CYBERCRIME AND INFORMAL ECONOMIES: LEGAL CHALLENGES, ECONOMIC DISRUPTIONS, AND SOCIAL WORK INTERVENTIONS

Eneh, N.[1]*; Chizurum, E. I.[2]; Eneh, C.[3]
[1]Ministry of Justice, Enugu state, Nigeria
[2]Department of Social work, University of Nigeria, Nsukka
[3]Department of Agricultural economics, University of Nigeria, Nsukka
*Author of correspondence; Email: enehnkechi@gmail.com

ABSTRACT

Cybercrime increasingly threatens informal economic activities in developing regions, undermining livelihoods, income stability, and social equity. Informal workers—such as traders, artisans, and small-scale entrepreneurs—operate with limited legal recognition and face high exposure to digital fraud, identity theft, and mobile payment scams. This study employs a mixed-method approach, combining quantitative analysis of income disruption and regression modeling with qualitative interviews and legal-policy review, to examine the impact of cybercrime on informal economies. Findings reveal significant economic disruption, disproportionate vulnerability of low-digital-literacy actors, and systemic gaps in legal and institutional protections. The study highlights the pivotal role of social work interventions, including digital literacy programs, advocacy, and community resilience-building, in mitigating risks and supporting recovery. Policy recommendations focus on inclusive cybersecurity laws, enhanced reporting mechanisms, financial inclusion with built-in safeguards, targeted support for vulnerable groups, and multi-layered public-private partnerships. By integrating legal, economic, and social dimensions, the study contributes to understanding cybercrime's multidimensional effects and presents actionable strategies for sustainable protection and development.

***Keywords*:** Cybercrime, Informal economies, Digital literacy, Social work interventions, Legal protection, Economic disruption, Financial inclusion

1. INTRODUCTION

The rapid expansion of digital technologies has fundamentally transformed economic systems across the globe, including the structure and functioning of informal economies. While digitalization has enhanced access to financial services, markets, and information, it has simultaneously introduced new vulnerabilities, particularly in developing regions where institutional safeguards remain weak (World Bank, 2022; UNCTAD, 2021). Among these vulnerabilities, cybercrime has emerged as a critical threat, disproportionately affecting informal economic actors who often lack the resources and protection mechanisms available to formal sector participants (Kshetri, 2010; Anderson et al., 2019).

1.1 Definition and importance of informal Economies in Developing regions

The informal economy broadly refers to economic activities that are not regulated, taxed, or protected by formal legal and institutional frameworks (Chen, 2012). It encompasses a wide range of activities, including small-scale trading, artisanal production, subsistence agriculture, and service provision, which are often characterized by low capital intensity and limited access to formal

financial systems (International Labour Organization [ILO], 2018). In developing countries, the informal sector plays a crucial role in employment generation, poverty reduction, and livelihood sustenance, accounting for more than 60% of total employment globally (ILO, 2018; Schneider et al., 2010).

Beyond its role in employment, the informal economy contributes significantly to economic resilience, particularly during periods of economic shocks and structural adjustment (Chen, 2012). However, its exclusion from formal regulatory and protection systems exposes participants to multiple risks, including financial insecurity, exploitation, and, increasingly, digital vulnerabilities (UNCTAD, 2021).

1.2 Growth of digital participation

In recent years, there has been a notable increase in digital participation among informal workers, driven by the proliferation of mobile technologies, fintech innovations, and digital platforms. Mobile banking, online marketplaces, and digital payment systems have enabled informal actors to expand their market reach, improve efficiency, and access financial services that were previously unavailable (Donou-Adonsou et al., 2016; World Bank, 2022). For instance, mobile money services have significantly enhanced financial inclusion in many developing countries by providing accessible and affordable transaction platforms (Suri & Jack, 2016).

Similarly, the rise of e-commerce and social media platforms has facilitated informal trade by connecting sellers directly with consumers, thereby reducing transaction costs and market barriers (UNCTAD, 2021). Fintech solutions, including digital lending and savings applications, have further supported entrepreneurial activities within the informal sector (OECD, 2020). Despite these benefits, the rapid adoption of digital technologies has often outpaced the development of adequate security measures and regulatory frameworks, thereby increasing exposure to cyber risks.

1.3 Rising exposure to Cyber threats

The increasing integration of digital tools into informal economic activities has led to a corresponding rise in exposure to cyber threats, including fraud, identity theft, phishing, and mobile money scams. Cybercriminals often target vulnerable populations with limited digital awareness and weak security practices, making informal workers particularly susceptible (Kshetri, 2010; Leukfeldt, 2014). Evidence suggests that cybercrime has evolved into a global industry with significant economic costs, affecting both individuals and businesses (Anderson et al., 2019).

In developing contexts, mobile-based fraud and social engineering attacks are especially prevalent, exploiting trust-based networks and information asymmetries (UNODC, 2013). Identity theft and unauthorized access to digital financial accounts can lead to substantial income losses and business disruptions, which are particularly devastating for informal workers who rely on daily earnings (World Bank, 2022). These threats not only undermine economic stability but also erode trust in digital systems, thereby limiting the potential benefits of digital inclusion.

1.4 Key Issues

i. Lack of regulation and protection

One of the primary challenges facing informal workers in the digital economy is the lack of effective regulatory frameworks and legal protections. Informal economic activities often fall outside the scope of formal legal systems, leaving participants without access to legal recourse in cases of cybercrime (Chen, 2012; UNCTAD, 2021). Additionally, existing cybercrime laws in many developing countries are either inadequate or poorly enforced, further exacerbating vulnerabilities (Wall, 2007; UNODC, 2013).

ii. Limited Digital literacy

Digital literacy plays a critical role in enabling individuals to navigate online environments safely and effectively. However, many informal workers possess limited knowledge of digital security practices, making them more susceptible to cyber threats (OECD, 2020). Low levels of education and limited access to training further constrain their ability to identify and respond to cyber risks, thereby increasing their exposure to fraud and exploitation (World Bank, 2022).

iii. Weak Institutional support

Institutional support mechanisms, including law enforcement, financial institutions, and social protection systems, are often inadequate in addressing the needs of informal workers affected by cybercrime. Weak coordination among institutions, bureaucratic inefficiencies, and limited resources hinder effective response and recovery efforts (UNODC, 2013). As a result, victims of cybercrime in the informal sector frequently lack access to compensation, legal assistance, and psychosocial support (Midgley, 2014).

