud and providing digital identity services.

There are FinTech rollouts in East Africa particularly in the insurance and banking industry that may embed the use of blockchains and smart contracts (EAVCA et al., 2018). Additionally, banking and financial services providers around the world are reported to be filing numerous blockchain-based patents indicating that financial firms are keen to explore the technology in service delivery (Crosman, 2019). The PwC (2019) report is optimistic on the future of Blockchain reporting that 40% of banks believe it will bring great change in delivery of financial services in the near future.

The Kenyan Government through the Ministry of Information Communications and Technology established the Distributed Ledgers Technology and Artificial Intelligence Task Force which released a comprehensive report in July 2019 to inform policy formulation and guide the use of blockchain and artificial intelligence to solve problems in key strategic areas. The task force proposes initiatives such as the use of a Central Bank Digital Currency (CBDC) as a digital equivalent of fiat currency as legal tender to drive digital transactions (Ministry of Information Communications and Technology, 2019a).

3.2 Cybersecurity Risks:

As banks have embraced financial technology innovation, they have also inadvertently taken up a requisite set of accompanying cybersecurity risks. Technologies supporting online banking, mobile
money services, remote access to bank systems and services have been particularly targeted. PwC (2019) study on how FinTech has changed the global financial services industry highlighted that the top challenge for technology adoption are risks associated with security, data privacy and compliance to regulations. EAVCA et al. (2018) and IMF (2019) also point out that credit and financial fraud risks increase with FinTech adoption.

Integrating newer technology platforms with older legacy systems also introduces complexity and risk assessments need to evaluate unprecedented risk scenarios. In addition, the cybersecurity risk challenge is amplified because firms also do not have a workforce that has sufficient skills and experience to securely develop, implement, configure, and operate these technologies.

According to survey responses obtained in this study, bank representatives perceived that the greatest loss from cybersecurity risk incidents, if they occurred, would be from cyber providers, business partners and malicious insiders. They ranked this higher than other external sources of cybersecurity threat such as organized cybersecurity syndicates. They also perceived the least threat would come from state-sponsored hackers. These results are illustrated in Error! Reference source not found. This raises questions on how well-prepared banks are to mitigate cybersecurity risk impacts should incidents stem from various actors. Banks are having a harder challenge and seem less prepared to mitigate risks from internal actors as opposed to external actors.

Key:
1. Low: Likelihood of its occurrence is minimal
2. Medium: There is a good chance it will occur, but with the measures in place, business operations will not be impacted as much
3. High: Its occurrence will definitely lead to huge losses for the organization.
3.2.1 **Organized Criminal Groups Targeting Banks:**

Group-IB, a Singapore based cybersecurity company, analyzed top hi-tech crime trends in their report for 2019 and 2020 and highlighted a number of attacks targeted at the financial services sector (Group IB, 2020). They carried out in-depth investigations on five cybercriminal groups that pose a real threat to banks all over the world. The three most notorious groups are attributed by Group-IB as Russian and go by the names Cobalt, MoneyTaker and Silence. The other infamous group named Lazurus is attributed to be North Korean and has been observed since 2014 conducting advanced attacks on financial systems. The newest entrant is a group named SilentCards, attributed to be Kenyan, was observed in 2018 conducting devastatingly effective attacks on ATM and card processing systems. SilentCards is reported by Amadala (2019), Genesis (2019) and Niba (2019) to be a home-grown Kenyan cartel that re-emerged from a previous cybercriminal group named Forkbombo that had been targeting banks in 2016 and 2017. SilentCards is known to use customized Python hacking scripts and malware variants on financial system servers, end-user machines and ATMs.

Kenyan financial institutions were put under high alert by various cybersecurity agencies and research firms in 2019 when operations of organized criminal groups came to their attention. There were clear signs of very skilled, well-coordinated and connected cybercriminal groups in operation within not just Kenya but the East African region.

The groups are suspected to be young recent IT graduates in their mid to late 20s. Various banks were hit hard with media reports highlighting targeted cyber heists. One international bank lost 11 million Kenya shillings when four of their ATMs were compromised by jackpotting malware in one Easter holiday weekend. Similarly, another local Kenyan bank is reported to have lost 6.9 million Kenya shillings in one week while another national bank is reported to have been robbed of 29 million Kenya shillings.

