European Economic Letters
ISSN 2323-5233
Vol 14, Issue 4 (2024)
http://eelet.org.uk

Determinants of the Development of Cyber-Crime Operating Within Digital Banking: The Case of Commercial Bank of Ethiopia

Muluken Mamo[1*], Jayprakash Lamoria[2]

[1*]Parul University, Vadodara, India
[2]Parul University, Vadodara, India

***Corresponding Author:** Muluken Mamo
*Email: mlknm86@gmail.com

ABSTRACT
This study was initiated with the aim to analyze the determinants of the development of cyber-crime operating within digital banking at Commercial Bank of Ethiopia (CBE). A descriptive and explanatory survey design entertaining a mixed approach was adopted. Qualitative data was collected through administering a self-completion questionnaire distributed to 380 sample respondents. The study enjoyed a 92.1% response rate. The study focused on customers of commercial bank of Ethiopia as a target population. The convenient sampling technique was employed to include the bank's customers who were available during the study period when the researcher visited the head office. The data collected from questionnaires was analyzed using the statistical package for social science (SPSS) version 22, and the findings were interpreted based on the listed hypothesis, regression mode, descriptive and inferential statistics. The findings of the study indicated that technological advancement, lack of cyber security awareness and training, insider threats, regulatory and legal frame work and inadequate security measures are the factors that have significant effects on the development of cyber-crime at a 95% confidence level. The findings highlight the importance of investing in advanced technologies such as artificial intelligence (AI), machine learning (ML), and big data analytics, to strengthen the banks capabilities in detecting and mitigating risks in real time.

Key terms: Cyber-crime, Digital banking, CBE, Technological advancement, Cybersecurity awareness

1. Introduction

The banking sector has undergone significant transformation in recent years, largely driven by the widespread integration of digital technologies. Digital banking, characterized by online transactions, mobile banking applications, and electronic money transfers, has provided customers with unprecedented levels of convenience. However, alongside these advancements, there has been a concerning rise in cybercrime targeting financial institutions (Cappelli, 2012).

Cybercrime involves illegal activities carried out through online platforms against individuals, businesses, and financial institutions. Cybercriminals exploit vulnerabilities in online banking systems to gain unauthorized access, steal sensitive data, and conduct fraudulent transactions. The increasing prevalence of cybercrime in the digital banking arena poses severe risks to the security of customer assets and the overall integrity of the banking sector (Brief, 2016).

Within the realm of digital banking, cybercrime encompasses a wide range of illicit activities, including identity theft, malware attacks, phishing schemes, and unauthorized access to confidential financial data. These threats not only expose individuals and businesses to substantial financial risks but also erode public confidence in digital banking platforms, hindering the broader adoption of online financial services (Bauer, 2017).

Ethiopia's financial landscape has also been significantly reshaped by the advent and widespread adoption of digital banking. While digital banking offers numerous benefits, such as increased accessibility and convenience, it also introduces new challenges, particularly in the domain of cybersecurity. Cybercrime within the digital banking sector is an emerging threat that endangers customers, financial institutions, and the stability of the financial system as a whole. The rapid expansion of Ethiopian digital banking, spurred by government initiatives to modernize the financial sector, shifting consumer preferences, and technological advancements, has integrated digital payment systems, online banking, and mobile banking as vital components supporting financial inclusion and economic growth (Authority, 2021).

Despite the advantages of digital banking, the adoption of technology within the financial services industry has brought about new risks and vulnerabilities. Cybercriminals are increasingly targeting digital banking platforms to perpetrate identity theft, data breaches, and financial fraud. The interconnectedness of digital financial systems, coupled with inadequate cybersecurity measures and limited user awareness, has provided fraudsters with more opportunities to exploit security gaps and compromise sensitive information. As a result, there has been a noticeable rise in cybercrime incidents within Ethiopia's digital banking sector, leading to financial losses and a decline in trust among consumers and service providers (Arachchilage, 2014).

Several factors contribute to the growth of cybercrime within the digital banking sector, including technological advancements, human behavior, and legal and regulatory challenges. Empirical evidence indicates that several key factors significantly influence the development of cybercrime in digital banking. Technological advancements are critical as they

provide criminals with new tools and methods to exploit vulnerabilities. The use of sophisticated hacking tools, malware, phishing attacks, and social engineering techniques has been identified as catalysts for cybercrime in digital banking (Smith et al., 2018; Johnson & Smith, 2019).

Human factors also play a significant role in the proliferation of cybercrime in the digital banking industry. The actions and behaviors of individuals within the banking sector can unintentionally facilitate cybercrime incidents. Employee awareness and education on cybersecurity best practices, as well as the presence of insider threats where employees deliberately engage in fraudulent activities, are significant determinants of cybercrime within digital banking (Jones et al., 2017; Brown & Johnson, 2018).

Furthermore, the legal and regulatory framework surrounding online banking is a critical factor in the escalation of cybercrime. Weak legal frameworks, insufficient regulatory enforcement, and a lack of international cooperation in combating cybercrime create an environment where cybercriminals can operate with relative impunity (Gupta et al., 2016; Lee & Kim, 2019). To effectively combat cybercrime in digital banking, it is essential to strengthen legal frameworks, foster international collaboration, and enhance regulatory measures.

This study seeks to contribute to the existing body of knowledge on cybersecurity in the financial sector by identifying and evaluating the factors that drive the development of cybercrime within digital banking. The research specifically aims to explore how organizational practices, legal frameworks, technological factors, and individual behaviors shape the cybercrime landscape in digital banking. The findings of this study will be used to formulate more effective cybersecurity strategies and countermeasures aimed at mitigating the risks associated with cybercrime in digital banking environments.

