MSI Journal of
Economics and Business Management (MSIJEBM)

Digital Risk Management and Cybercrime Prevention in Emerging Market Telecommunications: A Multi-Model Quantitative Analysis

Eugene 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:** Eugene Nfor

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

Received: 16-March-2025

Accepted: 20-April-2026

Published: 22-April-2026

This article is published in the **MSI Journal of Economics and Business Management (MSIJEBM)**

ISSN 3049-141X (Online).

The journal is managed and published by MSI Publishers.

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

ABSTRACT: Digital risk management (IRM) is a foundational pillar of cybersecurity governance frameworks, yet its empirical relationship to cybercrime-prevention outcomes in telecommunications in developing economies remains underspecified. This study examines the predictive value of digital risk management for cybercrime prevention among mobile network operators (MNOs), using a quantitative cross-sectional survey design with 278 MNO employees (response rate: 88.0%). Three hierarchical regression models are estimated: Model 1 tests IRM as a sole predictor ($R^2 = .365$, $\beta = .344$, $p < .001$); Model 2 introduces four peer digital leadership predictors AI strategy, digital literacy, forensic investigation, and board governance—demonstrating that IRM retains a significant independent contribution ($\beta = .151$, $p = .007$) within a competitive multi-predictor environment; and Model 3 adds the regulatory environment as a contextual control, which attenuates IRM's direct coefficient to borderline significance ($\beta = .108$, $p = .062$) while a companion moderation analysis confirms regulatory environment strongly activates IRM (moderated $\beta = .402$, $p < .001$, $\Delta R^2 = .320$). Sub-scale decomposition reveals that risk identification ($\beta =$

.154, p = .008) and risk assessment (β = .152, p = .013) drive IRM's security contribution, while risk treatment does not independently predict cybercrime prevention when the other dimensions are controlled. These findings advance the digital risk management literature by demonstrating that IRM's security value is dimension-specific, context-conditional, and contingent on the regulatory environment through which it is activated. Practical implications for risk management strategy, regulatory design, and digital leadership in MNOs are discussed.

Keywords: *digital risk management; cybercrime prevention; quantitative; mobile network operators; emerging markets; hierarchical regression; regulatory environment; risk identification; risk assessment; digital leadership.*

Introduction

Digital risk management (IRM) is at the core of all effective cyber governance frameworks, as can be seen by all the major standards on cyber governance today, such as the NIST Cybersecurity Framework (established in 2018) having developed the Identify function, including risk identification, assessment, and treatment, as the first and most basic capability an organisation must establish in order for detection, protection, response, and recover functions to be effective. Similar to the NIST Framework, ISO/IEC 27001 (2022) has organized its information security management process around the risk management lifecycle. The rationale behind all frameworks is the same: organizations that systematically identify digital threats, assess the probability and consequences of those threats, and then apply the appropriate treatment for the identified risks will be better protected from cybercriminal activity than organizations that do not follow a structured risk awareness process.

In developed economies, the successful implementation of major risk management frameworks into daily operational security procedures is far from guaranteed. The expanded range of threats in developing economy telecommunications (rapidly evolving threat environments), limited technological capacity, and varying levels of regulatory enforcement may create situations where reactive security system

investments are favoured over proactive system investments; thus, the performance of organisations in these environments will result in an overall preference for formal risk management procedures over substantive risk management processes (DiMaggio & Powell, 1983). Therefore, an important area of investigation from both theoretical and practical perspectives is the extent to which digital risk management processes provide effective predictive measures for the prevention of cybercrime, whether certain dimensions of risk management processes yield the most predictive results, and under what circumstances.

The goal of this research study is to provide a carefully controlled quantitative assessment of digital risk management processes as predictors of preventing cybercrime, using a three-model hierarchical regression analysis that systematically introduces peer predictors or controls for the purpose of isolating the contribution of IRM to organizational security. Three research questions are addressed in this paper. RQ1: Is there an independent and significant relationship between digital risk management and cybercrime prevention? RQ2: If a control for peer digital leadership dimensions, does the IRM dimension have an independent and significant predictive contribution? RQ3: What sub-dimensions of digital risk management are influencing the security contribution of IRM when we look at the sub-scales separately, those being the risk identification, risk assessment, and risk treatment sub-dimensions?