The SilentCards group is suspected to be the most prolific criminal group operating in East Africa and is behind cyber heists robbing banks, microfinance and savings and credit societies (SACCOs). An investigation in 2018 revealed SilentCards operations included bribing of bank staff to plant infected laptops in organization networks and in one scheme the group was able to get away with a total of 400 million Kenya shillings by infiltrating financial processing systems. The groups are reported by Sunday (2020) to have stolen over 2.6 billion Kenya shillings in 2018 and 2019 while Kenya’s Cybercrime Investigations Unit reported that Kenya lost 17 billion Kenya shillings to hackers in 2016.

3.2.2 **Trends in Cybersecurity Incidents:**

Current trends in cybersecurity incidents established from surveys filled in by bank representatives show that the most prevalent type of cybersecurity attack is social engineering through phishing as
illustrated in Figure 7. This is followed by card fraud and mobile money fraud, which are designed to make it easy for customers to carry out financial transactions but are also heavily targeted by fraudsters. This confirms warnings from IMF (2019) cautioning against the downsides of FinTech which involve increased hacking, financial fraud, data theft and data privacy incidents.

Figure 7: Prevalence of Cyber Security Attacks

Key:

1. Not at all: Does not contribute to any attack
2. Small Extent: Means contributes to less than 20% of attacks
3. Some Extent: Contributes to 20-40% of attacks
4. Moderate Extent: Contributes to 40-60% of attacks
5. Great Extent: means contributes to 60-80% of attacks
6. Very Great Extent: indicates contributes to more than 80% of attacks

3.3 Policy, Legislative and Regulatory Provisions for Financial Technology Innovation and Cybersecurity Risk:

United Nations (2018) supports technological innovation that promotes sustainable development leading to the attainment of the 2030 Agenda for Sustainable Development Goals. For innovation
systems to be integrated smoothly it is imperative for states to have policy frameworks that foster innovation. Such policies would help address how, in a rapidly advancing world, to avoid the pitfalls of emergent technologies while enjoying the numerous advantages they bring. Without these regulatory and policy frameworks in place, developing countries will have a hard time adjusting to these emergent technologies (Schneier, 2019a, 2019b; United Nations, 2018). Christiansen (2001) points out that there is need to integrate a policy framework at every stage of technological advancement but also critically examine and understand the synergy between public policy and technological innovation.

The International Telecommunications Union setup the Global Cybersecurity Index (GCI) as a way to measure commitment of countries to cybersecurity. The aggregated index considers five key pillars when measuring the cybersecurity maturity in a country and these are: (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Building, and (v) Cooperation. ITU (2019) reported that only two African countries had high GCI scores demonstrating high commitment to all five pillars of the index. These countries were Egypt with 0.842 and Kenya with 0.748. Majority of the African states had low GCI scores and low commitment to cybersecurity. East Africa scores are outlined in Table 1 where Tanzania and Uganda had a score of 0.642 and 0.621 respectively (ITU, 2018). However, they have since published National Cybersecurity strategies that are likely to increase their scores in subsequent reviews. Burundi and South Sudan lack National Cybersecurity Strategies and it is evidenced by their low GCI scores of 0.087 and 0.065 respectively (Jabar et al., 2020).
Table 1: ITU Global Cybersecurity Index (GCI) Scores for East Africa (ITU, 2018):

<table>
<thead>
<tr>
<th>Country</th>
<th>GCI Score</th>
<th>African Ranking</th>
<th>Global Ranking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kenya</td>
<td>0.748</td>
<td>2</td>
<td>44</td>
</tr>
<tr>
<td>Rwanda</td>
<td>0.697</td>
<td>3</td>
<td>49</td>
</tr>
<tr>
<td>U. R. Tanzania</td>
<td>0.642</td>
<td>6</td>
<td>59</td>
</tr>
<tr>
<td>Uganda</td>
<td>0.621</td>
<td>7</td>
<td>65</td>
</tr>
<tr>
<td>Burundi</td>
<td>0.087</td>
<td>33</td>
<td>151</td>
</tr>
<tr>
<td>South Sudan</td>
<td>0.065</td>
<td>35</td>
<td>157</td>
</tr>
</tbody>
</table>

Increased internet penetration and dependence on information and communication technologies led the Africa Union in 2014 to establish the African Union Convention on Cyber Security and Personal Data Protection. The Cybersecurity treaty mandated member states to establish regulatory and policy measures to foster cybersecurity governance and curb cybercrime. Orji (2018) points out that the convention was set in place to address the insufficiency of structures and institutions required for effective and efficient cybersecurity governance in Africa. Africa Union Member States are required to have frameworks that descriptively address all the elements of cybersecurity (technical, organizational, policy, and legal) to protect individuals, the society and critical information infrastructure. The intended result of the treaty was to promote cyber stability, which is defined as “a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels”.

