MSI Journal of
Arts, Law and Justice (MSIJALJ)

WORKFORCE COMPOSITION AND CYBER CRIME PREVENTION

Eugine Nfor[1*], Dr. Caleb Onjure, Ph. D[2], Dr. Eng John Mosonik, Ph. D[3]

[1*]Ph. D student Africa International University.

[2]Senior lecturer Africa International University.

[3]Senior lecturer Africa International University.

*** Correspondence:** Eugine Nfor

The authors declare that no funding was received for this work.

OPEN ACCESS

Received: 19-March-2026

Accepted: 20-April-2026

Published: 22-April-2026

This article is published by **MSI Publishers** in **MSI Journal of Arts, Law and Justice (MSIJALJ)**

ISSN 3049-0839 (Online)

The journal is managed and published by MSI Publishers

Volume: 3, Issue: 4 (April-2026)

ABSTRACT: Cybercrime incidents are a practical threat to online safety and economic stability. Criminals target key sectors in economies due to inadequate patching of systems, low user awareness of various threat vectors, and an increase in the use of innovations such as Artificial Intelligence and machine learning technologies. The general objective of this study was to determine the influence of digital leadership on cybercrime prevention in the Mobile Telephone Network in Cameroon. This objective was operationalized under four constructs: digital risk management, collaboration with the board of directors, digital literacy, digital forensics, and artificial intelligence. The study was both qualitative and quantitative, with a target population of 2519 and a sample size of 316. 278 of the respondents responded. The study established that workforce composition influence cybercrime prevention in the in Mobile Telephone Network in Cameroon. In addition, employee role in the organization, employee functional area in the organization and employee experience have significant influence in cyber-crime prevention in the Mobile Telephone Network in Cameroon. The study concluded that employee experience, education

level, and functional area are significant influence in cybercrime prevention within MTN Cameroon. The study recommended that the company strengthen onboarding programs for new employees, adopt role-based (functional) security training, implement continuous cybersecurity training, promote a strong cybersecurity culture, enforce access control and least-privilege principles, regularly update security policies and practices, and leverage workforce diversity.

Keywords: *work force composition, and cybercrime prevention.*

1.1 Background of the Study

In the early 2000s, data from the United States revealed a broad spectrum of cybercrime activities, including internet theft, identity fraud, terrorism, pornography, pedophilia, stalking, illegal contraband purchases, information warfare, virus creation, hate crimes, bank fraud, and espionage. To address these challenges, the Federal Bureau of Investigation (FBI) and the Department of Justice established the Internet Fraud Center (Dannis Hall, 2000). Similarly, the Council of Europe countries implemented standardized cybercrime laws to combat the rising threat. By the mid-2000s, concerns over the security of election servers became a prominent public issue (Kabay, 2008). Kelly (2013) further observes that during this period, cybercrime evolved from isolated, individual acts into highly advanced, well-coordinated operations resembling an organized crime industry.

From an African perspective, a study by KnowBE4 (2020) suggested that cybercrime increased exponentially during COVID-19. A recent study shows that by 2025, cyberattacks will increase to 29%, doubling the incidents in 2023. (KnowBe4 Africa 2024). This was primarily due to cybercriminals' sophisticated use of AI tools in a context where vulnerable endpoints are prevalent.

The Interpol Africa Cyber Threat Assessment Report (2024) notes a rapid evolution of threat actors and their methods of operations, including the growing exploitation of emerging trends such as artificial intelligence, social media, and advanced social engineering techniques. To combat this crime wave, AFROPOL Report 2024 posits that a cumulative of 10490 arrests were made in some 19 African countries between January and December 2023, about cybercrime. Between September and October

2024, Interpol arrested 1006 in an operation dubbed “Operation Serengeti” (Interpol Africa Cyber Threat Assessment Report 2024). From a Kenyan touch between these two months, AFROPOL reported an arrest of 24 persons who extorted 8.6 million dollars in a credit card cyber scheme. Senegal recorded a loss of 6milion dollars with a gang including both Senegalese nationals and five Chinese nationals in a Ponzi scheme (AFROPOL Report 2024).