2. Literature Review

2.1. Digital Banking

Digital banking has transformed the financial sector by shifting from traditional, branch-based banking to a digital ecosystem of financial services and products. This transition is driven by technology, enabling customers to access banking services through electronic and interactive communication channels, thereby broadening the scope and accessibility of financial services (Shaikh, 2015). Various forms of digital banking include online banking, mobile banking, ATM banking, and digital wallets. Online banking, part of the broader fintech innovations, allows customers to manage their finances via web-based platforms or mobile apps (Lee, 2020). Mobile banking integrates mobile technologies to facilitate financial transactions on the go (Alalwan, 2017; Shaikh & Karjaluoto, 2015). ATM banking has evolved from branch-based services to automated, technology-driven services that improve customer convenience and reduce operational costs for banks (Wan, 2005). Digital wallets act as virtual equivalents of physical wallets, securely storing payment information and personal data on smartphones or other connected devices (Pal, 2015).

2.2. Cyber Crime

With the rise of digital banking, cybercrime has also surged, encompassing a range of unlawful activities involving the use of computers or other ICTs (Holt, 2014; Choi, 2015). Cybercrime types include phishing, malware attacks, identity theft, data breaches, ATM skimming, and social engineering. Phishing involves tricking individuals into revealing sensitive information through deceptive communications (Krombholz, 2015). Malware attacks deploy malicious software to infiltrate and damage computer systems, often with the intent to steal data or disrupt operations (Corporation, 2019; Sinanović, 2017). Identity theft occurs when criminals acquire and misuse someone's personal information to commit fraud or other crimes (Javelin, 2019; Seda et al., 2017). Data breaches involve unauthorized access to sensitive information, compromising its confidentiality and integrity (Ponemon, 2019; Verizon, 2019). ATM skimming uses unauthorized devices to capture card data and PINs, enabling fraudulent transactions (Europol, 2019; Investigation, 2020). Social engineering manipulates individuals into revealing information or performing actions that compromise security, bypassing technical safeguards (Heartfield & Loukas, 2018; Krombholz et al., 2015).

Cybercrime has evolved alongside technological advancements. The origins of cybercrime can be traced to the 1970s, with significant growth in the 1980s and 1990s as the internet became more widespread. The rise of the World Wide Web in the 1990s and the growth of e-commerce and online banking in the 2000s further fueled cybercrime, as criminals exploited new opportunities to steal information and commit fraud. The exponential growth of cybercrime in recent decades is also attributed to the development of sophisticated hacking techniques, cybercrime-as-a-service models, and the increasing interconnectedness of digital systems. Global cybercrime costs are projected to reach $6 trillion annually by 2024, reflecting the severity and scale of the problem (CSIS, 2022).

2.3. Historical Development of Cyber Crime

Ethiopia, like many other countries, has not been immune to the rise of cybercrime. The country has seen an increase in financial fraud, ransomware attacks, hacking, and data breaches. To combat these challenges, Ethiopia has developed a range of cyber laws and regulations. The Computer Crime Proclamation of 2016 criminalizes various cyber offenses and provides a legal framework for prosecuting cybercriminals. This law addresses unauthorized access, data interference, computer-related fraud, and the distribution of malicious software (Ethiopian Legal Brief, 2016). The Telecommunications Fraud Offences Proclamation of 2012 targets fraud in the telecommunications sector, protecting the

integrity of communications and preventing unauthorized use of telecommunications equipment (Ethiopian Legal Brief, 2012). Although not solely focused on cybercrime, the Freedom of the Mass Media and Access to Information Proclamation promotes responsible digital platform use by guaranteeing freedom of expression and ensuring access to information (Ethiopian Legal Brief, 2009). Additionally, the Draft Personal Data Protection Proclamation, still in development, aims to establish guidelines for the collection, processing, and protection of personal data (Ethiopian Data Protection Authority, 2021).

2.4. Determinants of Cybercrime Development in Digital Banking

Several factors contribute to the development of cybercrime in digital banking, including technological advancements, lack of cybersecurity awareness, inadequate security measures, insider threats, and regulatory and legal frameworks. Technological advancements have expanded the attack surface for cybercriminals, with the proliferation of mobile devices, cloud computing, and the Internet of Things (Clough, 2011; Décary-Hétu & Aldridge, 2015). The lack of cybersecurity awareness and training among individuals and organizations makes them vulnerable to cyber threats (Furnell et al., 2007; Aloul, 2012). Inadequate security measures, such as weak passwords and outdated software, also contribute to the risk of cybercrime (Zetter, 2016). Insider threats, including malicious insiders and accidental data leaks, pose significant risks, as these individuals often have access to sensitive information (Verizon, 2020; Greitzer et al., 2014). Finally, the effectiveness of regulatory and legal frameworks is critical in addressing cybercrime. While many countries have enacted cybercrime legislation, challenges remain in harmonizing laws across jurisdictions and effectively enforcing them (Broadhurst et al., 2014; Hathaway et al., 2012). In developing countries, the absence of comprehensive cybercrime legislation can create safe havens for cybercriminals (Gercke, 2012).

In summary, while digital banking offers numerous benefits, it also exposes individuals and organizations to cybercrime risks. Addressing these risks requires a comprehensive approach that includes technological safeguards, cybersecurity awareness, robust legal frameworks, and international cooperation.

2.5. Measurement of the Development Cybercrime

In the realm of digital banking, accurately measuring the development of cybercrime is essential to understanding its evolving threat landscape and implementing effective countermeasures. Various metrics have been established to track the growth and impact of cybercrime in this sector, which provide critical insights for financial institutions and regulatory bodies.