1.5 Research Questions

In light of these challenges, this study seeks to address the following research questions:

1. How does cybercrime disrupt informal economic activities?
2. What legal gaps expose informal workers to cyber risks?
3. What role can social work play in mitigation and recovery?

1.6 Contribution and Originality

This study makes several important contributions to the existing literature. First, it bridges the gap between cybercrime research and informal economy studies by providing an integrated analysis of how digital risks affect informal economic systems. While prior studies (Kopp et al., 2017; Midgley, 2014; Kshetri, 2010) have examined cybercrime primarily from technological or criminological perspectives, this research adopts a multidisciplinary approach that incorporates economic, legal, and social dimensions.

Second, the study provides empirical evidence on the economic impact of cybercrime within the informal sector, an area that remains underexplored in current research. By employing a mixed-method approach, it captures both quantitative and qualitative dimensions of cybercrime-related disruptions.

Third, the study highlights the critical role of social work interventions in addressing cybercrime impacts, thereby extending the discourse beyond traditional policy and regulatory frameworks. By emphasizing community-based support, digital literacy, and advocacy, the research contributes to the development of inclusive and sustainable strategies for mitigating cyber risks.

Overall, this study advances understanding of the intersection between digital transformation, vulnerability, and development, and provides actionable insights for policymakers, practitioners, and researchers seeking to promote secure and inclusive digital economies.

2.0 Literature review

2.1 Informal Economies and Digital Transformation

i. Characteristics of Informal sectors

The informal economy comprises economic activities that operate outside formal regulatory, taxation, and legal frameworks, often characterized by low entry barriers, small-scale operations, and reliance on family labor (Chen, 2012; International Labour Organization [ILO], 2018). These activities typically lack formal contracts, social protection, and institutional oversight, making participants vulnerable to economic and social risks (Schneider et al., 2010). Informality is also associated with limited access to finance, infrastructure, and legal systems, which constrains productivity and growth (La Porta & Shleifer, 2014).

ii. Role in employment and economic development

Despite its structural limitations, the informal sector plays a critical role in employment generation and economic development, particularly in developing countries. It accounts for a significant share of total employment and serves as a primary source of livelihood for marginalized populations, including women and youth (ILO, 2018). The sector also contributes to poverty reduction and economic resilience by providing flexible income opportunities during economic downturns (Chen, 2012). However, its exclusion from formal systems limits its potential for productivity enhancement and sustainable growth (World Bank, 2022).

iii. Increasing Digitization (Mobile Money, Online Marketplaces)

Recent years have witnessed a rapid increase in the digitization of informal economic activities, driven by mobile technologies, fintech innovations, and online platforms. Mobile money services have expanded financial inclusion by enabling secure and convenient transactions for previously unbanked populations (Suri & Jack, 2016). Similarly, online marketplaces and social media platforms have facilitated market access, allowing informal traders to reach broader customer bases (UNCTAD, 2021). While digitization enhances efficiency and economic opportunities, it also introduces new risks, particularly in environments with weak regulatory frameworks (OECD, 2020).

2.2 Cybercrime in low-regulation environments

a. Types of Cybercrime affecting informal actors

i. Mobile fraud: Mobile fraud, including unauthorized transactions and SIM swap fraud, has become increasingly prevalent in developing countries, where mobile money systems are widely used (Kshetri, 2010). Informal workers are particularly vulnerable due to limited awareness of security practices and reliance on mobile platforms for financial transactions (UNODC, 2013).

ii. Phishing and scams: Phishing attacks and online scams exploit human vulnerabilities by deceiving individuals into revealing sensitive information such as passwords and financial details. These attacks often

target individuals with low digital literacy, making informal sector participants prime victims (Leukfeldt, 2014). Social engineering techniques further amplify the effectiveness of such scams in trust-based communities (Anderson et al., 2019).

iii. Digital payment exploitation: Digital payment systems, while facilitating transactions, are also susceptible to exploitation through hacking, malware, and fraudulent applications. Weak security infrastructures and inadequate user awareness contribute to increased risks of financial loss (Kopp et al., 2017).

b. Structural vulnerabilities

The vulnerability of informal actors to cybercrime is rooted in structural factors, including limited digital literacy, lack of access to secure technologies, and absence of institutional protection (OECD, 2020). Additionally, socioeconomic inequalities and digital divides exacerbate exposure to cyber risks, particularly in rural and low-income communities (Donou-Adonsou et al., 2016). These structural vulnerabilities create an enabling environment for cybercriminal activities, especially in low-regulation contexts.

2.3 Legal frameworks and enforcement gaps

i. Overview of Cybersecurity and Cybercrime laws

Many countries have developed legal frameworks to address cybercrime, including laws on data protection, electronic transactions, and cybersecurity (UNODC, 2013). These frameworks aim to deter cybercriminal activities, protect users, and enhance digital trust. However, the effectiveness of such laws varies significantly across regions, particularly in developing countries where institutional capacity is limited (Wall, 2007).

ii. Challenges

a. Limited coverage of informal actors: Existing legal frameworks often focus on formal sector entities, leaving informal workers outside the scope of protection. This exclusion limits access to legal recourse and compensation mechanisms for victims of cybercrime (Chen, 2012; UNCTAD, 2021).

b. Weak enforcement capacity: Weak enforcement capacity, including inadequate technical expertise, limited resources, and corruption, undermines the effectiveness of cybercrime laws (UNODC, 2013). Law enforcement agencies often struggle to investigate and prosecute cyber offenses, particularly in complex and transnational cases (Kshetri, 2010).

c. Jurisdictional and reporting barriers: Cybercrime often transcends national boundaries, creating jurisdictional challenges for enforcement. Additionally, underreporting of cyber incidents is common among informal workers due to lack of awareness, distrust in institutions, and perceived inefficacy of legal processes (Anderson et al., 2019).

2.4 Economic disruptions

i. Income loss and business instability: Cybercrime has significant economic implications, including direct financial losses and disruption of business operations. Informal workers, who rely on daily income, are particularly affected by such disruptions, which can lead to immediate livelihood crises (World Bank, 2022).

ii. Reduced trust in digital systems: Repeated exposure to cyber threats can erode trust in digital platforms,

discouraging adoption and limiting the benefits of digital inclusion (OECD, 2020). This loss of trust can hinder economic participation and slow the growth of digital economies (UNCTAD, 2021).

iii. Market inefficiencies and reduced productivity: Cybercrime contributes to broader market inefficiencies by increasing transaction costs, reducing productivity, and diverting resources toward risk mitigation (Kopp et al., 2017). These effects are particularly pronounced in informal economies, where resources are already constrained.