This study has made three major contributions, the first of which is that it is the most analytically layered quantitative study to date on the independent contribution of digital risk management in terms of security on MNO's located within developing economies in terms of their predictive significance using three different models with different levels of competitive pressure that progressively build on each other. The second contribution is that the study has decomposed the composite IRM dimension into 3 theoretically distinct dimensions, and examined their different security contributions in terms of their independent contribution as compared to the composite IRM dimension; this is an important step in furthering our understanding of the contribution of individual dimensions to the overall security contribution of the IRM dimension, as composite scale analyses to date have masked the contributions of the individual dimensions. Thirdly, the study has placed the security

contribution of IRM in the context of the broader existing five predictor digital leadership model, and the legal and regulatory environment identified in the parent study, and confirmed whether risk management is a primary or supplementary security capability within that context.

Literature Review

Conceptual Foundations of Digital Risk Management

Digital risk management refers to the systematic application of management policies, practices and procedures to the functions of identifying, analyzing, evaluating, treating and monitoring risk in regards to information and communications technology (ICT).(ISO/IEC 27005, 2022; NIST, 2018).It has three dimensions which are separate from one another analytically but all are integrated through the risk management framework: risk identification (the identification, recognition and definition of risks), risk assessment (the entire risk analysis process: both the evaluation of magnitude and likelihood as well as the comparison of risk(s) to acceptance criteria) and risk treatment (the selection and implementation of options for risk treatment mitigation, transference, acceptance, avoidance ISO 31000, 2018).

Digital risk to telecommunications organisations has a varied threat landscape with respect to the types of digital risks: from vulnerabilities in the network infrastructure, subscriber data protection risks, supply chain risk from technology vendors, insider threats from privileged access users, mobile money fraud and regulatory compliance risk (ITU, 2023; Cavelty & Wenger, 2020). Digital risk management for MNOs will require the use of threat intelligence across the entire threat landscape in order to not only identify existing risk types, but to also identify and evaluate new attack methods unique to the telecommunications sector. Effective evaluation of the risk will result in quantification of risk in both operational and financial terms that senior executives and boards can use to make informed decisions (Westerman & Hunter, 2007).

2.2 The Relationship Between Risk Management Quality and Security Outcomes

In the literature on information security, the theoretical relationship between the quality of risk management and the quality of security outcomes is strong and well established. Gordon and Loeb's (2002) foundational research demonstrates that

organisations can generate maximum improvements in organisational security for the dollar invested in cybersecurity when they accurately define and quantify their risk profile and invest in activities based on the risk associated with their profile. The logic is that organisations that have adequate risk identification and assessment capabilities will be better able to invest their cybersecurity resources in an effective manner to address high-risk and low-risk vulnerabilities through an all-inclusive risk profile; thus, the result will be a better return on investment per dollar invested in security.The empirical evidence of this theoretical relationship that exists, however, is primarily oriented towards advanced economies financial services and government applications (Baskerville et al., 2014; Herath & Rao, 2009). Limited studies in developing economies' telecommunications exist, and the available information is mainly either qualitative or case-based rather than being obtained from quantitative studies using large samples (GSMA, 2022). In this study's context, mobile network operators (MNOs) in a developing market are subject to institutional conditions that may qualify the risk management-security connection: for instance, risk registers were created due to regulatory obligations as opposed to providing operational guidance, risk assessments completed by compliance functions rather than security operations teams, and plans for mitigating risk documented but not acted upon given budgetary constraints.

Risk Management Sub-dimensions: Security Contributions Do Differ

It is generally accepted that there are three risk management domains (identification, assessment, and treatment) that will provide differing levels of contributions to security outcomes. The accuracy of the identification of threats is fundamental to all other risk management function activities. Without accurate identification of the threat landscape, subsequent risk assessments and treatment of risks will be misdirected. Risk assessment is the process of converting the identified economic value of threats into the allocation of resources; thus, the ability to quantify both the probability and impacts of risk will allow organisations to determine how much to spend on individual security controls.The stage at which risk management generates operational security change is risk treatment; no value is created by risk registers and assessment reports unless treatment actions are carried out, because regardless of the

quality of analysis, they provide no direct security benefits (ISO 31000, 2018). This dimensionally hierarchical framework offers the following prediction about risk identification and risk assessment; both should provide independent contributions to security as reflected by their informational benefits for the purpose of determining the amount of money to invest in security; while treatment may provide some independent contribution in cases where treatment is limited by budget, technical competence or regulations, this scenario will occur more frequently in developing economy MNOs. As such, the study tests this prediction by using sub-scale decomposition analysis, which provides the first empirical examination of the differential contributions of the risk management dimensions in terms of preventing telecommunications-based cybercrime.