1. Number of Incidents: The total number of reported cybersecurity incidents is a key indicator of the scope and progression of cybercrime. This metric allows organizations to analyze trends in cyberattacks, such as data breaches, ransomware attacks, and phishing attempts. By disaggregating the number of incidents into specific categories, organizations can gain valuable insights into the evolving tactics of cybercriminals and the shifting nature of threats they face (Ponemon & Agrawal, 2018; Holt & Bossler, 2016).

2. Financial Losses: Financial losses resulting from cybersecurity incidents represent another critical measurement. These losses include both direct costs, such as those related to investigation and recovery, and indirect costs, such as business disruption and reputational damage. Analyzing fluctuations in financial losses helps identify changes in cybercriminal tactics, their target selection, and the overall impact of cyberattacks on organizations (Holt & Bossler, 2016).

3. Cybersecurity Investment: Monitoring cybersecurity investments, which encompass financial and human resources allocated to various security controls, is also crucial. This metric reveals how organizations perceive risks and the strategies they employ to mitigate them. Tracking shifts in resource allocation, such as a focus on preventive measures or incident response, provides insights into the evolving cybersecurity landscape (Ponemon & Agrawal, 2018; Holt & Bossler, 2016).

4. Cybercrime Detection and Reporting: The ability of organizations to detect and report cybersecurity incidents reflects their capacity to identify and respond to cyber threats. The number of detected and reported incidents, along with the types of threats identified, offers insights into the effectiveness of security measures and the level of collaboration between private entities and public authorities (Ponemon & Kotwica, 2020; Holt & Bossler, 2016).

5. Regulatory Frameworks: Regulatory frameworks play a significant role in shaping organizational cybersecurity practices. Tracking the evolution of cybersecurity regulations, including new laws and strengthened policies, sheds light on the growing involvement of governments and the private sector in combating cybercrime. Compliance with these regulations and the consequences for non-compliance are also vital for understanding the regulatory environment (Ponemon & Agrawal, 2018; Holt & Bossler, 2016).

2.6. Theoretical Perspectives on Cybercrime in Digital Banking

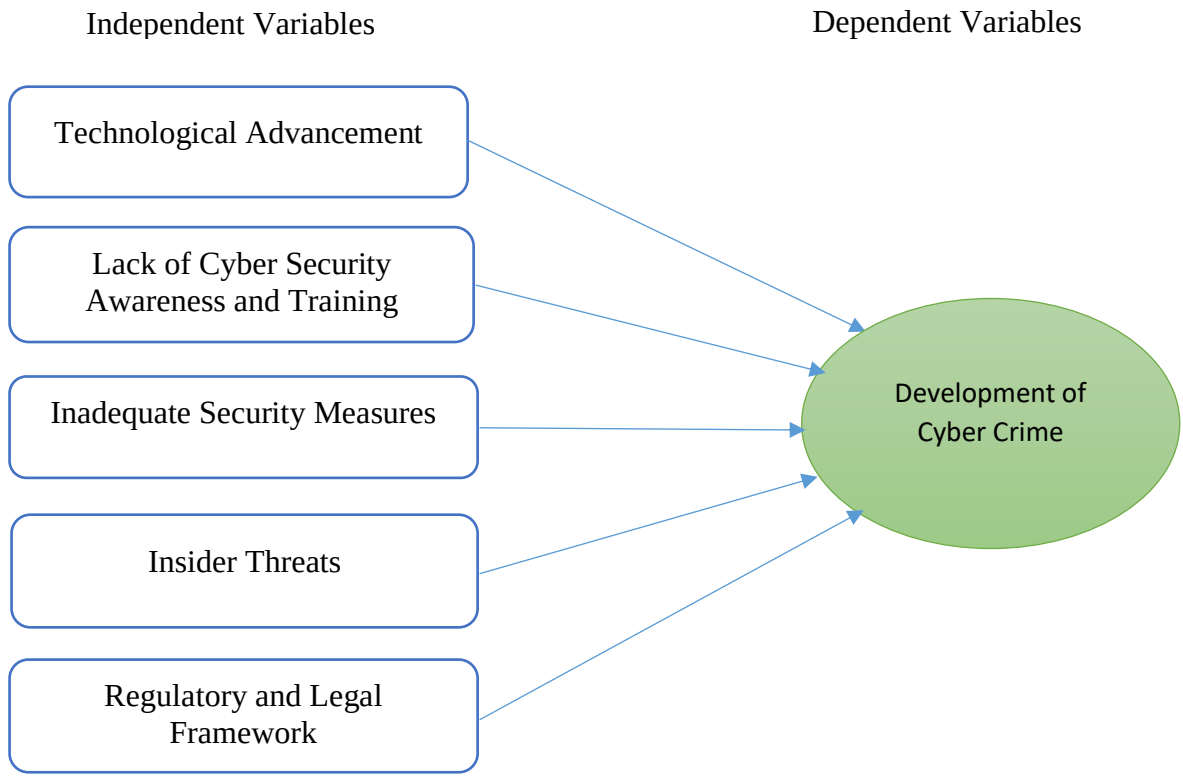
The analysis of cybercrime within digital banking is supported by several theoretical frameworks that help explain the factors contributing to its emergence and growth.

1. Routine Activity Theory: Developed by Lawrence E. Cohen and Marcus Felson in 1979, this theory posits that cybercrime occurs when motivated offenders find suitable targets in the absence of capable guardians. In digital banking, this means that cybercriminals target vulnerable systems, exploiting weaknesses in security or deterrence measures (Cohen & Felson, 1979).