The ITU supports legal frameworks to combat cybercrime, while the African Union’s AUCSEG addresses regional gaps in cybersecurity awareness and capacity (Cybersecurity threat-scape of African countries, 2023). Lena and Corlane (2024) posit that despite the efforts at the continent’s level, most African countries are still at the formative stages of implementing nationwide measures to prevent cybercrime. On a region-by-region basis, the study posits that role modeling regions in cybercrime prevention are Eastern, Northern, and Western Africa, and Southern Africa, while Central African countries are still at the initial starting phase of the prevention measures (Lena & Corlane, 2024).

ANTIC (2022) statistics show two prevalent cybercrimes in Cameroon: scamming, 61%, and phishing, 27.80%. This report shows that the areas most affected by cybercrime are the university cluster zones of Yaoundé, Douala, Molyko in Buea, and the Noun. The perpetrator's ages range between 16 and 35 (Esther, 2022). (André B. & Ngaundje, 2019) shows that 90% of software and operating systems used in Cameroon are hacked, ranging from emails to social media accounts of businesses, individuals, etc. Assongmo (2016) reported the prevalence of telephone call fraud in Cameroon. All sectors in Cameroon are included in the threats caused by cybercrime. The mobile telecom sector in Cameroon lost 18 billion in 2016. Voa.com (Feb. 10, 2018) reports that the state lost 46 billion FCFA. Asongmo (2016) reports equally that between November and December 2013, Cameroon lost 3.5 billion FCFA to cybercrime. These losses project the fact that cybercrime is an economic detriment to the nation and the corporate world in Cameroon. The fight against cybercrime in the telecom sector is not very popular in Cameroon. What is seen mostly are government activities to combat the ill, which remain a threat to the population and businesses, notwithstanding cybercrime and cyberattacks. The measures implemented by the

government range from awareness creation, policy formulation, creation of the National Agency for Information and Communication Technologies (ANTIC), and the Telecom Regulatory Board (TRB), which is under the tutelage of the Ministry of Post and Telecommunication.

Committed to high governance standards, MTN aligns with King IV principles, ensuring integrity and professionalism. In Cameroon, a six-member non-executive board oversees operations, supported by a commercial legal service division for regulatory compliance. Committees report quarterly to the board under defined terms of reference (MTN Group Sustainability Report, 2023; MTN Group Management Report, 2024). Managed by division heads reporting to the CEO, MTN Cameroon's structure includes units like CFO, Risk and Compliance, Marketing, CTO & CISO, Mobile Financial Services, and Customer Service. These units drive daily operations, ensuring service quality and business growth (MTN Cameroon, 2023).MTN Cameroon promotes financial inclusion and supports UN Sustainable Development Goals through its core operations and community initiatives, striving to deliver a modern, connected life for all (MTN Cameroon, 2023).

1.2 Statement of the Problem

Cameroon ranks eighth in Africa for cybercrime prevalence, with losses amounting to 12.2 billion CFA francs in 2021. (Andre & Ngaundje 2019) Key challenges identified in Cameroon include policy gaps, lack of technical expertise and awareness, insufficient specialization, legal and resource allocation issues, and inadequate classification of critical infrastructure (Ntoko, 2021). The most affected sectors are government agencies, private businesses, schools, and hospitals, which face reputational damage, financial losses, and operational disruptions. Global projections state that cybercrime will cost the global market 10 trillion dollars and above in 2025, and continuous projections put the losses at 15 trillion dollars in 2029 (Statista, 2023). Global cyber insurance premiums are expected to grow from 14 billion Dollars to 29 billion dollars in 2027. Ransomware, the most prevalent cybercrime, will cost companies worldwide 265 billion dollars in 2031, from 20 billion dollars in 2021 (Jacob, 2024).

1.3 Objectives of the Study

The following objectives will guide the study;

1.3.1 General Objective

To determine the influence of workforce composition on cybercrime prevention in the Mobile Telephone Network in Cameroon.