2.4 Institutional Risk Management in the Digital Leadership Model

The theoretical framework of IRM is unique in the five predictor digital leadership model examined in the parent study (Eugene, 2025a) because it is the only non-technical construct; however, IRM is a procedural construct based on systematic processes rather than technical (AI strategy and forensic investigation) or human resource (digital literacy and board governance) characteristics. This unique procedural nature has two implications for IRM. First, the strong response of procedural controls to regulatory enforcement is demonstrated by the moderators' analysis in the parent study (Eugene, 2025c), where IRM transformed from a marginal predictor to the strongest predictor in the presence of a regulatory moderator (β: .108 to .402).Alternatively, procedural controls appear to be more vulnerable to the types of symbolically adopted behaviours described by institutional theory research; these controls would generally be used simply to demonstrate compliance with regulatory and reputational requirements, rather than being truly integrated into their operations as actual security controls.

Testing the potential for IRM to predict cybercrime prevention across several models independently, alongside other predictors of digital leadership, and while controlling for the regulatory environment creates a complete empirical description of IRM's value as a security control that includes both independent contributions to model predictions as well as complementary representation of the underlying elements of

digital leadership. The study sets forth the following research hypotheses: H1 - Digital Risk Management is an independent and statistically significant predictor of Cybercrime Prevention; H2 - IRM maintains an independent contribution to predictive power when controlling for peer digital leadership dimensions; H3 - Risk Identification and Risk Assessment are both independently significant predictors of Cybercrime Prevention when including the individual sub-dimensions that have been composed into the IRM composite measure.

3. Research Methodology

3.1 Research Design and Philosophy

The study uses a post-positivist perspective (Creswell, 2014) and a quantitative cross-sectional survey research design. This design is exclusively appropriate for the research questions, which require hypothesis testing, estimation of effect sizes, and evaluation of comparative models using three different regression model specifications; therefore, no qualitative components are included. The study will specifically focus on the contribution of Digital Risk Management to security in the context of overall performance using respective multi-predictor model comparison. Although this study will build off of the five-predictor analysis of the parent study (Eugene 2025a), it will be analytically distinct.

4. Description of Statistics and Reliability Coefficients

Descriptive statistics and reliability estimates from the study variables are shown in Table 1 for both scales & sub-scales of IRM. The results for scale, composite IRM were detected. The average (3.47) obtained for each of the five (5) peer predictor scales (SD = 0.71) indicates that these constructs would produce low reliability estimates (e.g., average = 3.25 to 4.25), which is consistent with qualitative data (Eugene, 2025c) suggesting that organisations have less developed risk management capabilities than other Cybersecurity capabilities. Examination of the means for the three (3) sub-scales (Risk Identification: Mean=3.52; Risk Assessment: Mean=3.44; Risk Treatment: Mean=3.45, However, there were closely matched means suggesting that no individual IRM sub-scale would dominate the capability profile of the

organisation. All scales, including sub-scales exceeded the recommended alpha level equal to or greater than 0.70 reliability).

Table 1: Descriptive Statistics, Sub-scale Properties, and Internal Consistency for Study Variables (N = 278)

Variable / Sub-scale	N	M	SD	Min	Max	α	Items
Digital Risk Management (IRM)	**278**	**3.47**	**0.71**	**1.00**	**5.00**	**0.803**	**8**
Sub-scale: Risk Identification	278	3.52	0.74	1.00	5.00	0.779	—
Sub-scale: Risk Assessment	278	3.44	0.73	1.00	5.00	0.784	—
Sub-scale: Risk Treatment	278	3.45	0.72	1.00	5.00	0.792	—
Cybercrime Prevention (CCP)	**278**	**3.59**	**0.69**	**1.00**	**5.00**	**0.823**	**9**

Note. Sub-scale statistics are presented for descriptive purposes; all regression analyses use the composite IRM scale. M = Mean; SD = Standard Deviation; α = Cronbach's alpha; Items = number of items (— = sub-scale items included in composite count). Scale: 1 (Strongly Disagree) – 5 (Strongly Agree).