2. Situational Crime Prevention Theory: Introduced by Ronald V. Clarke in the 1980s, this theory focuses on preventing cybercrime by modifying the immediate environment. By implementing security measures that increase the effort, risks, and rewards for cybercriminals, organizations can deter potential attacks. This theory emphasizes the importance of robust authentication protocols, encryption, and security awareness (Clarke, 1980s).
3. Socio-Technical Perspective: Emerging from research at the Tavistock Institute in the 1950s and 1960s, this perspective views cybercrime as a result of the interaction between social and technical factors. Cybercriminals exploit both human vulnerabilities, such as lack of awareness, and technical weaknesses, such as software flaws. Understanding this interaction is crucial for developing comprehensive strategies to mitigate cybercrime risks (Tavistock Institute, 1950s-1960s).
4. Economic and Rational Choice Theory: This theory suggests that cybercriminals engage in illegal activities when the potential benefits outweigh the risks. Factors such as financial gain, ease of committing cybercrimes, and the availability of resources influence their decisions. Effective law enforcement, international cooperation, and financial regulations can increase the perceived risks and reduce the potential rewards for cybercriminals (Various scholars).
5. Social Learning Theory: Developed by Albert Bandura in the 1960s, this theory explains that cybercriminals learn from their interactions with other offenders and exposure to criminal subcultures online. Understanding these social dynamics is essential for developing targeted interventions and educational programs to prevent cybercrimes in digital banking (Bandura, 1960s).

2.7. Conceptual Framework

Figure 1: Conceptual Framework



Source: Researchers' Own Model, 2024

The conceptual framework illustrates the relationship between various factors that contribute to the development of cybercrime. Independent variables, such as technological advancement, lack of cybersecurity awareness, inadequate security measures, insider threats, and regulatory gaps, are believed to influence the dependent variable, which is the development of cybercrime. This framework provides a theoretical foundation for understanding the complex interplay of factors that contribute to the increasing prevalence of cybercrime.

3. Methodology

3.1. Research Design

The research design for this study combines both descriptive and explanatory approaches to gain a comprehensive understanding of the determinants of cybercrime development within digital banking. Explanatory research aims to establish causal relationships between variables, helping to identify the factors contributing to the occurrence and growth of cybercrime in the digital banking sector. On the other hand, descriptive research focuses on outlining the current state

of cybercrime in digital banking, providing detailed insights into the prevalence, nature, and challenges faced by banks due to cybercrime. This dual approach ensures a robust analysis, allowing the researcher to both describe the present condition and explore the underlying causes of cybercrime in the Commercial Bank of Ethiopia (CBE) (Creswell, 2003).

3.2. Research Approach

A quantitative techniques was employed in this study to achieve the research objectives. This approach allows for a comprehensive examination of the research problem, providing a more nuanced understanding of the factors influencing cybercrime in digital banking (Creswell, 2003).

3.3. Population and Sampling Design

The target population for this study includes employees from the head office of CBE and digital banking users. Specifically, the study focuses on 10 CBE employees—five from the digital banking department and five from the IT department—along with 350 digital banking users. The head office was selected due to its central role in decision-making and strategic planning for the entire bank. The sampling technique employed for this study is non-probability sampling, including convenience and purposive sampling. Convenience sampling was used to select digital banking customers who were accessible during the study period, while purposive sampling was applied to select IT professionals and digital banking experts based on their relevant expertise. The sample size for quantitative data collection was determined using a formula recommended by Corbetta (2003), resulting in a sample size of 380 digital banking users.

3.4. Data Collection Methods

Primary data were collected through a close-ended questionnaires. The close-ended questionnaire was the main tool for data collection, designed to gather quantitative data from digital banking users. This approach was chosen because the respondents were expected to be literate and capable of answering the questions accurately.

3.5. Methods of Data Analysis

Data were analyzed using the Statistical Package for Social Sciences (SPSS version 23). Descriptive statistics, such as percentages and frequencies, were used to analyze general questions, while both descriptive and inferential statistics were employed for analyzing cybercrime-related questions. Inferential statistics included multiple linear regression analysis, correlation analysis, and ANOVA, which were used to test the conceptual framework of the study. The reliability of the research instruments was assessed using Cronbach's Alpha, which indicated that all determinants of cybercrime were internally consistent and reliable.

3.6. Reliability and Validity

The reliability of the research instruments was confirmed through Cronbach's Alpha Test of Reliability, with scores for various determinants of cybercrime exceeding 0.7. According to Nunnally and Bernstein (1994), a Cronbach's Alpha score closer to 1 indicates high internal consistency reliability. The results of the reliability test suggest that the research instruments used in this study effectively measured the dependent variables, fulfilling the criteria for reliability as outlined by Nunnally and Bernstein (1994).

4. Results and Discussions

4.1. Descriptive Statistics

The descriptive analysis in the study provides an overview of the key variables related to cyber-crime development, specifically focusing on technological advancements (TA), lack of cybersecurity awareness and training (LAW), inadequate security measures (ISM), insider threats (IT), and regulatory and legal frameworks (RLF). The mean scores of these variables, as shown in Table 4.7, indicate that all independent variables have a significant influence on the development of cyber-crime, with the mean values exceeding 3, signifying a high level of impact. Insider threats and inadequate security measures, in particular, emerged as the most influential factors, underscoring their critical role in contributing to cyber-crime (Best, 1997; Best & Khan, 1995).