2.5 Social Work and Community-based interventions

i. Role of Social Workers in digital inclusion: Social workers play a critical role in promoting digital inclusion by facilitating access to technology, providing education, and advocating for marginalized populations (Midgley, 2014). Their involvement is essential in bridging the digital divide and enhancing resilience against cyber risks.

ii. Community Education and advocacy: Community-based education programs can improve digital literacy and awareness of cyber threats, thereby reducing vulnerability. Social workers and community organizations can deliver targeted interventions that address the specific needs of informal workers (OECD, 2020).

iii. Crisis intervention and recovery support: In the aftermath of cyber incidents, social workers can provide psychosocial support, financial counseling, and linkage to legal and institutional resources. Such interventions are crucial for recovery and rebuilding trust in digital systems (Midgley, 2014).

2.6 Research gap

Despite the growing body of literature on cybercrime and informal economies, there remains a significant gap in integrated analyses that combine these domains. Existing studies (Kshetri, 2010; Kopp et al., 2017) often examine cybercrime from technological or criminological perspectives, with limited attention to its economic and social implications for informal workers. Similarly, research (Chen, 2012) on informal economies tends to overlook the impact of digital risks and cyber vulnerabilities.

Furthermore, there is a lack of interdisciplinary approaches that incorporate legal, economic, and social dimensions, particularly in the context of developing countries. The role of social work in addressing cybercrime impacts is also underexplored, despite its potential to enhance resilience and recovery (Midgley, 2014). This study seeks to address these gaps by providing a comprehensive analysis of cybercrime, informal economies, and intervention strategies.

3.0 Theoretical Framework

This study is grounded in an interdisciplinary theoretical framework that integrates insights from Informal Economy Theory, Routine Activity Theory, Law and Economics Theory, and the Social Justice Framework. These perspectives collectively provide a robust analytical lens for understanding the intersection of cybercrime, informal economic activities, legal vulnerabilities, and social intervention mechanisms.

3.1 Informal Economy Theory: structure and vulnerabilities outside formal regulation

Informal Economy Theory explains the existence and persistence of economic activities that operate outside formal institutional and regulatory systems. According to this perspective, informality arises due to structural constraints such as excessive regulation, limited access to formal employment, and socioeconomic inequalities (Chen, 2012; La Porta & Shleifer, 2014). Informal enterprises are typically characterized by low capital intensity, absence of formal contracts, and limited access to legal protections and financial services (International Labour Organization [ILO], 2018).

While the informal economy provides essential livelihood opportunities and contributes significantly to employment and economic resilience, it also exposes participants to heightened vulnerabilities (Schneider et al., 2010). The absence of formal oversight and institutional support increases susceptibility to exploitation, financial instability, and, in the context of digital transformation, cybercrime risks (UNCTAD, 2021). This theoretical perspective is critical for understanding why informal workers are disproportionately affected by cyber threats and lack adequate mechanisms for protection and recovery.

3.2 Routine Activity Theory (Crime Perspective): exposure and lack of Guardianship

Routine Activity Theory, developed by Cohen and Felson (1979), provides a criminological framework for understanding the occurrence of crime based on the convergence of three elements: a motivated offender, a suitable target, and the absence of capable guardianship. In the context of cybercrime, informal workers often represent suitable targets due to their limited digital literacy and reliance on insecure digital platforms (Leukfeldt, 2014).

The increasing digitization of informal economic activities has expanded exposure to cyber threats, while the lack of institutional safeguards and cybersecurity awareness reflects the absence of capable guardianship (Kshetri, 2010). Cybercriminals exploit these vulnerabilities through phishing, mobile fraud, and digital payment manipulation, particularly in low-regulation environments (Anderson et al., 2019). Routine Activity Theory thus provides a useful lens for explaining how structural and behavioral factors interact to increase cybercrime risks among informal economic actors.

3.3 Law and Economics Theory: enforcement, deterrence, and incentives

Law and Economics Theory emphasizes the role of legal frameworks and enforcement mechanisms in shaping behavior through incentives and deterrence (Becker, 1968). According to this perspective, individuals engage in criminal activities when the expected benefits outweigh the expected costs, which are influenced by the probability of detection and severity of punishment.

In many developing contexts, weak legal frameworks, limited enforcement capacity, and low conviction rates reduce the deterrent effect of cybercrime laws (UNODC, 2013; Wall, 2007). Informal workers, who are often excluded from formal legal systems, face additional challenges in accessing justice and compensation (Chen, 2012). This creates an environment where cybercriminal activities

can flourish with minimal risk, while victims bear significant economic costs.

Furthermore, the lack of clear legal protections and enforcement mechanisms undermines trust in digital systems and discourages participation in formal economic activities (OECD, 2020). Law and Economics Theory therefore highlights the importance of strengthening legal institutions and aligning incentives to reduce cybercrime and protect vulnerable populations.

3.4 Social Justice Framework: equity, inclusion, and protection of vulnerable populations

The Social Justice Framework emphasizes the principles of equity, inclusion, and the protection of marginalized and vulnerable populations within society (Rawls, 1971; Midgley, 2014). In the context of informal economies, this framework underscores the need to address structural inequalities that limit access to resources, opportunities, and protections.

Cybercrime exacerbates existing social inequalities by disproportionately affecting individuals with limited digital literacy, low income, and weak institutional support (World Bank, 2022). Informal workers often lack the social, economic, and legal capital required to recover from cyber-related losses, leading to deeper marginalization and exclusion.

Social work interventions, grounded in social justice principles, play a critical role in addressing these challenges by promoting digital inclusion, providing education and awareness, and advocating for inclusive policies (Midgley, 2014). This framework is essential for understanding the broader societal implications of cybercrime and the need for holistic and inclusive intervention strategies.

3.5 Conceptual Link

The integration of these theoretical perspectives informs the conceptual framework of this study, which posits a sequential and interrelated relationship between cybercrime and socioeconomic outcomes in informal economies. Cybercrime acts as a primary disruptive force that directly impacts informal economic activities through financial losses, business interruptions, and reduced productivity (Anderson et al., 2019). These disruptions lead to increased economic vulnerability, as informal workers often lack savings, insurance, and institutional support mechanisms (Chen, 2012). Over time, this vulnerability contributes to broader social inequality, reinforcing existing disparities in income, access to resources, and opportunities (World Bank, 2022).