1.3.2 Specific Objectives

i. To examine the influence of gender on cybercrime prevention in the Mobile Telephone Network in Cameroon.
ii. To assess the influence of employee experience on cybercrime prevention in the Mobile Telephone Network in Cameroon.
iii. To establish the influence of employee role in the organization on cybercrime prevention in the Mobile Telephone Network in Cameroon.
iv. To evaluate the influence of employee level of education on cybercrime prevention in the Mobile Telephone Network in Cameroon.
v. To determine the influence of functional area in the organization on cybercrime prevention in the Mobile Telephone Network in Cameroon.

1.4 Research Hypothesis

H_{01}: Gender has no significant influence on cybercrime prevention in the Mobile Telephone Network in Cameroon.

H_{02}: Employee experience has no significant influence on cybercrime prevention in the Mobile Telephone Network in Cameroon.

H_{03}: Employee role in the organization has no significant influence cybercrime prevention in the Mobile Telephone Network in Cameroon.

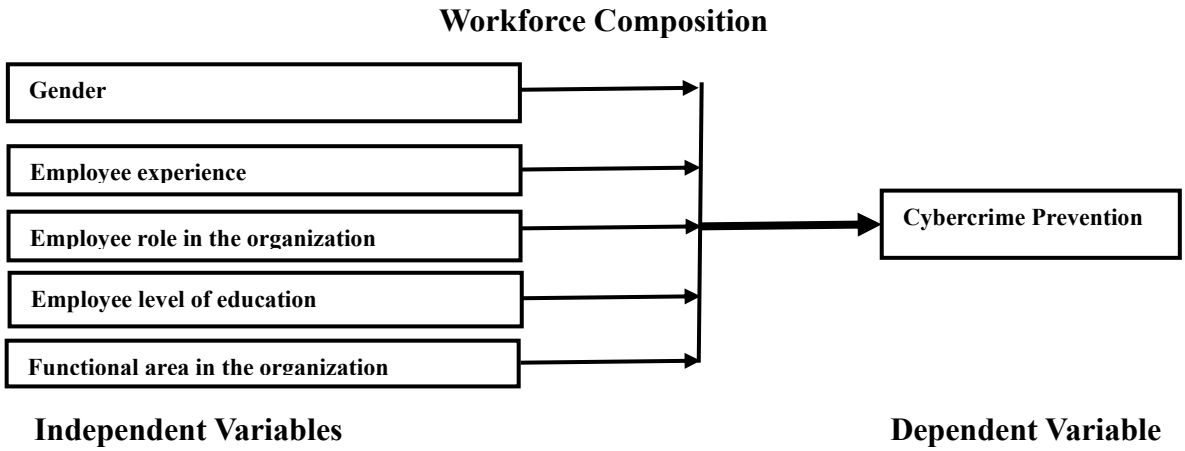
H_{04}: Employee level of education has no significant influence on cybercrime prevention in the Mobile Telephone Network in Cameroon.

H_{05}: Functional area in the organization has no significant influence cybercrime prevention in the Mobile Telephone Network in Cameroon.

2.1 Theories Reviewed

Theories reviewed include protection motivation theory, routine activity theory, theory of planned behavior, and knowledge, attitude, behavior model.

2.2 Conceptual Framework



Source: Author, 2025

4.1 Descriptive Analysis

4.1.1 Gender

The study investigated gender in Mobile Telephone Network in Cameroon. Gender refers to the roles, behaviors, activities, attributes and opportunities that any society considers appropriate for girls and boys, and women and men. This is because gender matters in cyber-crime prevention and is a human centric protection matter. Gender consideration prevent gender-blindness security policies, prioritizing safety of vulnerable groups, and boosting women participation in digital economy. From the findings as in Table 4.1, the majority of employees in the Mobile Telephone Network in Cameroon are males.

4.1 Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	194	69.8	69.8	69.8
	Female	84	30.2	30.2	100.0
	Total	278	100.0	100.0	

From the findings, more men participate in cybercrime prevention than women. However, women experience more of cyber staking and cyberbullying than men. The revealed the power dynamics, calls for more protective measures towards women than men. ITU report of 2019, revealed that the proportion of women using the internet globally was 48 percent, compared to 58 percent of men.