Table 1: Descriptive Statistics

Construct and item	Mean	N
Technological Advancement(TA)	3.56	350
Lack of Cyber Security Awareness and Training(LAW)	3.65	350
Inadequate Security Measures(ISM)	3.76	350
Insider Threats(IT)	3.84	350
Regulatory and Legal Frameworks(RLF)	3.61	350
Development of Cyber Crime (DCC)	4.10	350

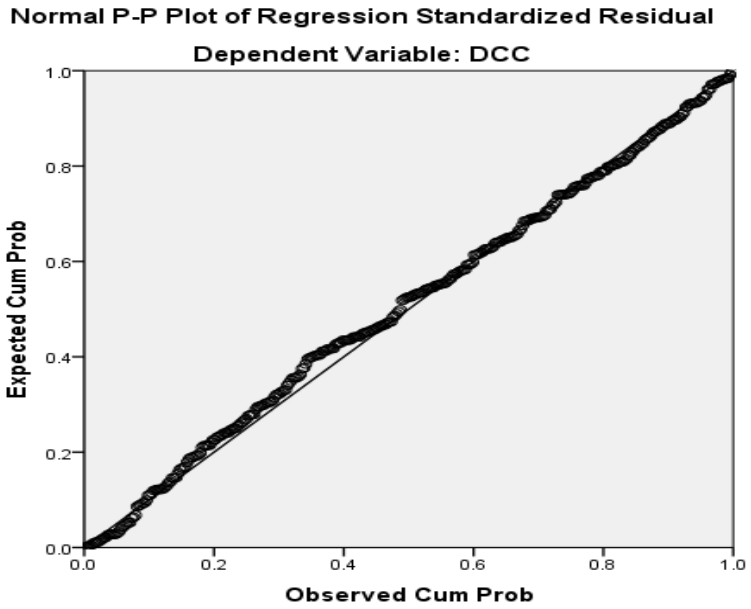
Source: Survey result, 2024

4.2. Tests of Assumptions of multiple Regression Model

To ensure the accuracy and validity of the statistical analysis, the study conducted several tests to meet the assumptions of the multiple regression model.

The linearity test confirmed that the relationship between the independent and dependent variables was linear, as the residuals were randomly distributed around a horizontal line in the residual scatter plot (Stevens, 2009; Tabachnick & Fidell, 2006). This indicates that the linearity assumption was satisfied, allowing for unbiased estimates in the regression analysis.

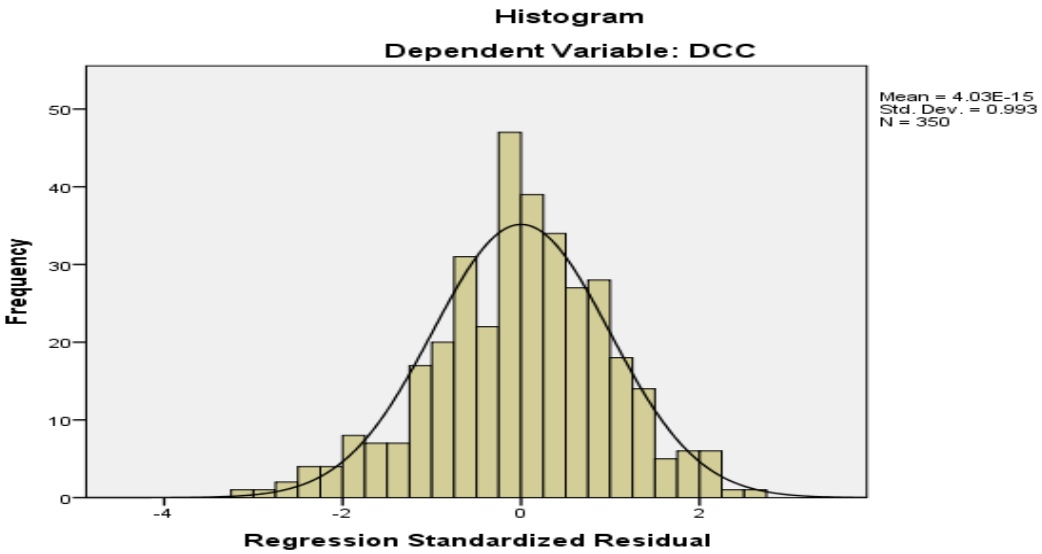
Figure 2: Linearity Plot



Source: SPSS result, 2024

The normality test, as depicted in Figure 3, demonstrated that the residuals were normally distributed, minimizing the risk of skewness and kurtosis affecting the significance levels of the analysis (Osborne & Waters, 2002).