The framework further posits that legal and social interventions serve as critical mitigating mechanisms. Effective legal frameworks and enforcement strategies can deter cybercrime and provide protection for victims, while social work interventions can enhance resilience through education, support, and advocacy (OECD, 2020; Midgley, 2014). The interaction between these elements highlights the need for a multidimensional approach to addressing cybercrime in informal economies.

In summary, the conceptual linkage can be represented as follows:

Cybercrime → Economic Disruption → Increased Vulnerability → Social Inequality

Legal and Social Interventions → Mitigation and Recovery

This integrated theoretical framework provides a comprehensive basis for analyzing the research questions and guiding empirical investigation.

4.0 METHODOLOGY

This study adopts a mixed-method research approach to examine the relationship between cybercrime and informal economies, with a particular focus on legal challenges, economic disruptions, and social work interventions. The methodology integrates quantitative and qualitative techniques to provide a comprehensive and triangulated understanding of the research problem, consistent with best practices in interdisciplinary research (Creswell & Plano Clark, 2018).

4.1 Research design

A mixed-method research design was employed, combining quantitative and qualitative approaches to enhance the robustness and validity of findings. The quantitative component focuses on economic impact analysis, specifically examining the relationship between cybercrime exposure and income loss among informal workers. This approach enables the identification of statistical patterns and causal relationships (Wooldridge, 2013).

The qualitative component complements the quantitative analysis through semi-structured interviews and legal/policy reviews. This approach provides deeper insights into the lived experiences of informal workers, institutional challenges, and the effectiveness of legal frameworks (Yin, 2018). The integration of both methods allows for methodological triangulation, improving the reliability and comprehensiveness of the study (Creswell & Plano Clark, 2018).

4.2 Data sources

The study utilizes multiple data sources to ensure a comprehensive analysis of the research questions. First, primary data were collected through structured surveys administered to informal workers, including traders, artisans, and small-scale entrepreneurs in urban, semi-urban and rural areas of Enugu state, Nigeria. These surveys captured information on income levels, cybercrime exposure, digital literacy, and access to legal protection. Survey-based approaches are widely used in informal sector research due to their ability to capture micro-level socioeconomic dynamics (Chen, 2012).

Second, secondary data on cybercrime incidents were obtained from national databases, as well as reports from telecommunications and financial institutions. These sources provide contextual information on the prevalence and types of cyber threats affecting digital users (UNODC, 2013; World Bank, 2022).

Third, legal documents and policy frameworks related to cybersecurity, digital finance, and consumer protection were reviewed to assess the adequacy of existing regulatory systems. Legal analysis is essential for understanding institutional gaps and enforcement challenges (Wall, 2007).

Finally, socioeconomic indicators, including income levels, education, and digital access, were incorporated to control

for structural factors influencing vulnerability to cybercrime. These indicators are critical for analyzing disparities within the informal economy (ILO, 2018).

4.3 Model specification

To empirically assess the impact of cybercrime on informal economic activities, the study specifies an econometric model in which income loss or business disruption serves as the dependent variable. This variable captures the economic consequences of cybercrime at the individual level.

The key independent variables include cybercrime exposure, digital literacy level, and access to legal protection. Cybercrime exposure is measured using an index based on the frequency and severity of cyber incidents experienced by respondents. Digital literacy is assessed using a composite score reflecting respondents' ability to use digital tools and identify cyber risks. Access to legal protection is captured as a binary variable indicating whether respondents have access to formal legal or institutional support mechanisms.

Control variables include education level, location (urban or rural), and type of informal activity. These variables account for heterogeneity among respondents and help isolate the effect of cybercrime exposure on economic outcomes (Wooldridge, 2013). The baseline econometric model is specified as follows:

$$Y_i = \beta_0 + \beta_1 CE_i + \beta_2 DL_i + \beta_3 LP_i + \beta_4 X_i + \varepsilon_i$$

Where:

- Y_i = Income loss or business disruption
- CE_i = Cybercrime exposure
- DL_i = Digital literacy level
- LP_i = Access to legal protection
- X_i = Vector of control variables (education, location, type of activity)
- ε_i = Error term

This specification is consistent with empirical studies analyzing the economic impacts of risk factors in developing contexts (Kopp et al., 2017).

4.4 Analytical Techniques

A combination of quantitative and qualitative analytical techniques was employed to address the research questions.

Regression analysis

Ordinary Least Squares (OLS) regression was used as the primary estimation technique to examine the relationship between cybercrime exposure and income loss. OLS is appropriate for continuous dependent variables and provides unbiased and efficient estimates under standard assumptions (Wooldridge, 2013). Where applicable, robustness checks using logistic or panel models were considered to validate findings.

Descriptive statistics

Descriptive statistics were used to summarize the characteristics of the sample population and key variables. Measures such as means, standard deviations, and frequency distributions provide insights into the extent of cybercrime exposure, levels of digital literacy, and access to legal protection among informal workers (Field, 2013).

Thematic analysis for qualitative data

Qualitative data from interviews and policy documents were analyzed using thematic analysis. This method involves identifying, coding, and interpreting patterns or themes within the data (Braun &

Clarke, 2006). Thematic analysis is particularly suitable for exploring complex social and institutional issues, such as legal gaps and social work interventions.

The analysis followed a systematic process, including data familiarization, coding, theme development, and interpretation. This approach enabled the identification of key themes related to cybercrime experiences, legal challenges, and coping mechanisms among informal workers.

4.5 Ethical considerations

Ethical considerations (Yin, 2018) were strictly adhered to throughout the research process. Informed consent was obtained from all participants, and confidentiality was maintained by anonymizing responses. The study also ensured that participants were not exposed to harm or undue risk, particularly given the sensitive nature of cybercrime experiences.

4.6 Methodological limitations

While the mixed-method approach enhances the robustness of the study, certain limitations should be acknowledged. Self-reported data may be subject to recall bias or underreporting, particularly in relation to cybercrime incidents (Anderson et al., 2019). Additionally, the cross-sectional nature of the data limits the ability to establish causal relationships over time. Despite these limitations, the integration of multiple data sources and analytical techniques strengthens the validity of the findings.

5. Results and findings

5.1 Descriptive statistics

The descriptive statistics provide an overview of the socioeconomic characteristics of respondents and the extent of cybercrime exposure within the informal economy. A total of 412 informal workers (traders, artisans, and small-scale entrepreneurs) were surveyed across urban and rural locations.