Cyber laws, e-Justice, and Information Security have been identified as the primal elements that will ensure that the framework for cyber laws are implemented successfully (UNCTAD, 2011). However, to ensure its successful implementation, the EAC came up with a Task Force whose mandate includes taking charge of the successful implementation of the cyber laws (UNCTAD, 2011). By September 2008, The Republic of Uganda had prepared an Electronic Transactions Bill, Digital Signatures Bill, and Computer Misuse Bill. The Republic of Kenya prepared an Electronic Transactions Bill that was inclusive of legal recognition of e-documents and transactions, institutional arrangement, offences, dispute resolution mechanism, and data protection and privacy. The Republic of Rwanda prepared an omnibus law that addressed electronic transactions and signatures. The United Republic of Tanzania did not specify their cyber laws but in 2005, they had submitted a legal framework for e-commerce
and cybercrimes. The Republic of Burundi did not specify their cyber laws (UNCTAD, 2011).

### 3.3.1 Cyber Policy, Legislative and Regulatory Provisions in East Africa:

A descriptive overview of the existing cyber-related legislation in the East African Community is captured in Table 2. Note that Kenya, Uganda, Tanzania and Rwanda have specific Cyber Legislation while Burundi and South Sudan are yet to enact such legislation. Subsequent sub-sections outline a detailed discussion of each of the country’s cyber policy, legislative and regulatory frameworks.

**Table 2: Key legislations in the East African Community:**

<table>
<thead>
<tr>
<th>COUNTRY IN EAC</th>
<th>KEY LEGISLATION(S)</th>
<th>REMARK(S)</th>
</tr>
</thead>
</table>
• Kenya National Cybersecurity Strategy, 2014  
• Kenya National ICT Policy, 2019  
• Computer Misuse and Cybercrimes Act, 2018  
• Data Protection Act, 2019 | Computer Misuse and Cybercrimes Act, 2018 is integral in addressing the rise of cybercrime and the emergent digital economy. It addresses content-related crime such as child pornography, offences against the CIA of computer data and systems, and computer-related offences such as cyber bullying. |
| Uganda         | • Computer Misuse Act, 2011  
• National Information Security Policy, 2014 | The Computer Misuse Act, 2011 is Uganda’s latest cyber law. This Act was assented to in 1st November 2010 and the initial day of implementation of the Act was 14th February 2011. It outlines various misuse offenses and promotes the security of electronic transactions and information systems. |
| U.R of Tanzania | • National ICT Policy, 2003  
• The Cybercrimes Act 2015 | Passed as a bill in March 2015 and then assented to in April 2015. This Act addresses criminal offences related to computer Systems, including fraud, forgery, and data espionage. However, it does not address personal data protection.  
• The Electronic and Postal | Adopted in March 2018. This legislature addresses the |
<table>
<thead>
<tr>
<th>COUNTRY IN EAC</th>
<th>KEY LEGISLATION(S)</th>
<th>REMARK(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Communications (Consumer Protection) Regulations 2018</td>
<td>collection, processing, and maintenance of personal data.</td>
</tr>
<tr>
<td>Rwanda</td>
<td>• African Union Convention on Cyber Security and Personal Data Protection, 2019</td>
<td>Passed on 27th June 2014, signed on 16th April 2019 and fully ratified on 14th November 2019. It mandates nations to set up their own regulatory and policy framework to enhance cybersecurity. It addresses the failures of older institutions and their frameworks of dealing with these challenges.</td>
</tr>
<tr>
<td></td>
<td>• Data Protection and Privacy Law, 2015</td>
<td>This law was revised in 2015. It addresses the protection and privacy of computer data with respect to its processing in Rwanda. It also addresses the free flow of non-personal data.</td>
</tr>
<tr>
<td>Burundi</td>
<td>• Penal Code, 2009</td>
<td>This is law was revised and passed on 22nd April 2009. However, there is no separate policy and legislation on cybercrime this penal code contains a specific legislation on cybercrime. Burundi has no have policies and regulations that govern personal data protection. **</td>
</tr>
<tr>
<td>South Sudan</td>
<td>• Penal Code, 2008</td>
<td>The penal code specifies cybercrime offences and regulations. As of 2013, a nationally recognized CIRT and cybersecurity body were nonexistent. Specific frameworks designed for cybersecurity were not approved for implementation in accordance with international cybersecurity standards. South Sudan lacks a cybersecurity roadmap, national and sectoral cybersecurity strategy.</td>
</tr>
</tbody>
</table>