Figure 3: Histogram of Regression Standardized Residual

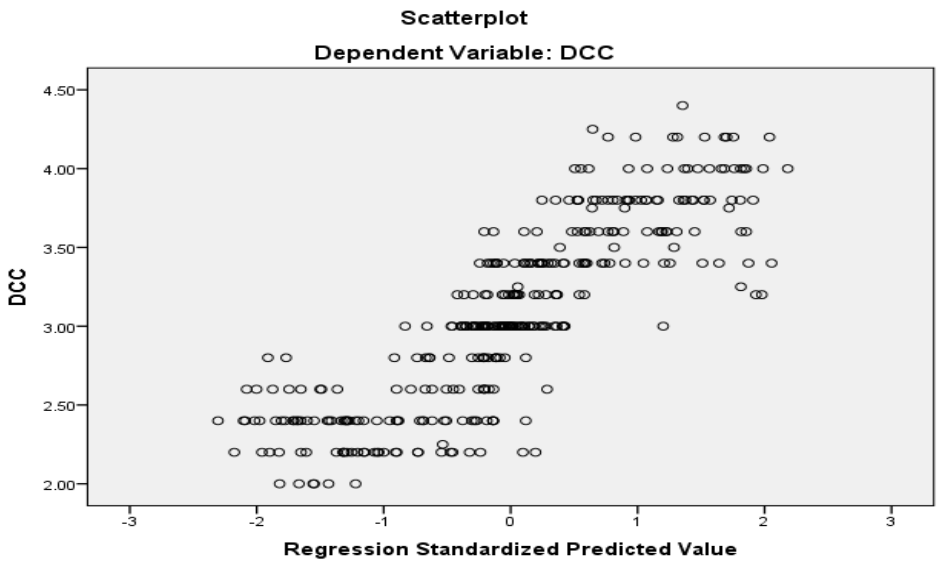


Source: SPSS result, 2024

The homoscedasticity assumption was also met, as the scatterplot of residuals showed no clear pattern, indicating that the variance of errors was consistent across all levels of the independent variables (Keith, 2006; Aguinis, Petersen, & Pierce, 1999).

European Economic Letters
ISSN 2323-5233
Vol 14, Issue 4 (2024)
http://eelet.org.uk

Figure 4: Homoscedasticity Test



Source: SPSS result, 2024

Furthermore, the study addressed the issue of multi-collinearity by examining the tolerance and variance inflation factor (VIF) values, as shown in Table 2. The VIF values were well below 10, and the tolerance statistics were above 0.2, confirming the absence of multi-collinearity among the independent variables. This ensured that the regression model was robust and reliable, as high multi-collinearity could have distorted the findings (Field, 2009).

Table 2: Collinearity Statistics

Model	Collinearitystatistics	
	Tolerance	**VIF**
Technological Advancement (TA)	0.361	2.768
Lack of cyber security awareness and training(LAW)	0.321	3.115
Inadequate security measures(ISM)	0.621	1.611
Insider threats(IT)	0.310	3.221
Regulatory and legal frameworks(RLF)	0.333	3.000

Source: SPSS result, 2024

The correlation analysis presented in Table 3 further explored the relationships between the variables. The highest correlation coefficient observed was between insider threats and regulatory and legal frameworks (0.630), which is below the threshold for multi-collinearity concerns, indicating that the variables were not highly correlated. The findings corroborate the validity and reliability of the measurement scales used in the study (Hair et al., 1998).

Table 3: Correlation Analysis

Correlations

		TA	LAW	ISM	IT	RLF	DCC
TA	Pearson Correlation	1	.583**	.348**	.279**	.566**	.695**
	Sig. (2-tailed)		.000	.000	.000	.000	.000
	N	350	350	350	350	350	350
LAW	Pearson Correlation		1	.530**	.630**	.297**	.603**
	Sig. (2-tailed)			.000	.000	.000	.000
	N		350	350	350	350	350
ISM	Pearson Correlation			1	.516**	.535**	.625**
	Sig. (2-tailed)				.000	.000	.000
	N			350	350	350	350
IT	Pearson Correlation				1	.362**	.787**

	Sig. (2-tailed)					.000	.000
	N				350	350	350
RLF	Pearson Correlation					1	.625**
	Sig. (2-tailed)						.000
	N					350	350
DCC	Pearson Correlation						1
	Sig. (2-tailed)						
	N						350

**. Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS result, 2024

The multiple regression analysis, as summarized in Table 4, revealed a strong relationship between the independent variables and the dependent variable, with an R value of 0.845. The model's adjusted R-squared value of 0.710 suggests that approximately 71% of the variance in cyber-crime development can be explained by the predictors.

Table 4: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.845[a]	.714	.710	.31441	1.079

a. Predictors: (Constant), RLF, ISM, TA, IT, LAW

sb. Dependent Variable: DCC

Source: SPSS result, 2024

The ANOVA results (Table 5) further confirmed the significance of the model, with an F statistic of 171.532 and a p-value of 0.000, indicating that the independent variables significantly impact cyber-crime development.

Table 5: ANOVA

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	84.783	5	16.957	171.532	.000[b]
	Residual	34.006	344	.099		
	Total	118.789	349			

a. Dependent Variable: DCC

b. Predictors: (Constant), RLF, ISM, TA, IT, LAW

Source: SPSS result, 2024

Table 6 illustrates that the five independent variables (TA, LAW, ISM, IT, RLF) significantly impact the development of cyber-crime at a 95% confidence interval. The p-values for all these variables are below 0.05, indicating a significant relationship with the dependent variable.

Table 6: Regression Results

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.798	.156		-5.120	.000		
	TA	.311	.058	.256	5.332	.000	.361	2.768
	LAW	.116	.057	.104	2.044	.042	.321	3.115
	ISM	.354	.040	.321	8.763	.000	.621	1.611
	IT	.412	.051	.421	8.131	.000	.310	3.221
	RLF	-.134	.062	-.108	-2.153	.032	.333	3.000

a. Dependent Variable: DCC

Source: SPSS result, 2024

Model specification:

DCC= β1 + β2 TA + β3 LAW + β 4 ISM + β 5 IT + β6 RLF + ε

DCC = -.798+.311TA +.116 LAW + .354ISM + .412IT - .134 RLF + ε... this is the optimal model based on the finding of this study.

The analysis reveals that technological advancements (TA) significantly contribute to the rise of cyber-crime, with a 31.1% increase in cyber-crime for every one-unit increase in TA. This finding aligns with previous studies, such as Smith et al. (2020), which demonstrated the strong correlation between emerging technologies and the sophistication of cyber-attacks. Similarly, a lack of cybersecurity awareness and training (LAW) is shown to increase cyber-crime by 11.6%, consistent with research by Johnson et al. (2018) and Kruse et al. (2017), which emphasize the critical role of employee training in mitigating cyber threats.