Table 1: Descriptive statistics of key variables

Variable	Mean	Std. Dev.	Min	Max
Income Loss (₦, monthly)	45,320	28,115	5,000	150,000
Cybercrime Exposure (index 0–1)	0.62	0.21	0.10	0.95
Digital Literacy (scale 1–5)	2.87	1.02	1.00	5.00
Access to Legal Protection (0/1)	0.34	0.47	0	1
Years of Education	9.8	4.3	0	18
Urban Location (0/1)	0.56	0.50	0	1

The results indicate a relatively high level of cybercrime exposure among informal workers (mean = 0.62), reflecting increasing digital integration without corresponding safeguards. The average digital literacy level remains moderate (2.87), suggesting limited capacity to identify and mitigate cyber risks. Only 34% of respondents reported having access to any form of legal protection, underscoring systemic institutional gaps. These findings align with prior studies indicating that informal sector participants are particularly vulnerable due to low institutional coverage and limited digital skills (Kshetri, 2010; UNCTAD, 2021).

5.2 Regression analysis

To examine the relationship between cybercrime exposure and economic disruption, an Ordinary Least

Squares (OLS) regression model was estimated.

Table 2: OLS Regression results (Dependent Variable: Income Loss)

Variable	Coefficient (β)	Std. Error	t-Statistic	p-value
Cybercrime Exposure	28,540***	4,210	6.78	0.000
Digital Literacy	-8,120**	2,980	-2.73	0.007
Legal Protection Access	-12,450***	3,560	-3.50	0.001
Education	-1,210	780	-1.55	0.122
Urban Location	5,870*	3,120	1.88	0.061
Constant	22,300	6,540	3.41	0.001
R^2	0.47			
N	412			

*Significance levels: *p < 0.1, **p < 0.05, ***p < 0.01*

The regression result reveal that cybercrime exposure has a strong positive and statistically significant effect on income loss (β = 28,540, p < 0.01), indicating that increased exposure leads to substantial financial disruption. This finding supports existing literature highlighting cybercrime as a growing economic threat, particularly in digitally transitioning economies (Anderson et al., 2019; Kopp et al., 2017).

Digital literacy exhibits a significant negative relationship with income loss (β = -8,120, p < 0.05), suggesting that higher levels of digital competence reduce vulnerability to cyber threats. Similarly, access to legal protection significantly reduces income loss (β = -12,450, p < 0.01), emphasizing the protective role of institutional frameworks. These findings are consistent with studies emphasizing the importance of digital skills and legal infrastructure in mitigating cyber risks (OECD, 2020; World Bank, 2022).

Urban location shows a marginally significant positive effect, indicating that urban informal workers may face higher cyber risks due to greater digital exposure, corroborating findings from developing economies (Donou-Adonsou et al., 2016).

5.3 Thematic Analysis (Qualitative Findings)

The qualitative component, based on 32 semi-structured interviews and policy document reviews, revealed three dominant themes:

Theme 1: Cybercrime-induced economic disruption

Respondents frequently reported financial losses due to online fraud, mobile money scams, and phishing attacks. Many participants indicated that cyber incidents directly affected their working capital and disrupted daily operations.

"I lost my entire weekly sales through a fake bank alert scam… I had no backup or support." (Trader 3, Ogbete (Urban) Market)

This supports prior findings that cybercrime disproportionately impacts small and informal businesses lacking risk mitigation mechanisms (Leukfeldt, 2014).

Theme 2: Legal and institutional gaps

A significant number of respondents expressed lack of awareness of legal recourse or inability to access justice mechanisms. Weak enforcement and bureaucratic barriers were commonly cited.

"Even when I reported, nothing happened… I don't think the system protects people like us." (Artisan 2, Opi Market (Rural Area))

Policy analysis further revealed fragmentation in cybercrime legislation and weak enforcement structures, particularly regarding informal sector protection. This aligns with evidence that legal systems often lag behind technological advancements, especially in developing contexts (Wall, 2007; UNODC, 2013).

Theme 3: Role of social support and digital literacy

Participants emphasized the importance of community support, awareness programs, and digital education in mitigating cyber risks. Social networks often served as informal coping mechanisms.

"It was through a cooperative group that I learned how to avoid scams." (Entrepreneur, (Ogige Market) Semi-urban)

This finding underscores the potential role of social work interventions in awareness creation, recovery support, and resilience building, consistent with development-oriented social protection frameworks (Midgley, 2014).

6.0 Summary of key Findings

- Cybercrime significantly disrupts informal economic activities through income loss and business instability.
- Digital literacy and legal protection are critical mitigating factors.
- Informal workers face substantial legal and institutional exclusion.
- Social and community-based interventions play a key role in coping and recovery.

7.0 Discussion

The findings of this study provide strong empirical and qualitative evidence that cybercrime constitutes a significant and growing threat to informal economic systems. The positive and statistically significant relationship between cybercrime exposure and income loss confirms that informal workers are highly vulnerable to digital risks, particularly in contexts characterized by weak institutional support and limited regulatory coverage. This directly addresses the first research question and aligns with global evidence (Anderson et al., 2019) that cybercrime imposes disproportionate costs on less protected economic actors.

A critical insight from this study is the structural vulnerability of the informal economy. Unlike formal sector entities, informal workers often lack access to legal protections, insurance mechanisms, and formal dispute resolution systems. The regression results and thematic findings jointly demonstrate that limited access to legal protection exacerbates economic losses, highlighting systemic legal gaps. This finding supports existing scholarship (Chen, 2012; UNCTAD, 2021) that emphasizes the exclusion of informal actors from formal governance frameworks.

The role of digital literacy emerges as a key mitigating factor. The negative relationship between digital literacy and income loss suggests that improving digital competencies can significantly reduce vulnerability to cyber threats. This finding is consistent with prior studies (OECD, 2020) linking digital inclusion to economic resilience and security. However, the relatively low average digital literacy observed indicates a critical need for targeted capacity-building interventions.

The interaction between weak legal systems, economic vulnerability, and social exclusion further explains why informal economies are disproportionately affected. Informal workers operate at the intersection of limited state protection and increasing digital exposure, creating a "double vulnerability" effect. This aligns with theoretical perspectives on structural inequality and digital divides in developing economies (Donou-Adonsou et al., 2016; World Bank, 2022).

Importantly, the qualitative findings highlight the potential of social work interventions in addressing cybercrime impacts. Social workers can play a pivotal role in awareness creation, digital literacy training, psychosocial support, and advocacy for inclusive policies. This expands the discourse on cybercrime beyond technical and legal frameworks to include social and developmental dimensions, consistent with integrated development approaches (Midgley, 2014).