*Kenya:*

The first piece of legislation enacted to guide ICT and cyber matters in Kenya was the Kenya Information and Communications Act (KICA) in 1998, which was later amended in 2013 and subsequently had Cyber security regulations included in 2016. KICA led to the establishment of the Communications Authority of Kenya (CA) as the independent regulatory licensing authority for the
information and communication technology sector including telecommunication, information technology and electronic commerce. The Communications Authority has led in cyber security initiatives particularly through the National Kenya Computer Incident Response Team Coordination Center (National KE-CIRT/CC) which was setup in 2012. The National KE-CIRT/CC is the focal point for cyber security matters and it coordinates with industry-specific, regional and international Cyber Security Incident Response Teams (CSIRTs). It champions capacity building and knowledge sharing through collaborative multi-stakeholder engagement, publication of research reports, and spearheading awareness initiatives such as the Child Online Protection (COP) initiatives. The National KE-CIRT/CC Cybersecurity Committee (NKCC) is composed of members from law enforcement such the police, Directorate for Criminal Investigations (DCI), National Intelligence Service (NIS) but also the military, government agencies, banking sector, telecommunications sector, Internet Service Providers, academia and consumer advocacy groups among others.

The Ministry of ICT, Innovation and Youth Affairs was created in 2004 (initially called Ministry of Information Communications and Technology) and has the mandate to set up policy to guide technology innovations and to guide the nation’s cybersecurity strategy. It set out the national ICT policy first in 2006 and this was later reviewed in 2016 and its latest version was published in 2019 (Ministry of Information Communications and Technology, 2019). This policy establishes ICT innovation, cyber security and protection of vulnerable populations as key strategic goals.

The Ministry of ICT set out Kenya’s five-year National Cybersecurity Strategy in 2014. The strategy defines Kenya’s cybersecurity vision and goals for enhancing the nation’s cybersecurity posture in a manner that: facilitates the country’s growth, safety, and prosperity; builds the nation’s capability by raising cybersecurity awareness; develops Kenya’s workforce to address cybersecurity needs; and fosters information sharing and collaboration (Ministry of Information Communications and Technology, 2014). The Ministry of ICT also set out Kenya’s National ICT Masterplan to institutionalize a cyber-security management framework that would help in the implementation of the strategy and implement a cyber-security policy.

The Computer Misuse and Cybercrimes Act of 2018 was acceded to law on 16 May 2018. Some sections of the Act were suspended when they were contested at the High Court, but the suspensions were lifted on 20 February 2020. This Act aims to promote cybersecurity by facilitating detection, investigation, prosecution, and punishment of computer crimes, while also fostering international cooperation when dealing with computer crimes. Through this law, a National Computer and Cybercrimes Coordination Committee and operational secretariat were enacted to provide the government with guidance on security matters.
The Data Protection Act (2019) came into effect on 25th November 2019 and is aimed at protecting personal data in the context of technologically advanced digital platforms that collect vast amounts of data over years with the aim of delivering innovative services supported by advanced analytics and automation.

The Central Bank of Kenya (CBK) is the regulator for banks, microfinance institutions and the financial services industry as a whole. No bank or financial services company can operate without approval of the CBK. In 2017, CBK issued the Guidance Note on Cybersecurity that outlined the minimum cybersecurity provisions that banks must put in place for effective cybersecurity governance and cyber security risk management (Central Bank of Kenya, 2017). In 2019, CBK issued new guidelines that extended mandatory provisions to all Payment Service Providers (Central Bank of Kenya, 2019). The guidelines require that banks and other Payment Service Providers (PSPs) have a Chief Information Systems Officer (CISO), who is to design and implement the organization’s cybersecurity strategy and must report to the board at least once a quarter. It also requires that banks and other major PSPs report attacks within two hours of their occurrence.

**Uganda:**

The Republic of Uganda constituted the National Task Force in 2003 with a mandate to initiate cyber laws. A cyber legal framework was enacted in 2011 and the Electronic Transaction Bill, Electronic Signatures Bill, and Computer Misuse Bill were passed. The Electronic Transaction Bill and Computer Misuse Bill are cornerstones for e-Commerce while the Electronic Signatures Bill are an embodiment of international best practices. Uganda through its National Information Technology Agency (NITA-U) set out their National Information Security Policy in 2014, which outlines guidelines for governance, information security, physical security and personnel security. Uganda also has the National Computer Emergency Response Team (CERT.UG) operated by the National Information Technology Agency (NITA-U) under the supervision of the Ministry of Information and Communications Technology.