4.2 Employee Experience

The study further investigated in employee years of experience because it directly dictates the likelihood of human error, the susceptibility to social engineering, and the speed of incident reporting. It is about how experience shapes awareness, judgment, and response. Experience builds pattern recognition and stronger risk awareness.

4.2 Years have worked in your organization					
		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	Less than 1 year	9	3.2	3.2	3.2
	1-5 years	168	60.4	60.4	63.7
	6-10 years	30	10.8	10.8	74.5
	11-15 years	18	6.5	6.5	80.9
	16 years and above	53	19.1	19.1	100.0
	Total	278	100.0	100.0	

From the findings, the majority 71.2% have worked for between 1 and 10 years. 71.2% have worked for more than 16 years. Employees with more years of experience are generally better at identifying suspicious activities such as phishing emails, fake links, or unusual system behavior.

4.1.3 Employee Role in the Organization

The study carried out an investigation on employee experience. The findings were as in Table 4.3.

4.3 Role in the Organization					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Management	28	10.1	10.1	10.1
	Direct employee	218	78.4	78.4	88.5
	Indirect employee	32	11.5	11.5	100.0
	Total	278	100.0	100.0	

Majority of employees are in direct employment. 10.1% are in the management.

4.1.4 Employee Level of Education

The study examined the level of education. This was important because it helps organizations understand how human factors influence cyber security. Cybercrime is most out of human error.

4.4 Employee Level of Education					
		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	Nil	1	.4	.4	.4
	Primary	8	2.9	2.9	3.2
	Secondary	13	4.7	4.7	7.9
	University	256	92.1	92.1	100.0
	Total	278	100.0	100.0	

Majority of employees among Mobile Telephone Network in Cameroon are university graduates.

4.1.5 Functional area in your organization

This was carried out to allow for the identification of department-specific vulnerabilities, tailored risk management, and the mitigation of insider threats. The findings were as in Table 4.5.

4.5 Employee functional area in the organization

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Security	56	20.1	20.1	20.1
	HR	57	20.5	20.5	40.6
	Marketing	48	17.3	17.3	57.9
	Finance	38	13.7	13.7	71.6
	Others	79	28.4	28.4	100.0
	Total	278	100.0	100.0	

4.2 Correlation Analysis

The study carried out a correlation analysis among the variables. The findings were as in Table 4.7.

Table 4.7 Correlations

		Gender	EE	ER	ELE	FA	CCP
Gender	Pearson Correlation	1	-.053	-.088	.123*	.046	.008
	Sig. (2-tailed)		.382	.144	.041	.446	.896
	N	278	278	278	278	278	278
EE	Pearson Correlation	-.053	1	.012	-.152*	.072	.111
	Sig. (2-tailed)	.382		.843	.011	.233	.065
	N	278	278	278	278	278	278
ER	Pearson Correlation	-.088	.012	1	-.028	.090	.134*
	Sig. (2-tailed)	.144	.843		.642	.132	.026
	N	278	278	278	278	278	278
ELE	Pearson Correlation	.123*	-.152*	-.028	1	.012	.036

	Sig. (2-tailed)	.041	.011	.642		.844	.547
	N	278	278	278	278	278	278
FA	Pearson Correlation	.046	.072	.090	.012	1	-.129*
	Sig. (2-tailed)	.446	.233	.132	.844		.032
	N	278	278	278	278	278	278
CCP	Pearson Correlation	.008	.111	.134*	.036	-.129*	1
	Sig. (2-tailed)	.896	.065	.026	.547	.032	
	N	278	278	278	278	278	278
*. Correlation is significant at the 0.05 level (2-tailed).							

Table 4.7 presents the Pearson correlation coefficients among the study variables, all significant at $p < 0.01$ (two-tailed), with a sample size of 278. Cybercrime prevention and employee functional area, gender and employee experience, gender and employee role in the organization, employee level of education and employee role in the organization, employee level of education and employee experience all have negative correlation. From the findings, only employee role in the organization and functional area in the organization has significant correlation with cyber crime prevention.