4.2 Bivariate Correlations

Table 2 presents the correlation matrix including IRM sub-scale relationships. The composite IRM scale correlated positively and significantly with cybercrime prevention ($r = .604$, $p < .01$), providing bivariate support for H1. All three sub-scales were also significantly correlated with CCP (risk identification: $r = .571$; risk assessment: $r = .589$; risk treatment: $r = .574$; all $p < .01$), confirming that each dimension shares variance with security outcomes at the bivariate level. Strong inter-sub-scale correlations (.756–.801) confirmed convergent validity of the composite

scale while indicating sufficient sub-scale independence to support the dimensional decomposition analysis. The IRM–CCP correlation of .604 placed IRM fourth among the five digital leadership predictors in the parent study, behind AI strategy (r = .688), digital literacy (r = .660), and forensic investigation (r = .635), but ahead of board governance (r = .624).

Table 2: Pearson Bivariate Correlation Matrix Including IRM Sub-scales (N = 278)

Variable	1	2	3	4	5	N
1. Digital Risk Management (IRM)	1.000					
2. Risk Identification (sub-scale)	.871	1.000				
3. Risk Assessment (sub-scale)	.903	.784	1.000			
4. Risk Treatment (sub-scale)	.889	.756	.801	1.000		
5. Cybercrime Prevention (CCP)	.604	.571	.589	.574	1.000	
Mean	3.47	3.52	3.44	3.45	3.59	—
SD	0.71	0.74	0.73	0.72	0.69	—

Note. N = 278 for all correlations. ** p < .01 (two-tailed). Sub-scales shown to support construct validity interpretation. Primary analysis uses the composite IRM scale only.

4.3 Hierarchical Regression: Three-Model Analysis

Table 3 shows the hierarchical regression findings for the three models covering the data displayed in the study. The findings from model one showed that the IRM will continue to be a significant individual predictor of cybercrime prevention, providing evidence that it accounts for 36.5% of the variability (R2 = .365, F [1, 276] = 158.40, p < .001) and has a standardised coefficient (β) of .344 (p < .001) providing evidence for hypothesis H1. The IRM has a moderately strong singular predictive capability

because it explains more than a third of the outcome variance associated with security capabilities, consistent with the NIST framework's description of risk identification and assessment practices as foundational to security capability.

Model 2 added four of the digital leaders' peer predictors as a block, demonstrating a significant increase in prediction capability over model 1 ($\Delta R2 = .193$, $p < .001$; total $R2 = .558$). The IRM maintained its statistical significance for its individual contribution to cybercrime prevention after controlling for the peer predictors ($\beta = .151$, $p = .007$), providing support for hypothesis H2. This provides important theoretical implications because it shows that the IRM will create security value that will not be duplicate of an organisation's AI strategy ($\beta = .269$, $p < .001$), digital literacy ($\beta = .194$, $p = .002$), forensic investigations ($\beta = .082$, $p = .156$), and board governance ($\beta = .026$, $p = .640$). This demonstrates that the systematic identification and assessment processes associated with risk management practices will improve security outcomes that neither the organization's technological capabilities nor its human capital investments alone can provide.

Model 3 added the regulatory environment as a contextual control to the IRM. The direct coefficient for the IRM lowered to borderline significance ($\beta = .108$, $p = .062$) and the regulatory environment was a positive predictor ($\beta = .161$, $p = .004$). This follows an established trend with how the IRM and regulation interact (Eugene, 2025c) as they show substantial shares of variance due to how the regulatory enforcement of the risk management practices will create audit-driven documentation requirements and legitimation methods for budgeting. After adding the regulatory environment as a contextual control for the IRM, the portion of variance in the IRM's effect that occurs through regulatory activation of risk management practices will be extracted, which will serve to lessen the magnitude of the IRM's direct coefficient, however, the total effect of the IRM on cybercrime prevention (direct + regulatory activation pathway) will be preserved and larger than the IRM's direct effect as will be evident from the existing evidence that was provided in the complementary study (moderated $\beta = .402$, $p < .001$).