**Tanzania:**

Prior to 2003 when the National ICT Policy was published, the United Republic of Tanzania had no regulatory frameworks that specifically focused on ICT. The legal regulations on paper-based transactions did not address these technological changes. Laws such as the Penal Code and the Criminal Procedure Act fell short of addressing the fast-paced technological space. This created a loophole for criminal offenders to escape prosecution. However, in 2003, the government adopted a National ICT Policy and in 2009 the Tanzanian Communications Regulatory Authority defined processes that allowed for electronic communications (UNCTAD, 2011).

On 25th April 2015, the United Republic of Tanzania signed into law their Cybercrimes Act. It aims to
make provisions for criminalizing offences related to computer systems and Information Communication Technologies and provide for investigation, collection, and use of electronic evidence and for matters related therewith. It details specific crimes such as illegal access and interference of computer systems, fraud, forgery and data espionage, as well as their punishments which include fines and prison sentences (The Cybercrimes Act, 2015). United Republic of Tanzania also established a National CERT, TZ-CERT, in 2010 and it is operated under the Tanzania Communication Regulatory Authority.

Tanzania still has not signed the African Union Convention on Cybersecurity and Personal Data Protection (The African Union, 2019). The country has no overall cyber strategy or vision and the existing laws don’t deal explicitly with individual privacy and cyber security (ITU, 2018). It is in the process of coming up with a data protection bill as previous laws have not regulated how data should be collected maintained and handled (Green, 2019).

**Rwanda:**

In the Republic of Rwanda, the frameworks for cybercrime and cybersecurity address any acts that threaten the confidentiality, integrity, and availability of computers, and their data. These frameworks safeguard all ICT assets that back up the ICT goals of Rwanda. Rwandan policy is a three-point perspective and includes (i) Safeguarding the core ICT assets against cyberattacks and enhancing cybersecurity education (ii) Responding to cyberattacks by developing local capacities and promoting international collaboration on cybersecurity. The government of Rwanda is promoting awareness by ensuring that its citizens are performing their due diligence on matters pertaining the security of ICT.

Enacted in November 2007, Law No. 55 requires the National Bank of Rwanda to manage the financial industry of Rwanda. The AML/CFT Law No. 47 that was enacted in 2008 ensured that a Financial Investigation Unit was constituted, and finally, the Regulation No. 04 that was enacted in April 2011 defined mobile money operations within Rwanda (UNCTAD, 2011).

Rwanda has Law No 26/2017 that establishes the mission, organization, and functioning of its National Cyber Security Authority. In addition, Law No.24/2016 was set to govern information and communication technologies by establishing a framework for legislation and outlining matters of national interest.

Rwanda has an operational national CSIRT Rw-CSIRT established in 2014 that serves as the national point of contact on cyber security matters for coordination, research, information dissemination on current and emerging cyber threats.
**Burundi:**

In the Republic of Burundi, the Code Pénal Revisé 2009 has Article 467 that specifically addresses computer misrepresentation and Articles 468 - 470 that address computer fraud. Under cybercrime and cybersecurity, the security of the digital economy is captured in Chapter VII (Articles 60 to 72). The Central Bank of Burundi has the mandate of providing the legal and regulatory tools such as (i) Legal Framework for Système Brut de Paiement en Temps Réel au Burundi (ii) Legal Framework for Monetique in Burundi (iii) Legal Framework for mobile banking in Burundi (UNCTAD, 2011).

**South Sudan:**

South Sudan is considered a member of the East African Community. It established the National Communications Authority in 2012 which oversees policy and regulates on matters of technology and communications. Its cyber legislative framework is enshrined in its Penal Code of 2008 particularly sections 388, 389, 390, 391 and 392 that define and address penalties for unauthorized access, computer viruses, manipulation of computer programs and aggravating circumstances in relation to identified offenses.

### 3.4 Gaps in Policy, Legislative and Regulatory Provisions:

Despite these policy, legislative and regulatory efforts, gaps still exist in guiding technology innovation in the financial services sector and in addressing cybersecurity risk. A lack of skilled professionals has brought challenges in the development, implementation and integration of national policy and regulatory frameworks for cybersecurity governance. For instance, it is estimated that there is one certified security professional for every 177,000 people in Africa (Adomako et al., 2018).