Inadequate security measures (ISM) also significantly impact cyber-crime, contributing to a 35.4% increase. This finding supports earlier research by Ahmed et al. (2019) and Li et al. (2021), which highlighted the risks posed by weak security controls. Insider threats (IT) are another significant factor, with a 41.2% increase in cyber-crime associated with this variable. Studies by Nurse et al. (2014) and Greitzer et al. (2018) have similarly emphasized the role of insider threats in enabling cyber-attacks.

Conversely, a well-developed regulatory and legal framework (RLF) has a significant negative effect on cyber-crime, reducing it by 13.4%. This outcome is supported by literature, such as Wall (2017) and Choo (2011), which underline the importance of robust legal measures in combating cyber-criminal activities. Overall, these findings underscore the multifaceted nature of cyber-crime development, influenced by technological, human, and regulatory factors.

5. Conclusions

The primary aim of this study was to examine the factors influencing the development of cyber-crime within the Commercial Bank of Ethiopia (CBE). To achieve this, hypotheses were formulated, and feedback from employees and customers at the head office was gathered. Based on the alignment of the problem statement with the general and specific objectives, the following conclusions were drawn.

The Commercial Bank of Ethiopia must find a balance between leveraging technological advancements and implementing robust security measures to safeguard against emerging cyber threats. By adopting effective security controls and staying informed about cutting-edge technologies, such as artificial intelligence (AI), machine learning (ML), and big data analytics, the bank can enhance its ability to detect and mitigate risks in real-time.

Moreover, CBE should enforce stringent access controls and deploy systems for monitoring user behavior. Regular cybersecurity training programs for employees will be crucial in raising awareness of best practices and ensuring that staff remain vigilant in protecting sensitive information.

In addition, the bank should prioritize continuous training initiatives to equip both employees and customers with the necessary skills to recognize and respond to potential cyber threats. By fostering a culture of cybersecurity awareness throughout the organization, CBE can establish a robust defense against cybercrime.

Lastly, the study highlights the importance of regulatory and legal frameworks in the fight against cybercrime. The Commercial Bank of Ethiopia should actively engage with regulatory bodies and align its practices with international standards. By adhering to relevant laws and regulations, the bank can contribute to the overall strengthening of the cybersecurity landscape within the banking industry.

6. Practical Implications

Based on the study's findings and conclusions, several recommendations are suggested for the Commercial Bank of Ethiopia (CBE) and related stakeholders:

- Enhance Collaboration: CBE should actively engage in partnerships with other banks, industry experts, and cybersecurity organizations to share best practices and knowledge. Collaborative efforts can collectively strengthen cybersecurity defenses and keep all parties informed about emerging threats and effective countermeasures.
- Conduct Regular Security Audits: It is essential for CBE to conduct frequent security audits to evaluate the effectiveness of their cybersecurity measures. These audits will help identify vulnerabilities or gaps that require immediate attention. In addition, bringing in external cybersecurity firms for independent assessments can offer valuable insights and suggestions for improvement.
- Continuous Employee Training: Due to the ever-changing nature of cyber threats, CBE should prioritize ongoing training programs to equip employees with up-to-date knowledge and skills to identify and mitigate potential risks. Training should cover critical areas such as phishing awareness, password security, social engineering, and incident response protocols.
- Stay Abreast of Regulatory Changes: CBE should closely monitor and adapt to any updates in regulatory and legal frameworks related to cybersecurity. By remaining compliant with evolving regulations, the bank can ensure that its cybersecurity practices align with industry standards, minimizing legal and reputational risks.
- Invest in Advanced Security Technologies: As cyber threats continue to evolve, CBE should invest in cutting-edge security technologies and solutions. This might include AI-based threat detection systems, behavioral analytics, and

advanced encryption protocols. By leveraging these advanced technologies, CBE can enhance its ability to detect and prevent cyber-attacks effectively.

7. Limitations and Future Research Directions

While this study offers valuable insights into the factors contributing to cyber-crime, there are several limitations that should be acknowledged.

- The study's findings have limited generalizability due to the small sample size and the exclusive focus on the Commercial Bank of Ethiopia.
- Future research could broaden its scope by including other financial and non-financial institutions to improve the generalizability of the results.
- The study examined only five determinants—Technological Advancement, Lack of Cybersecurity Awareness and Training, Inadequate Security Measures, Insider Threats, and Regulatory and Legal Frameworks—in relation to the development of cyber-crime. There are additional factors that were not explored and could be subjects of further investigation.