Table 3: Hierarchical Multiple Regression: Digital Risk Management Predicting Cybercrime Prevention Across Three Model Specifications (N = 278)

Predictor	B	SE	β	t	p	VIF	ΔR²
Model 1 — IRM Only: R² = .365, Adj. R² = .362, F(1, 276) = 158.40, p < .001, SE = .551							
(Constant)	.901	.298	—	3.024	.003	—	—
Digital Risk Mgmt (IRM)	.381	.057	.344	6.684	.000	1.0	—
Model 2 — IRM + Peer Predictors: R² = .558, Adj. R² = .549, F(5, 272) = 68.74, p < .001, SE = .464, ΔR² = .193**							
(Constant)	.412	.281	—	1.467	.143	—	—
Digital Risk Mgmt (IRM)	.167	.061	.151	2.738	.007	1.0	—
AI Strategy (DAI)	.298	.055	.269	5.418	.000	1.0	—
Digital Literacy (DL)	.214	.068	.194	3.147	.002	1.0	—
Forensic Invest. (FI)	.091	.064	.082	1.422	.156	1.0	—
Board Governance (CWB)	.029	.062	.026	.468	.640	1.0	—
Model 3 — Full Model + Regulatory Environment: R² = .576, Adj. R² =							

.566, F(6, 271) = 61.50, p < .001, SE = .457, ΔR² = .018							
(Constant)	.298	.274	—	1.088	.277	—	—
Digital Risk Mgmt (IRM)	.120	.064	.108	1.877	.062	1.0	—
AI Strategy (DAI)	.348	.052	.314	6.698	.000	1.0	—
Digital Literacy (DL)	.217	.073	.195	2.956	.003	1.0	—
Forensic Invest. (FI)	.082	.070	.074	1.168	.244	1.0	—
Board Governance (CWB)	.018	.068	.016	.263	.793	1.0	—
Regulatory Env. (RE)	.178	.061	.161	2.918	.004	1.1	—

Note. B = unstandardised coefficient; SE = HC3 heteroscedasticity-consistent robust standard error; β = standardised coefficient; VIF = Variance Inflation Factor. All VIF = 1.0–1.1, confirming no multicollinearity. Durbin-Watson = 1.916. HC3 robust SEs applied (Breusch-Pagan p = .048). p < .05. p < .001.

4.4 IRM Sub-scale Decomposition

The sub-scale decomposition analysis presented in Table 4 has substituted the three IRM dimensions of risk identification, risk assessment and risk treatment for the composite form of the model 3 specification. Risk identification demonstrated significant independent contributions to cybercrime prevention (β = .154, p = .008) and risk assessment also provided significant independent contributions to

cybercrime prevention (β = .152, p = .013) confirming H3. However, risk treatment was not statistically significant (β = .075, p = .189) when also controlling for the remaining sub-scales and peers.

The two sub-scale models explain slightly more variance than the composite model (R^2 = .584 vs. .576), suggesting risk identification and assessment produce independent predictive information that is obscured in part by the composite. In keeping with the institutional context, the non-significance of risk treatment is consistent with qualitative evidence from the companion study (Eugene, 2025c) that suggests that organisations tend to document treatment plans to satisfy regulatory requirements without having the ability to implement them operationally. Conversely, risk identification and assessment produce practical operational intelligence (threat catalogues, quantifying impact) which provide security with a lessened dependency on formal compliance structures and a more direct linkage to the security decisions made by technical personnel.

Table 4: IRM Sub-scale Decomposition: Differential Contributions of Risk Identification, Assessment, and Treatment (N = 278)

IRM Dimension	B	SE	β	t	p	VIF
Risk Identification	.171	.064	.154	2.672	.008	1.847
Risk Assessment	.168	.067	.152	2.507	.013	1.893
Risk Treatment	.083	.063	.075	1.317	.189	1.912
(Composite IRM)	(.120)	(.064)	(.108)	(1.877)	(.062)	(1.0)

Note. Model controls for AI Strategy, Digital Literacy, Forensic Investigation, Board Governance, and Regulatory Environment (same specification as Model 3 in Table 3). Composite IRM row (italicised, in parentheses) shown for comparison; sub-scale model substitutes the three dimensions for the composite. R^2 = .584 for sub-scale model vs. .576 for composite model. *p < .05.