Policy makers tend not to have in-depth knowledge and expertise in the technology advancements that are changing the face of banking and financial services and this has brought about gaps in policy and legislative guidance (Schneier, 2019a; UNCTAD, 2011).

Additionally, there is inadequate capacity to formulate and effectively implement cybersecurity legal frameworks to combat the high rate of cybercrime. Due to the spatiality of the internet, cybersecurity cannot be tackled solely at a national level but there are insufficient cybersecurity initiatives in Africa (UNECA, 2014). Only 11 African countries had cybercrime laws, 12 had enacted partial laws, and 30 had no cybercrime laws by 2016 (Adomako et al., 2018).

In many East African Countries there is insufficient police capacity required for the detection, investigation, and prosecution of the those who commit cyber offenses (UNCTAD, 2011). There are no unified laws in Africa that allow cyber criminals to be extradited and insufficient joint-cooperation for cross-border law enforcement in the continent (Jabar et al., 2020).
African countries and firms have not invested heavily in cybersecurity measures and this lack of proper funding has not only deterred the research that needs to go into initiatives for cybersecurity but has also made cybersecurity to become an afterthought in the development and implementation of national policies. Financial constraints have also affected the quality of professionals and tools engaged for cybersecurity risk management (Orji, 2018).

Malebe (2020) points out a number of key gaps with relation to financial technology innovation and cybersecurity risk management. No specific regulations exist for internet e-commerce, cloud computing, big data, artificial intelligence, machine learning, blockchain and cryptocurrencies as discussed in Table 3. Since Kenya is the leader in FinTech adoption and cyber regulation in the East African Region, this table takes the case of Kenya in analyzing gaps in policy, regulatory and legislative provisions regarding FinTech. The findings are representative of other East African countries.

**Table 3: Gaps in Policy, Regulatory and Legislative Provisions relating to FinTech:**

<table>
<thead>
<tr>
<th>Financial Technology Innovation</th>
<th>Specific Regulation</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Mobile Money</td>
<td>Exists</td>
<td>The National Payment Systems Act and The Banking Act give specific regulatory provisions for payment systems and payment service providers and gives CBK powers to regulate this.</td>
</tr>
<tr>
<td>2. Online Banking and E-Commerce</td>
<td>Indirect</td>
<td>Sections of the Kenya Information and Communications Act apply.</td>
</tr>
<tr>
<td>3. Digital Lending</td>
<td>Indirect</td>
<td>The Data Protection Act applies with regard to data privacy and the Banking Act requires CBK to approve financial providers to operate. However, various aspects of lending services such as lending rates are not regulated. The Financial Market Conduct Bill may regulate this when it comes to effect.</td>
</tr>
<tr>
<td>Financial Technology Innovation</td>
<td>Specific Regulation</td>
<td>Remarks</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td>5. Big Data</td>
<td>Indirect</td>
<td>The Data Protection Act applies with regard to data privacy but no regulation data operations and innovation around this.</td>
</tr>
<tr>
<td>6. Artificial Intelligence, Machine Learning</td>
<td>None</td>
<td>The Distributed Ledgers Technology and Artificial Intelligence Task Force under the Ministry of ICT released a report in July 2019 to inform policy formulation and guide projects in key areas. Al Kenya founded in 2017 is a community lobbying for favorable laws relating to Artificial Intelligence and Data Science in Kenya and East Africa.</td>
</tr>
<tr>
<td>7. Robotics and Automation</td>
<td>None</td>
<td>The Distributed Ledgers Technology and Artificial Intelligence Task Force under the Ministry of ICT released a report in July 2019 to inform policy formulation and guide projects in key areas. Al Kenya founded in 2017 is a community lobbying for favorable laws relating to Artificial Intelligence and Data Science in Kenya and East Africa.</td>
</tr>
<tr>
<td>8. Blockchain and Cryptocurrencies</td>
<td>None</td>
<td>The Distributed Ledgers Technology and Artificial Intelligence Task Force under the Ministry of ICT released a report in July 2019 to inform policy formulation and guide projects in key areas.</td>
</tr>
</tbody>
</table>

Policy makers and regulators need to be supportive of technology innovation and its adoption and one popular way of doing this has been through adopting regulatory sandboxes and innovation hubs (Buckley et al., 2020; Omarova, 2020). The introduction of the Whitebox (2018) and Capital Markets Authority (2019) Sandbox are a crucial component in supporting FinTech innovation and adoption while addressing gaps in policy, regulatory and legislative provisions.