From a policy perspective, the findings suggest the need for a multi-dimensional approach that integrates legal reform, digital education, and social protection. Strengthening cybercrime legislation, improving enforcement mechanisms, and extending legal protections to informal workers are essential steps. Additionally, investment in digital literacy programs and community-based interventions can enhance resilience and reduce exposure to cyber risks.

Overall, this study contributes to the literature by bridging the gap between cybercrime research and informal economy analysis, while also highlighting the critical role of social work in mitigating digital-era vulnerabilities. The findings underscore the importance of inclusive digital development strategies that prioritize vulnerable populations within the informal sector.

8.0 Legal challenges and policy gaps

The intersection of cybercrime and informal economies reveals significant legal and policy deficiencies that exacerbate the vulnerability of informal workers. Despite the increasing reliance on digital platforms, legal and regulatory frameworks have not evolved sufficiently to address the unique risks faced by informal economic actors. This section examines key legal challenges, including limited legal recognition, barriers to reporting cybercrime, weak enforcement mechanisms, and gaps in consumer protection and financial regulation.

8.1 Limited Legal recognition of informal actors

A fundamental challenge in addressing cybercrime within informal economies is the limited legal recognition of informal workers and enterprises. Informal economic activities often operate outside formal registration and regulatory systems, which excludes participants from legal protections and institutional support mechanisms (Chen, 2012; International Labour Organization [ILO], 2018). As a result, informal actors are frequently unable to access legal recourse when affected by cybercrime.

Legal frameworks governing cybercrime and digital transactions are typically designed with formal sector entities in mind, thereby neglecting the realities of informal economic participation (UNCTAD, 2021). This exclusion creates a structural gap in which informal workers are neither adequately protected nor

effectively integrated into legal systems. Consequently, victims of cybercrime in the informal sector often face difficulties in proving ownership, establishing contractual relationships, or seeking compensation (La Porta & Shleifer, 2014).

Furthermore, the lack of formal identification and documentation among informal workers further complicates their legal standing, limiting their ability to engage with formal financial institutions and dispute resolution mechanisms (World Bank, 2022). This systemic exclusion reinforces vulnerability and perpetuates inequality within digital economic systems.

8.2 Barriers to reporting Cybercrime

Reporting cybercrime remains a significant challenge for informal workers due to a combination of structural, institutional, and behavioral factors. One major barrier is the lack of awareness regarding reporting procedures and legal rights, which is closely linked to low levels of digital and legal literacy (OECD, 2020). Many informal workers are unaware of where or how to report cyber incidents, leading to widespread underreporting.

Distrust in law enforcement agencies and perceived inefficiency of the justice system further discourage reporting (UNODC, 2013). Informal workers often believe that reporting cybercrime will not lead to meaningful outcomes, particularly in contexts where enforcement capacity is weak and case resolution rates are low (Wall, 2007). Additionally, fear of victim-blaming, stigma, or exposure of informal business activities may deter individuals from engaging with formal institutions (Leukfeldt, 2014).

Practical barriers such as cost, time, and bureaucratic complexity also play a significant role. Reporting cybercrime often requires navigating formal procedures that are inaccessible or burdensome for informal workers, especially those in rural or underserved areas (Anderson et al., 2019). These barriers collectively contribute to a substantial gap between cybercrime incidence and reporting, limiting the effectiveness of policy responses.

8.3 Lack of Enforcement mechanisms

Even where legal frameworks exist, enforcement mechanisms are often inadequate to effectively address cybercrime, particularly in developing countries. Law enforcement agencies frequently face constraints such as limited technical expertise, insufficient funding, and lack of specialized cybercrime units (UNODC, 2013). These challenges hinder the investigation and prosecution of cyber offenses, reducing the deterrent effect of existing laws.

The transnational nature of cybercrime further complicates enforcement efforts, as jurisdictional limitations and lack of international cooperation impede effective action (Kshetri, 2010). Informal workers, who typically operate at the local level, are disproportionately affected by these enforcement gaps, as their cases may not receive priority attention within overstretched legal systems.

Moreover, the absence of effective monitoring and regulatory oversight of digital platforms creates opportunities for cybercriminal activities to flourish (OECD, 2020). Weak enforcement not only emboldens perpetrators but also undermines public confidence in digital systems and legal institutions (World Bank, 2022). This situation reinforces a cycle of

vulnerability in which informal actors remain exposed to repeated cyber risks without adequate protection.

8.4 Gaps in consumer protection and financial regulation

Consumer protection and financial regulation frameworks are critical for safeguarding users in digital economies; however, significant gaps exist in their application to informal sectors. Many regulatory policies are designed for formal financial systems and fail to account for the unique characteristics of informal transactions and digital financial inclusion (UNCTAD, 2021).

Informal workers often rely on mobile money services, fintech platforms, and peer-to-peer transactions, which may not be fully covered by existing consumer protection laws (Suri & Jack, 2016). This creates vulnerabilities in areas such as fraud prevention, dispute resolution, and compensation for financial losses. In many cases, service providers are not held accountable for security breaches or fraudulent activities affecting users (OECD, 2020).

Additionally, regulatory fragmentation and lack of coordination among financial authorities, telecommunications regulators, and cybersecurity agencies contribute to gaps in oversight (Kopp et al., 2017). This fragmentation limits the effectiveness of policy interventions and creates inconsistencies in protection across different platforms and jurisdictions.

The absence of inclusive regulatory frameworks also limits the ability of informal workers to build trust in digital financial systems, thereby constraining the potential benefits of digital inclusion (World Bank, 2022). Addressing these gaps requires a comprehensive approach that integrates consumer protection, financial regulation, and cybersecurity within a unified policy framework.

8.5 Synthesis

Overall, the legal challenges and policy gaps identified in this study highlight the structural and institutional weaknesses that exacerbate the vulnerability of informal workers to cybercrime. Limited legal recognition, barriers to reporting, weak enforcement mechanisms, and gaps in consumer protection collectively create an environment in which cyber risks are amplified and recovery options are constrained. These findings underscore the need for inclusive, adaptive, and well-coordinated policy responses that address the unique characteristics of informal economies within the digital landscape.

9.0 Social work interventions

Social work interventions are critical in mitigating the economic and social impacts of cybercrime on informal workers. These interventions span preventive, protective, and recovery-oriented strategies, focusing on enhancing digital literacy, advocating for inclusive policies, and fostering community resilience (Payne, 2014). Informal workers, often excluded from formal regulatory protections, are particularly vulnerable to cyber risks, making social work engagement essential for both individual and collective empowerment (Friedman & Riemer, 2020).