4.3 Regression Analysis

The study carried out a regression analysis and results were as in Tables 4.7, 4.8, and 4.9.

Table 4.8 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.238[a]	.057	.039	.86815506

a. Predictors: (Constant), functional area in your organization., employee level of education, employee's roles in the organization, gender, employee experience

The overall model is highly statistically significant, as reflected by an F-statistic of 3.264 ($p < 0.007$), confirming that the set of predictors, as a whole, reliably accounts for variation in the dependent variable. P-value of less than 0.05 suggests that the regression model significantly explains the variation in the dependent variable (Field, 2013).

Table 4.9 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.300	5	2.460	3.264	.007[b]
	Residual	205.005	272	.754		
	Total	217.304	277			

a. Dependent Variable: Cyber Crime Prevention

b. Predictors: (Constant), functional area in the organization., employee level of education, employee role in the organization, Gender, experience

Findings, as in Table 4.10, show relationship between independent variables and dependent variables. These further tests are the power of Model 1

Able 4.10 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.213	.583		3.798	.000
	Gender	.053	.115	.028	.465	.642
	Employee experience	.094	.043	.130	2.180	.030
	Employee role in the organization	.286	.113	.150	2.525	.012
	Employee level of education	.122	.125	.059	.979	.329
	Functional area in the organization.	-.090	.035	-.154	-2.587	.010

a. Dependent Variable : Cyber Crime Prevention

On the influence of gender on cybercrime prevention in the Mobile Telephone Network in Cameroon. The result as in Table 4.10 show (t = .465 p = .642), and since p –value is greater than p = 0.05, the study failed to reject the null hypothesis and confirmed that gender has no significant influence on cybercrime prevention in the Mobile Telephone Network in Cameroon.

On the influence of employee experience on cybercrime prevention in the Mobile Telephone Network in Cameroon. The result as in Table 4.10 show (t = 2.180 p = .030), and since p –value is less than p = 0.05, the study rejected the null hypothesis and confirmed that employee experience has significant influences on cybercrime prevention on the Mobile Telephone Network in Cameroon.

On the influence of employee role in the organization on cybercrime prevention in the Mobile Telephone Network in Cameroon. The result as in Table 4.10 show (t = 2.525 p = .012), and since p –value is less than p = 0.05, the study rejected the null hypothesis and confirmed that employee role in the organization has significant influences on cybercrime prevention in the Mobile Telephone Network in Cameroon.

On the influence of employee level of education on cybercrime prevention in the Mobile Telephone Network in Cameroon. The result as in Table 4.9 show (t = .979 p = .329), and since p –value is greater than p = 0.05, the study failed to reject the null hypothesis and confirmed that employee level of education has no significant influence on cybercrime prevention in the Mobile Telephone Network in Cameroon.

On the influence of functional area in the organization on cybercrime prevention in the Mobile Telephone Network in Cameroon. The result as in Table 4.10 show (t = -2.587 p = .010), and since p –value is less than p = 0.05, the study rejected the null hypothesis and confirmed that functional area in the organization has significant influence on cybercrime prevention in the Mobile Telephone Network in Cameroon.

The estimated regression equation based on Table 4.10 is:

$$\mathbf{Y= 2.213+ .053X_1+ .094X_2 +.286X_3 + .122X_4 - .090X_5 + .86815506}$$

The equation show that by improving gender by 1 unit, cybercrime prevention in the Mobile Telephone Network in Cameroon will increase by .053 units. By improving employee experience by 1 unit, cybercrime prevention in the Mobile Telephone

Network in Cameroon will increase by .094 units. By improving role in the organization by 1 unit, cybercrime prevention in the Mobile Telephone Network in Cameroon will increase by .286 units. By improving employee level of education by 1 unit, cybercrime prevention in the Mobile Telephone Network in Cameroon will increase by .122 units. By improving functional area in the organization by 1 unit, cybercrime prevention in the Mobile Telephone Network in Cameroon will increase by -.090 units.