The Ministry of ICT Huduma Whitebox functions as an innovation hub with facilities, mentorship, training, coaching, and networking opportunities, particularly for innovators who are helping fulfil the
government’s big four agenda. The government pledges to consume successful inventions as guided by procurement laws.

Innovators are required to apply to the Capital Markets Authority sandbox if their innovations do not clearly fall within existing regulatory provisions. The sandbox gives innovators a yearly lease to deploy and test their innovations under minimal regulatory requirements while giving the regulators an opportunity to study the innovations and formulate specific regulatory guidelines through an evidence-based approach.

3.5 Theories Explaining the Divergence Between Technological Innovations and Policies:

3.5.1 Cultural Lag:
Cultural lag refers to the delay that occurs when nonmaterial culture needs to catch up with material culture and the resultant problems that arise due to this lag (Ogburn, 1957). Changes in technology innovation are considered as part of material culture while the corresponding policies are considered as part of non-material culture. The gap between the emerging technology innovation and required policies to regulation the innovations often results in social conflicts and weakening of social cohesion (Sreedevi, 2016). Emerging technologies present various risks and potential for harm that are capitalized upon by both inadvertent and malevolent actors. How do we provide a cover for their (potentially) disruptive and destructive acts? If policy frameworks are not put in place to address, mitigate, and prevent these risks then cultural lag will be a product of a society struggling to adapt and gain traction with technological innovation and advancement (Schneier, 2019a).

3.5.2 Disruptive Innovation and the Progress Trap of Innovation:
The term disruptive innovation refers to innovations that have a significant impact on a market and on the economic activity of that market (Christensen et al., 2015). Novel innovations take advantage of the gap left at the bottom of the market by meeting the needs of customers using products and services that are simple yet cheaper and more convenient. Once they gain traction in the market, they completely disrupt the market by displacing dominant players. Undoubtedly, disruptive innovation theory holds significant weight in the financial services sector since innovative technologies such as Blockchain and Artificial Intelligence are predicted to redefine traditional and conventional ways of banking. Existing banks will have to embrace digital transformation in order to remain relevant in years to come.

Innovations are continually disrupting the market. They are giving leaders the task of going back to the drawing board to come up with marketing, operational, and innovation strategies that will prove sustainable and relevant in a rapidly evolving and competitive market. However, as incumbents set to
release new technologies into the market, they must remain cognizant that consumers can only take so much innovation at a time. This calls for strategic, structural, and systematic release of novel technologies to avoid depreciating returns, which is termed as the progress trap of innovation. Incumbents are advised to hold on to the release of their subsequent innovations until the market reaches maturity to avoid overwhelming the market. On the other hand, firms should not take light years to give their customers new products and service lest they lose their niche in the market. Therefore, for firms to stay competitively relevant they must learn the art of striking a neat and strategic balance between sustaining their current releases and promoting novel innovations (Christensen et al., 2017).

3.6 Potential Strategies and Policy Towards New Technologies:

The governance of technology innovations should be emphasized as a core security priority for pre-emptive cybersecurity risk mitigation. (Schneier, 2019a, 2019b) emphasizes the need to have policies strictly governing the revolutionizing technological space before these advancements create problems for society. It is also important to increase policy makers understanding of innovative technologies and to co-opt technologists to policy making organs. Technologists and policymakers must collaborate to make effective policies for technological advancements.

Oluoch (2018) proposes various recommendations for banks to: invest more in updating and fortifying their protective systems including access control systems that require multi-factor authentication and recognize multiple failed login attempts, firewalls for filtering traffic, intrusion detection and prevention systems, data loss protection technologies and secure remote-access and network communication solutions.

Organizations surveyed as part of this study also identified the challenges they experienced when handling cybersecurity risk as illustrated in Figure 8. The greatest challenges were in relation to limited budget allocation for cybersecurity tools, lack of appropriate skills, poor organization cyber culture and ever evolving threats. These are areas organizations should address and push additional resources towards in order to address cyber risks effectively.
3.7 Potential Cyber Risk Management Strategies and Policy Applications:

Participants engaged in this study also shared cyber risk management strategies that they were using to address cybersecurity risk. As relates to pre-emptive controls, the respondents reported the extent to which they implemented those listed in Figure 9. Those that were more prevalently implemented were: network firewalls, anti-malware, backups, domain access management, information security policies, system auditing, security education training and awareness, log management, network intrusion detection and prevention systems, data loss prevention systems, penetration testing, use of proxy servers, asset management, patch management, encryption, web application firewall and incident response teams. Those least implemented included data classification, digital forensics and security operation centers.
Figure 9: Controls Used to Mitigate Cybersecurity Risks

Key:
0: Not at all: we have not implemented the control
1: Small extent: We are in the process of implementing the control
2: Moderate Extent: We have implemented the control but not extensively across the organisation
3: Great Extent: We have implemented the control extensively across the entire organisation
4: Very Great Extent: Gone above and beyond. We benchmark with industry leaders.