9.1 Preventive strategies

Preventive strategies aim to reduce exposure to cybercrime by equipping informal workers with knowledge and tools for digital safety. Digital literacy programs,

including basic cybersecurity awareness, password management, phishing detection, and safe online transaction practices, have been shown to significantly lower vulnerability to cyber threats in low-regulation environments (Livingstone & Helsper, 2007; Chen et al., 2021).

Community-based training initiatives further strengthen preventive efforts by delivering context-specific education through local networks, cooperatives, and community centers. Such programs leverage peer-to-peer learning, enabling informal workers to share experiences, identify risks collectively, and adopt safer digital practices (Midgley, 2013). The social work profession can facilitate these initiatives by designing inclusive curricula that address literacy gaps, cultural considerations, and technological accessibility (Netting et al., 2012).

9.2 Protective Mechanisms

Protective mechanisms involve structural and systemic interventions that shield informal actors from cybercrime's immediate and long-term consequences. Advocacy for inclusive cyber policies is a core component, as social workers can collaborate with government agencies, financial institutions, and civil society organizations to ensure informal workers are represented in regulatory frameworks (Ferguson, 2018). Such advocacy helps bridge legal gaps, ensuring that policy responses reflect the unique risks and needs of the informal sector.

Support systems for victims are equally vital. Social workers provide psychological support, crisis counseling, and guidance on navigating legal procedures following cybercrime incidents. Evidence suggests that timely support mitigates stress, reduces social isolation, and promotes faster recovery for individuals and small businesses affected by digital fraud (Saleebey, 2013). These protective strategies align with social justice principles by addressing inequities in access to protection and resources (Dominelli, 2002).

9.3 Recovery and reintegration

Recovery-oriented interventions aim to restore financial stability and social participation among victims of cybercrime. Financial counseling and support programs are central, offering budgeting guidance, debt management, access to microcredit, and training in digital payment security to prevent re-victimization (Healy, 2014). For informal entrepreneurs, such interventions can directly influence business continuity and sustainability.

Community resilience building complements individual recovery by fostering collective capacities to respond to cyber risks. Social workers engage local associations, cooperatives, and community groups to develop peer monitoring, shared resources, and cooperative security measures, enhancing both social cohesion and digital economic resilience (Midgley, 2013; Payne, 2014). Integrating preventive, protective, and recovery strategies allows social work interventions to address cybercrime's multi-dimensional impacts, promoting inclusive economic development and equitable digital participation.

10.0 Policy framework proposal

Addressing cybercrime in informal economies requires a holistic policy framework that integrates legal, economic, and social interventions. Cyber risks affect

vulnerable informal actors disproportionately due to regulatory gaps, limited digital literacy, and economic precarity (Chen et al., 2021; Friedman & Riemer, 2020). A multi-layered policy framework ensures that preventive, protective, and recovery mechanisms are coordinated, reducing systemic vulnerability while promoting digital inclusion and economic resilience (Payne, 2014).

10.1 Integrated Approach

Legal layer: Inclusive Cyber laws and enforcement

An inclusive legal layer involves the development and enforcement of cyber laws that explicitly recognize and protect informal workers. This includes extending regulatory coverage to mobile-based trade, digital microtransactions, and small-scale online services that constitute the informal sector (Ferguson, 2018). Legal instruments should define cybercrime offenses, outline reporting mechanisms, and establish accessible judicial procedures for informal actors. Strengthening enforcement capacity, including local law enforcement training and dedicated cyber units, is critical to ensuring compliance and deterrence (Grabosky, 2007).

Economic layer: financial protection and risk-sharing mechanisms

Economic interventions must provide informal workers with mechanisms to absorb losses from cybercrime. These can include micro-insurance programs, digital fraud compensation schemes, and risk-sharing platforms facilitated by financial institutions and cooperatives (Chen et al., 2021). By promoting access to secure financial tools and protective measures, informal actors can maintain business continuity and trust in digital systems. Risk mitigation policies should also incentivize safe practices, such as adopting verified payment systems and cybersecurity protocols (Aker et al., 2016).

Social layer: education, advocacy, and community support

The social layer emphasizes capacity-building through education, advocacy, and community engagement. Digital literacy programs, cybersecurity awareness campaigns, and peer-led community initiatives empower informal workers to navigate online platforms safely (Livingstone & Helsper, 2007). Social work practitioners play a pivotal role in advocacy, ensuring that informal sector concerns are represented in policymaking and that community-based support systems are established to assist victims of cybercrime (Friedman & Riemer, 2020; Midgley, 2013).

10.2 Implementation strategies

Public-Private Partnerships: Effective implementation requires collaboration between government, private sector actors, and technology providers. Public-private partnerships (PPPs) can leverage technological infrastructure, training resources, and enforcement capabilities, creating an integrated network for cybercrime prevention and mitigation (Healy, 2014). PPPs enable scalable solutions such as mobile fraud monitoring systems and rapid reporting channels that are accessible to informal workers.

Collaboration with NGOs and Social Workers: Non-governmental organizations (NGOs) and social work professionals provide grassroots-level engagement, ensuring interventions reach marginalized populations. Their involvement facilitates

education, advocacy, and crisis response, complementing formal legal and economic measures (Dominelli, 2002; Saleebey, 2013). Social workers can monitor program effectiveness, gather feedback from beneficiaries, and advocate for continuous policy refinement.

Inclusion of Informal sector representatives: Policy design and implementation must actively include representatives from informal economies to ensure relevance, legitimacy, and community buy-in. Participatory policymaking enables co-creation of protective mechanisms, ensures context-specific solutions, and fosters compliance and trust among informal workers (Netting et al., 2012). Engaging stakeholders directly affected by cyber risks strengthens both the preventive and recovery dimensions of the framework.

11.0 Policy recommendations

To effectively address cybercrime in informal economies, this study proposes evidence-based policy recommendations grounded in legal, economic, and social perspectives. These recommendations aim to mitigate economic disruptions, protect vulnerable actors, and strengthen institutional and community resilience.

11.1 Expand Cybersecurity laws to cover informal sector participants

Current legal frameworks often exclude informal workers from protections against digital fraud, phishing, and mobile-based scams (Chen et al., 2021; Friedman & Riemer, 2020; Ferguson, 2018; Grabosky, 2007). Expanding cybersecurity laws to explicitly include informal sector participants ensures legal recognition, enhances deterrence, and empowers enforcement agencies to act on behalf of all economic actors. Policymakers should also develop sector-specific provisions, such as protections for micro-entrepreneurs, street vendors, and informal online traders, to reduce exposure to cyber risks.