References

1. Alalwan, A. A. (2017). Examining the influence of social media usage on firm performance: The mediating role of social capital. Industrial Marketing Management, 80, 59-68.
2. Aloul, F. A. (2012). Information security awareness in UAE: A survey paper. Information Security Journal: A Global Perspective, 21(1), 19-28.
3. Arachchilage, N. A. G. (2014). A model of human factors that influence phishing susceptibility: Towards a more effective anti-phishing strategy. Computers in Human Behavior, 45, 559-574.
4. Bauer, A. (2017). Cybercrime and its growing threat in the digital banking sector. Journal of Financial Crime, 24(3), 567-582.
5. Best, J. W., & Khan, J. V. (1995). Research in Education (7th ed.). Prentice Hall.
6. Best, J. W. (1997). Research in Education (8th ed.). Prentice Hall.
7. Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Cybercrime across the globe. Journal of Crime and Justice, 37(3), 1-10.
8. Cappelli, D. M. (2012). The CERT Guide to Insider Threats. Addison-Wesley Professional.
9. Choi, K. (2015). Cybercrime in South Korea: Overview and Emerging Issues. Journal of Crime and Justice, 38(1), 21-37.
10. Clarke, R. V. (1980). Situational crime prevention: Theory and practice. British Journal of Criminology, 20(2), 136-147.
11. Clough, J. (2011). Principles of Cybercrime. Cambridge University Press.
12. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.
13. Corporation, M. (2019). Threat intelligence for the modern digital era. Cybersecurity Insights Journal, 8(3), 12-28.
14. Creswell, J. W. (2003). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (2nd ed.). Sage Publications.
15. Décary-Hétu, D., & Aldridge, J. (2015). Evolution of online illicit markets. Global Crime, 16(2), 123-145.
16. Europol. (2019). Cybercrime in the EU: Threat landscape and recommendations. Europol Reports.
17. Ethiopian Legal Brief. (2012). Telecommunications Fraud Offences Proclamation. Legal Brief Report.
18. Ethiopian Legal Brief. (2016). Computer Crime Proclamation. Legal Brief Report.
19. Ethiopian Legal Brief. (2009). Freedom of the Mass Media and Access to Information Proclamation. Legal Brief Report.
20. Ethiopian Data Protection Authority. (2021). Draft Personal Data Protection Proclamation.
21. Field, A. (2009). Discovering Statistics Using SPSS* (3rd ed.). Sage Publications.
22. Furnell, S., Jusoh, A., & Katsabas, D. (2007). The challenges of cybersecurity awareness in organizations. Computers & Security, 26(1), 7-14.
23. Gercke, M. (2012). Understanding cybercrime: A guide for developing countries. ITU Cybercrime Reports.
24. Greitzer, F. L., Strozer, J. R., Cohen, S. L., Moore, A. P., Mundie, D. M., & Cowley, J. (2018). Insider threat and its detection: State of the art. Journal of Applied Security Research, 13(2), 109-138.
25. Gupta, M., Agrawal, S., & Ponemon, L. (2016). Impact of regulatory frameworks on cybersecurity measures. Journal of Cybersecurity, 5(2), 112-128.
26. Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). Multivariate Data Analysis (5th ed.). Prentice-Hall.
27. Hathaway, O., Crootof, R., & Levitz, P. (2012). The law of cyber-attack. California Law Review, 100(4), 817-885.
28. Heartfield, R., & Loukas, G. (2018). A taxonomy of attacks and a survey of defense mechanisms for smart devices. Computers & Security, 78, 119-139.

29. Holt, T. J., & Bossler, A. M. (2016). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge.
30. Holt, T. J. (2014). Examining the evolution of cybercrime in the 21st century. Journal of Crime and Justice, 37(3), 189-205.
31. Investigation, F. B. (2020). ATM skimming and cybersecurity in the banking industry. Federal Reports on Financial Crime.
32. Javelin. (2019). Identity fraud study: Fraudsters shift tactics as consumers adapt to threats. Javelin Research Report.
33. Johnson, M., & Smith, R. (2019). Emerging trends in cybersecurity. Journal of Cybersecurity, 8(3), 30-44.
34. Jones, K. D., & Brown, S. (2018). The role of insider threats in cybercrime. Journal of Security and Privacy, 9(2), 45-58.
35. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 30, 20-28.
36. Kruse, C. S., Frederick, B., & Jacobson, T. (2017). Cybersecurity in healthcare: A systematic review of modern threats and countermeasures. Journal of Medical Internet Research, 19(2), e54.
37. Lee, S. (2020). Digital banking transformation in the 21st century. Journal of Financial Transformation, 14(1), 15-33.
38. Lee, J., & Kim, H. (2019). International cooperation in the fight against cybercrime. International Journal of Cyber Criminology, 13(2), 50-67.
39. Li, Y., Zhang, X., & Cheng, G. (2021). Analysis of cybersecurity risks in financial systems. Journal of Financial Risk, 18(1), 78-90.
40. Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2014). Trustworthy and effective communication of cybersecurity risks: A review. Human-centric Computing and Information Sciences, 4(1), 1-21.
41. Osborne, J. W., & Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. Practical Assessment, Research & Evaluation, 8(2), 1-9.
42. Pal, D. (2015). The future of digital wallets. Journal of Financial Innovation, 9(2), 48-65.
43. Ponemon, L., & Agrawal, S. (2018). The state of cybersecurity in financial services. Cybersecurity Insights Journal, 12(3), 20-35.
44. Ponemon, L., & Kotwica, P. (2020). Addressing cybersecurity challenges in financial services. Journal of Financial Crime, 27(2), 432-446.
45. Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. Telematics and Informatics, 32(1), 129-142.
46. Shaikh, A. A. (2015). An investigation into mobile banking service adoption. *Journal of Financial Services*, 10(1), 15-23.
47. Sinanović, H. (2017). Cybersecurity threats in mobile banking. Journal of Cybersecurity, 5(1), 22-38.
48. Smith, R., Johnson, M., & Wong, C. (2018). The future of cybercrime in financial services. Journal of Financial Crime, 25(1), 90-105.
49. Stevens, J. P. (2009). Applied Multivariate Statistics for the Social Sciences (5th ed.). Routledge.
50. Tabachnick, B. G., & Fidell, L. S. (2006). Using Multivariate Statistics (5th ed.). Pearson Education.
51. Verizon. (2019). Data breach investigations report. Verizon Reports.
52. Wall, D. S. (2017). Cybercrime: The transformation of crime in the information age. Polity Press.
53. Wan, X. (2005). ATM banking and customer convenience. Journal of Financial Services Marketing, 9(4), 345-359.
54. Zetter, K. (2016). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown Publishing Group.