5.1 Summary of findings

From the findings, workforce composition influence cybercrime prevention in the in Mobile Telephone Network in Cameroon. In addition, employee role in the organization, employee functional area in the organization and employee experience has significant influence in cyber-crime prevention in the Mobile Telephone Network in Cameroon. Employees' gender and level of education have no significant influence on cybercrime prevention.

5.2 Conclusions

The study concludes that employee experience, education level, and functional area are significant influence in cybercrime prevention within MTN Cameroon. Employees with adequate experience and higher education levels tend to demonstrate better awareness of cyber threats and are more capable of adhering to security protocols. Without continuous training and awareness programs, employees may become complacent or fail to keep up with evolving cyber threats. This calls for balanced workforce supported by continuous learning, role-specific training, and strong organizational policies grounded in Cybersecurity principles. Additionally, different functional areas face varying levels of exposure to cyber risks, with departments such as IT and finance being more vulnerable due to their access to critical systems and sensitive data. Focus on gender and employee level of education does not meaningfully improve cybercrime prevention posture.

5.3 Recommendations

Strengthen onboarding programs for new employees, adopt role-based (functional) security training, implement continuous cybersecurity training, promote a strong

cybersecurity culture, enforce access control and least-privilege principles, regularly update security policies and practices, and leverage workforce diversity.

Provide equal cybercrime prevention training for all, regardless of gender or level of education. Strengthen security awareness programs, focus on role-based training, promote a security-conscious culture, implement clear policies and procedures, have regular assessments, and encourage inclusivity and avoid bias. Enhance training for non-technical staff, leverage experienced employees, continuous learning programs, clear security responsibility, and simulate real cyber threats.

References

1. African Media Agency. (2023). *International Women's Day: Addressing the gender gap in the technology sector*. Imane Charioui.
2. Akafor, O., & Asare, B. (2021). Examining the role of governance in telecom cybersecurity: A comparative analysis of Cameroon and Nigeria. *International Journal of Telecommunication and Cybersecurity, 9*(2), 90–106.
3. Dambaba, S., & Ngom, A. (2020). The effectiveness of cybersecurity governance in Africa: A case study of Cameroon's telecom sector. *Journal of Cybercrime & Digital Policy, 8*(1), 14–28.
4. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate data analysis* (7th ed.). Pearson Education.
5. Hilbert, M. (2012). The end justifies the definition: The manifold outlooks on the digital divide and their practical usefulness for policy-making. *Telecommunications Policy, 35*(8), 715–736.
6. Kane, G. C., Phillips, A. N., Copulsky, J., & Andrus, G. R. (2019). *The technology fallacy: How people are the real key to digital transformation*. MIT Press.
7. Kone, L., & Tchana, M. (2019). Cybersecurity governance and risk management in the mobile telecommunications industry: An African perspective. *Journal of African Telecommunications, 7*(4), 221–225.

8. Mbe, P., & Amang, J. (2020). The impact of digital literacy on cybercrime prevention in Africa: A focus on Cameroon. *International Journal of Cybersecurity Education, 7*(3), 153–168.

9. Mugenda, O. M., & Mugenda, A. G. (2003). *Research methods: Quantitative and qualitative approaches*. Acts Press.

10. Mve, S., & Ndangam, R. (2019). Enhancing digital literacy to curb cybercrime: A study on mobile network security in Cameroon. *Cybersecurity Policy Review, 4*(2), 48–62.

11. Ndiaye, T., & Wounang, R. (2019). Digital literacy and its role in reducing cybercrime in African telecom sectors. *Journal of African Telecommunications and Cybersecurity, 13*(2), 150–164.

12. Njoh, F., & Essama, L. (2020). Governance structures and cybercrime prevention in the telecommunications sector in Cameroon. *International Journal of Information Security and Privacy, 14*(3), 57–73.

13. Nsom, E., & Nguepjou, C. (2021). Enhancing digital literacy to combat cybercrime: Case study of telecom operators in Cameroon. *African Journal of Information and Communication Technology, 11*(1), 45–59.