11.2 Improve access to reporting and legal redress mechanisms

Informal actors frequently face barriers in reporting cybercrime, including procedural complexity, fear of retaliation, and lack of awareness of legal rights (Payne, 2014; Dominelli, 2002). Governments and regulatory agencies should create simplified, accessible reporting platforms, including mobile and online channels, and provide legal aid support to guide victims through redress processes. Community-level liaison officers or local social work practitioners can act as intermediaries to facilitate reporting and enhance trust in formal mechanisms.

11.3 Promote Financial Inclusion with Built-In Security Safeguards

Financial exclusion amplifies the vulnerability of informal workers to cybercrime (Chen et al., 2021; Aker et al., 2016). Integrating digital security safeguards into financial inclusion initiatives—such as fraud-resistant mobile wallets, encrypted payment systems, and automatic transaction alerts—can reduce income disruption and build confidence in digital tools. Collaboration between financial institutions, regulators, and community organizations is essential to ensure that such tools are both accessible and secure for informal actors.

11.4 Invest in Digital literacy programs

Limited digital literacy increases susceptibility to cyber threats, including identity theft, phishing, and mobile scams

(Friedman & Riemer, 2020; Livingstone & Helsper, 2007). National and local governments, in partnership with NGOs and social work agencies, should implement targeted digital literacy programs. These programs should focus on practical cybersecurity skills, safe online transactions, and awareness of cybercrime reporting channels. Peer-to-peer education and community-based workshops can enhance uptake and retention among informal sector participants.

11.5 Develop targeted interventions for vulnerable groups

Certain groups within the informal economy—including women, youth, and low-income traders—face heightened exposure to cyber risks due to socio-economic marginalization (Midgley, 2013; Saleebey, 2013). Tailored interventions, such as micro-insurance schemes, emergency financial support, mentorship programs, and psychosocial assistance, can reduce vulnerability and accelerate recovery after cybercrime incidents. Social workers and community advocates should play a central role in designing and monitoring these interventions to ensure responsiveness and equity.

Conclusion

This study demonstrates that cybercrime poses significant threats to informal economies, exacerbating income instability, market inefficiencies, and social inequality. Informal sector participants are particularly vulnerable due to limited legal recognition, low digital literacy, and weak institutional support, leaving them exposed to various forms of cybercrime, including mobile fraud, phishing, and digital payment exploitation. Findings underscore that economic disruptions are compounded by gaps in law enforcement and regulatory frameworks, necessitating integrated legal, economic, and social interventions. Social work initiatives—such as community education, advocacy, and resilience-building—emerge as critical mechanisms to protect, prevent, and recover affected actors. The study's policy recommendations, including expanded cybersecurity legislation, accessible reporting channels, financial safeguards, and targeted support programs, provide actionable solutions for mitigating cybercrime's impact. Ultimately, addressing cybercrime in informal economies requires a collaborative, multi-layered approach, combining legal reform, digital empowerment, and community-centered social interventions to foster inclusive and resilient economic systems.

Reference

Aker, J. C., Boumnijel, R., McClelland, A., & Tierney, N. (2016). Payment mechanisms and economic inclusion in informal economies: Evidence from mobile money in developing countries. *Journal of Development Economics, 121*, 1–17. https://doi.org/10.1016/j.jdeveco.2016.03.002

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the changing cost of cybercrime. *Journal of Cybersecurity, 5*(1), 1–18.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169–217.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Chen, M. A. (2012). The informal economy: Definitions, theories and policies. *WIEGO Working Paper*.

Chen, X., Zhang, C., & Xu, H. (2021). Digital literacy and cybercrime prevention: Evidence from small-scale entrepreneurs in developing countries. *Journal of Information Technology & People, 34*(2), 567–585. https://doi.org/10.1108/JITP-12-2020-0331

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

Dominelli, L. (2002). *Anti-oppressive social work theory and practice*. Palgrave Macmillan.

Donou-Adonsou, F., Lim, S., & Mathey, S. (2016). Technological progress and economic growth in developing countries. *Economic Modelling, 52*, 726–737.

Ferguson, I. (2018). *Global perspectives on social work and digital inclusion*. Routledge.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). SAGE Publications.

Friedman, E., & Riemer, J. (2020). Social work and digital risk: Protecting vulnerable populations in informal economies. *International Social Work, 63*(3), 329–342. https://doi.org/10.1177/0020872819886956

Grabosky, P. (2007). *Countering cybercrime: Evidence-based policy and strategies*. Springer.

Healy, L. M. (2014). *International social work: Professional action in an interdependent world* (2nd ed.). Oxford University Press.

International Labour Organization (ILO). (2018). *Women and men in the informal economy: A statistical picture*. ILO.

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *IMF Working Paper*.

Kshetri, N. (2010). *The global cybercrime industry: Economic, institutional and strategic perspectives*. Springer.

La Porta, R., & Shleifer, A. (2014). Informality and development. *Journal of Economic Perspectives, 28*(3), 109–126.

Leukfeldt, R. (2014). Cybercrime and social ties. *Trends in Organized Crime, 17*(4), 231–249.

Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people, and the digital divide. *New Media & Society, 9*(4), 671–696. https://doi.org/10.1177/1461444807080335

Midgley, J. (2013). *Social development: Theory and practice*. SAGE Publications.

Netting, F. E., Kettner, P. M., McMurtry, S. L., & Thomas, M. L. (2012). *Social work macro practice* (5th ed.). Pearson.

OECD. (2020). *Digital security risk management in a global digital economy*. OECD Publishing.

Payne, M. (2014). *Modern social work theory* (4th ed.). Oxford University Press.

Rawls, J. (1971). *A theory of justice*. Harvard University Press.

Saleebey, D. (2013). *The strengths perspective in social work practice* (6th ed.). Pearson.

Schneider, F., Buehn, A., & Montenegro, C. (2010). Shadow economies all over the world. *World Bank Policy Research Working Paper*.

Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science, 354*(6317), 1288–1292.

UNCTAD. (2021). *Digital economy report 2021*. United Nations.

UNODC. (2013). *Comprehensive study on cybercrime*. United Nations Office on Drugs and Crime.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Wooldridge, J. M. (2013). *Introductory econometrics: A modern approach* (5th ed.). Cengage Learning.

World Bank. (2022). *World development report 2022: Finance for an equitable recovery*. World Bank Publications.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.