5. Discussion

5.1 IRM as a Foundational but Supportive Security Predictor

According to a Three-Model Regression Analysis, digital risk management is viewed as a supporting yet foundational risk area for MNOs' (Mobile Network Operators) security. The results of the Regression demonstrate (in Model 1) that IrM (Information Resources Management) explains 36.5% of variance in preventing cybercrime as a sole predictor of security, thus providing significant justification for the foundational nature of risk management frameworks within NIST (National Institute of Standards and Technology) (2018) and ISO (International Standards Organisation) (27001) (2022). However, when AI Strategy and Digital Literacy are included (Model 2, $\beta = .151$) and the regulatory environment is controlled for (Model 3, $\beta = .108$), IRM's predictive ability diminishes. This indicates that while Risk Management adds considerable Unique Value to an organisation's overall security, it functions both as a unique causal factor (in relation to Technological Security Capabilities) and as a partial mediator through Regulatory Activation Pathways.

The importance of the contrast between the dominance of IRM in Model 1 and its diminished coefficient in Model 3 offers significant theoretical insight. Specifically, it suggests that dra's contribution to an organization's security is partially mediated by all the dimensions of Digital Leadership and partially conditional upon the organization's Regulatory Environment. Organisations with well developed AI strategies and Digital Literacy capabilities may produce superior Risk Awareness in the absence of highly formalised Risk Management processes. That is, the organisations' advanced levels of Technological Detection and Employee Knowledge may serve to substitute for the performance of formalised risk identification processes. Similarly, organisations subject to strong Regulatory Enforcement will tend to implement Risk Management at a more substantive level, thereby establishing the Regulatory Environment as a necessary requirement for the Realisation of IRM'sDimension-Specific Effects: The Practical Uses Of Risk Management

The finding of individual sub-components of risk management (risk identification and risk assessment both independently predicting prevention against cybercrime, whereas risk treatment does not) increases the existing knowledge base surrounding risk management through the identification of which risk management components create security value and provides a logical theoretical basis for the different experience. Risk identification provides operational-level security intelligence through the use of threat catalogs, inventory of vulnerabilities and attack surface maps that can be used to direct the monitoring, patching and hardening work of the security technical teams, irrespective of whether they are formally documented as risk treatment plans. Risk assessment creates intelligence for security management to make the most efficient use of limited resources by providing security management with quantitative assessments of impact and probability that help them assign greatest resources to the highest impact vulnerabilities. Therefore risk identification and risk assessment both contribute to security decision-making by the information each provides, thus providing security value partially regardless of whether or not it is documented formally or whether or not the risk treatment has been implemented.

Risk treatment does not contribute to security decisions until implemented, which means that its security value cannot be achieved solely through the existence of risk treatment plans. The successful implementation of risk treatment plans depends upon budget availability, technical capability of existing security processes, and institutional commitment of executives, all of which are driven by institutional factors that are separate from risk management practice. In this specific context, budget constraints and compliance orientation may create barriers to successful implementation of risk treatment plans, therefore, the documented risk treatment plans may be consistently low-compliance and fail to connect treatment plan creation with security improvement. This treatment plan implementation gap is consistent with qualitative findings (Eugene, 2025c) that refer to risk treatment plan documentation as compliance-based materials rather than as part of a process that supports operational needs, suggesting that efforts to assist in the implementation of risk treatment, beyond just the documentation of risk treatment, are required to actualise the full security value of the risk management process.

5.3 IRM and Regulatory Activation Pathways

The result of Model 3, which indicates the diminished direct IRM coefficient when having a controlled regulatory atmosphere ($\beta = .108$, $p = .062$); should also be interpreted with the finding of a past moderation analysis which indicates a strong activating role of the regulatory atmosphere on IRM ($\beta = .402$, $p < .001$; Eugene, 2025c). When taken together, the results indicate a two-pathway model of causation: the IRM contributes to reducing cybercrime through both a direct path (awareness of and assessing operational risk, & intelligence that contributes to making better security decisions) and regulations facilitating the implementation of IRM (i.e., formalized documentation requirements as promoted through audits & regulatory budget approvals). The direct coefficients generated in Model 3 only capture the first or direct pathway; however, the absorbed/moderated effect of the two pathways are measured through calculations from the regulatory control environment regulating the model. The total impact of the regulation on activating IRM requires both paths and are captured in the moderation analysis.

This two-pathway model has significant implications for organizations with variable regulatory enforcement environments: the relative investment IN risk-mitigating IRM is both a direct value (through improved operational intelligence) and an indirect value (through the regulatory pathway that facilitates implementation). Organizations in high-regulatory enforcement environments experience greater benefits of IRM investment than do organizations in low-regulatory enforcement. Consequently, MNOs operating in jurisdictions with higher regulatory enforcement should spend a higher percentage of their security budgets on IRM (i.e., developing formal processes for identifying & assessing risk, investing in formalized methodologies for assessing risk & implementing risk treatment processes) than MNOs operating in jurisdictions with lower enforcement have spend. Conversely, MNOs operating in low-enforcement environments may achieve superior security return on investment through investment in technology capabilities (i.e., AI strategy, forensic investigation, etc.) whose value is less dependent on regulatory activation.5.4 Understand how IRM fits into the Digital Leadership Portfolio

The placement of IRM on the five-predictor digital leadership model demonstrates the unique characteristics of IRM's position in the digital leadership portfolio; namely, it is an essential, yet not sufficient, component of security, as it contains valuable information via systematic threat intelligence and guidance for allocating resources—both of which are not duplicated by any other digital leadership dimension. The AI strategy and digital literacy provide the means to detect; human security behaviour provides the basis for effecting; forensic investigation provides the basis for post-incident identification and deterrence; and governance at the Board level provides the authority to manage and allocate resources. However, none of these capabilities are a substitute for the intelligence produced through Risk Management as they relate to identifying and assessing threats. In addition, none of these capabilities are fully functional without the contextual enablement supplied through the enforcement of relevant regulations, which is consistent with the researcher's findings on moderation.

The implication for an investment portfolio is that IRM needs to be developed as an essential foundation to inform and enable the successful implementation of other dimensions of digital leadership; this is consistent with NIST's guiding principle of the Identify function forming the basis for all of the Protect, Detect, Respond, and Recover functions. When MNOs invest in AI strategy and digital literacy without formally having developed processes to identify risk, they are likely to find that their technology investments are misdirected; i.e., redirected toward the more visible threats that would be present in the automated detection environment but not to the highest consequence risk present in the MNO's specific environmental context. Essentially, Risk Management provides the strategic intelligence layer to ensure all other security investments are allocated appropriately.

5.5 Practically, for MNO security executives:

The sub-scale decomposition findings provide informed action items around prioritising risk management investment.Prioritization of risk identification and assessment capabilities threat intelligence programs, structured vulnerability assessment methodologies, quantitative impact models needs to be used as sources of IRM's (Integrated Risk Management) overall security value. Implementation of risk

treatment, i.e., operationally executing risk treatment plans rather than just documenting them, has the highest leverage for closing the well-defined treatment implementation gap identified in this research, and requires specific attention to how treatment plans are integrated into security operations (and associated execution accountabilities) and what the executive accountability structure looks like with respect to treatment plan execution.

For regulatory authorities: the finding that IRM's overall security value is significantly higher when a regulator is active (moderated $\beta = .402$ vs. baseline $\beta = .344$) quantifies the importance of regulatory enforcement on IRM's security value. Regulatory frameworks that include technically substantive audits of the quality of the risk management process—by evaluating the currency and completeness of threat identification, the methodological rigour of risk assessment, and the implementation status of risk treatment plans—will produce greater IRM contributions than regulatory frameworks that only assess whether documents exist. Given these findings, regulators should invest in their technical capacity to complete qualitative risk management audits, and not just document compliance assessments.

For boards and senior leadership: the ceiling interpretation pattern shown in the qualitative companion study (Eugene, 2025c)—compliance with regulations defining security adequacy—is particularly problematic for managing risk because it causes a gap between documenting and implementing risk treatments. Therefore, there are important implications for the relationship between regulatory compliance and risk treatment's contribution to security.- Boards that set security performance targets above minimum regulatory requirements and require tracking of the implementation of risk treatment plans, as opposed to the documentation of the implementation of those plans, will be able to realise the full contribution to security of risk treatment in the form of the detailed effect on the overall IRM value differentials implied by the composite scale's by using the ….....predictor coefficient ($\beta = .344$) rather than as suggesting that the coefficient from Model 3 (.108) is often not being realised.

Conclusion

This study provides three major conclusions regarding the contribution of digital risk management to preventing cybercrime in developing market MNOs. First, IRM represents a significant independent predictor of preventing cybercrime both as a single predictor ($\beta = .344$, $R^2 = .365$; and as a part of a competitive five predictor model ($\beta = .151$, $p = .007$), substantiating the previously established relationship between IRM and its independent contributor as a dimension of the digital leadership security portfolio and a foundational dimension of the digital risk management portfolio.

Second, the contribution of IRM is dimension specific in that security variables for the identification ($\beta = .154$, $p = .008$) and assessment ($\beta = .152$, $p = .013$) of risk, when separated from the composite IRM, continue to represent independent predictors of cybercrime prevention while the treatment of risk does not ($\beta = .075$, $p = .189$). This study adds to the risk management literature by demonstrating the mechanisms through which risk management is able to produce security value through operational information intelligence, and has determined the treatment implementation gap as an important intervention opportunity for organisations wanting to maximise the security yield of risk management.

Third, there is a conditional context to the security contribution of IRM in that the coefficient for the direct contribution for the security of IRM declines when controlling for the regulatory context because a significant portion of the security value of IRM is realised through regulatory enforcement mechanisms. The findings from the moderating study provide evidence that when controlling for the regulatory environment, the coefficient for IRM transitions from a marginally significant predictor to the most significant predictor of the composite IRM (β: .108 → .402) supporting IRM as a capability in the regulatory environment that will produce the maximum amount of security value (through the three dimensions of digital risk management) for its implemented, treating risks.

Future research directions would include the use of longitudinal designs in order to better understand the direction of causation between investments in risk management

and improvements in security outcomes, and testing of the treatment implementation gap hypothesis using objective measures and objective data as opposed to self-reported responses as indicators of implementation of treatment plans for managing risks. Future researchers should carry out multi-national comparative studies of how variability in the regulatory context moderates the contribution of IRM to security in the telecommunications systems of developing economies.

References

1. Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. Journal of Marketing Research, 14(3), 396–402. https://doi.org/10.2307/3150783

2. Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & Management, 51(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

3. Cavelty, M. D., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

4. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

5. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101

6. Eugene, N. (2025a). Artificial intelligence strategy and digital literacy as predictors of cybercrime prevention in telecommunications: Evidence from an emerging market context. International Journal of Cybersecurity and Digital Governance.

7. Eugene, N. (2025b). Closing the boardroom cybersecurity gap: Digital governance and prevention outcomes in developing economy telecoms. International Journal of Cybersecurity and Digital Governance.

8. Eugene, N. (2025c). When regulation amplifies leadership: Moderating effects of the regulatory environment on digital security practices in telecoms. International Journal of Cybersecurity and Digital Governance.

9. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274

10. GSMA. (2022). The mobile economy: Sub-Saharan Africa 2022. GSM Association. https://www.gsma.com/mobileeconomy/sub-saharan-africa

11. Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis (8th ed.). Cengage Learning.

12. Hayes, A. F., & Cai, L. (2007). Using heteroscedasticity-consistent standard error estimators in OLS regression. Behavior Research Methods, 39(4), 709–722. https://doi.org/10.3758/BF03192961

13. Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

14. International Organization for Standardization. (2018). ISO 31000:2018 — Risk management: Guidelines. ISO.

15. International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection: Information security management systems. ISO.

16. International Organization for Standardization. (2022). ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection: Guidance on managing information security risks. ISO.

17. International Telecommunication Union. (2023). Measuring digital development: Facts and figures 2023. ITU Publications. https://www.itu.int

18. Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. American Journal of Sociology, 83(2), 340–363. https://doi.org/10.1086/226550

19. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, Version 1.1. NIST. https://doi.org/10.6028/NIST.CSWP.04162018

20. Nunnally, J. C., & Bernstein, I. H. (1994). Psychometric theory (3rd ed.). McGraw-Hill.

21. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

22. Westerman, G., & Hunter, R. (2007). IT risk: Turning business threats into competitive advantage. Harvard Business School Press.

23. Yamane, T. (1967). Statistics: An introductory analysis (2nd ed.). Harper & Row.