Additional measures recommended by the survey participants included: appropriate continuous monitoring, patch management, role-based access control, regular penetration testing, Virtual Private Cloud networks, and partnerships with existing firms to leverage on expertise.

**Recommendations for risk minimization** included: upskilling and retention of cybersecurity personnel, proper user awareness training, appropriate investment in cybersecurity skills and tools, regular asset assessment and penetration tests, full-service internet security suites, strong passwords,
software updates and service auditing.

**Recommendations for adaptive measures** that they can employ to continuously improve on their approach to addressing cyber security risk included: continuous and enhanced monitoring of risks, continuous diagnosis of mitigating controls, adherence to cybersecurity policies, proper change management, information sharing and that risk acceptance must be signed off at the top to reflect responsibility acceptance and awareness of the choice.

**Recommendations for enhancement measures** included: continuous monitoring and evaluation, continuous security audits, feedback loop between risk and control remediation to ensure constant growth, patch management, penetration tests, investment in cybersecurity technologies, collaboration with national, regional, and global Computer Incidence Response Teams (CIRTS) and undertaking accurate risk assessment to help when designing strategies for addressing cybersecurity risks.

**Discussion and Recommendations:**

Results from this study reveal key take-outs regarding technology innovation by banks in the East Africa region and the associated cybersecurity risks. Intellecap, Financial Sector Deepening-Africa, FMO, and UKAid shows that USD $722 million has been invested into FinTech in East Africa during the period 2010 to 2017 with Kenya receiving the largest investment. The top five technology advancements that are revolutionizing the East African banking industry are: mobile banking, online banking, open banking, bank assurance and cloud computing. The drive for the adoption of these technology innovations is to provide quick access to 24/7 banking services, increase operational efficiencies while driving down costs. During the COVID-19 pandemic, these technologies have also lowered the need for person-to-person interaction and have provided flexible work options and business continuity when people have had to work from home. Additionally, East African banks have not yet operationalized artificial intelligence and have a negative perception of blockchain technologies despite these technologies having potential benefits in mitigating cybersecurity risks and fighting fraud.

With regard to cybersecurity risk, banks are facing huge risks relating to financial fraud, data theft and malware attacks. The greatest source of these risks are malicious insiders and organized crime syndicates. This is because of the presence of homegrown organized criminal actors such as SilentCards that have successfully stolen billions of shillings using customized malware on ATMs and infiltrating financial systems with the help of accomplice insiders.

There have been commendable advancements in the enactment of cybercrime and data protection
legislation by East African countries following the establishment of the 2014 African Union Convention on Cyber Security and Personal Data Protection. Such legislation makes it possible to prosecute cybercriminals and act as a deterrent factor when enforced. However, a number of technology innovations in the banking sector such as artificial intelligence, blockchain and cryptocurrencies are yet to have policy guidance due to their nascent stages of development. A leading model used by regulators is to have these emerging FinTech innovations first observed in a controlled sandbox environment before being allowed into the market. Regulators are keen not to stifle innovation while ensuring their policy guidelines are well informed to avert negative outcomes and cybersecurity risks.

Technology controls that East African banks found to be essential were in relation to network firewalls, anti-malware solutions, backups, domain access management, information security policies, system auditing, security education training and awareness and log management. Those least implemented included data classification, digital forensics and security operation centers. Processes relating to regular patch management, penetration testing, risk assessments and incidence response through a coordinated response team and security operations center were found to be essential.

There is a notable shortage of skilled and experienced professionals needed in the formulation, implementation and enforcement of cybersecurity best practices and policies. Policy makers, law enforcement and the judicial officers lack requisite cybersecurity training and expertise to guide the changing face of technology innovation and to avert potential cybersecurity risks. More investment needs to be made in human resource development and a lot more co-operation needs to take place between FinTech innovators and regulatory bodies to ensure technology innovation delivers desired benefits while avoiding pitfalls and cybersecurity risks.
References:


