

Security Culture and Its Boundary Conditions Explain Effective and Accountable Information Security Management in Vietnam

Hieu Trung Tran

Van Lang University

Nguyen Trong Gia Nguyen

RMIT Vietnam

Khanh Ngoc Phuong Nguyen

RMIT Vietnam

Bao Nguyen Nhat Dang

Ton Duc Thang University

Linh Thi Hai Tran

RMIT Vietnam

Long Nguyen Phi Duong

RMIT Vietnam

Cuong Hong Le

Ton Duc Thang University

Uyen Le Tu Pham

22265427@student.westernsydney.edu.au

Western Sydney University

Research Article

Keywords: information security management effectiveness, security culture and competency, resource-based view, institutional theory, fuzzy-set qualitative comparative analysis (fsQCA), sustainable development goals

Posted Date: October 13th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10788833/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Security breaches continue to expose organizations in complex, digitally integrated supply chains, even where information security is treated as a compliance checklist. Effective information security management includes organizational governance and safety in socio-technical systems. Resource-based and institutional antecedents of information security management effectiveness (ISME) have been studied separately, leaving it unclear how internal resources, leadership commitment, and external pressure affect security outcomes. This study investigates whether security culture and competency (SCC) functions as the capability-conversion mechanism linking resource capability (RC), top management commitment (TMC), and external institutional pressure (EIP) to ISME and whether organizational maturity affects this mechanism. Survey data from 358 Vietnamese organizations were analyzed using covariance-based structural equation modeling in AMOS with maximum likelihood estimation. An interaction term tested the moderating role of institutional pressure; bootstrapping with 5,000 resamples verified robustness; Chow tests and multi-group analysis examined heterogeneity across security-team size and organizational tenure; and fuzzy-set qualitative comparative analysis identified configurational paths to firm competitiveness. Top management commitment and external institutional pressure significantly strengthened security culture and competency, which in turn strongly predicted security management effectiveness. Resource capability influenced effectiveness directly rather than through security culture, and the security-culture-by-pressure interaction was not significant. Structural relationships differed significantly across security-team size and organizational tenure, and several equally valid configurations led to high competitiveness. This study provides a contingency-aware account of how organizations build effective and competitive information security management by integrating resource-based and institutional perspectives on security culture as a capability-conversion mechanism and using symmetric structural modeling and asymmetric configurational analysis. These findings are relevant for organizations which cannot improve security capability by budgets alone considering that security culture is predominantly influenced by leadership and institutional pressures rather than resource availability. They also contribute to the achievement of SDG target 16.6 on effective and accountable institutions and SDG target 9.1 on reliable and resilient infrastructure, with a further link to productivity under SDG target 8.2.

1. Introduction

1.1 Background and Research Context: Cybersecurity as an Organizational Capability Challenge

Digital transformation has embedded organizations of every size within interconnected networks of suppliers, customers, and regulators, expanding the attack surface for cyber incidents well beyond the boundaries of a single firm [1, 2, 60]. As supply chains digitize procurement, logistics, and production data, information security is no longer a purely technical concern confined to an IT department; it has become an organizational capability that shapes operational continuity, regulatory standing, and

competitive positioning [3, 4]. Firms operating in emerging markets, where regulatory frameworks and security maturity vary considerably across sectors, face a particularly acute version of this challenge [5].

Much of the practitioner and academic conversation about information security has historically emphasized technical controls and compliance checklists, firewalls, access control, and certification against standards such as ISO/IEC 27001 [6]. While necessary, a compliance-centered view treats security as a static state to be certified rather than a capability that organizations must continuously build, and it offers limited insight into why organizations with similar technical investments achieve markedly different security outcomes [7, 8]. From a sustainable-development perspective, these governance concerns extend beyond cybersecurity to the governance and resilience of increasingly digital organizational systems. They align most directly with SDG target 16.6 via effective and accountable institutions and with SDG target 9.1 through reliable and resilient digital operations, although corporate competitiveness establishes a tertiary association with SDG target 8.2.

1.2 Research Problem: From Compliance Checklists to Capability-Building

An emerging stream of research has instead conceptualized information security management effectiveness (ISME) as an organizational outcome shaped by internal resources and leadership behavior [9, 10]. Resource-based view (RBV) scholars argue that dedicated security expertise, budget, and infrastructure—resource capability (RC)—constitute a foundation for effective security management [11, 12]. Parallel research on managerial behavior emphasizes that top management commitment (TMC) signals strategic priority and secures the investment needed for security initiatives to succeed [13, 14].

However, these internal-resource explanations coexist with an institutional perspective, which holds that firms adopt security practices to conform to pressures from regulators, customers, and industry peers rather than purely from internal capability calculations [15, 16]. External institutional pressure (EIP), encompassing regulatory mandates, partner requirements, and industry norms, has been shown to drive security investment independently of internal resource availability [17, 18]. These two literatures—resource-based and institutional, have rarely been integrated within a single model, leaving open the question of how internally generated capability and externally imposed pressure jointly translate into effective security management.

1.3 Theoretical Gap: The Missing Mediating Role of Security Culture

A further limitation is that existing studies frequently treat ISME as a direct outcome of resources, leadership, or pressure, without specifying the organizational mechanism through which these antecedents are converted into effective practice. Security culture and competency (SCC), the shared values, skills, and behavioral norms that embed security into everyday organizational routines [19, 20], offers a plausible conversion mechanism, yet it has rarely been modeled as a mediator connecting resource-based and institutional antecedents to ISME within a single structural framework. Without this

mechanism, organizations and researchers cannot distinguish between security investments that merely exist on paper and those that are embedded into organizational behavior [21, 22].

1.4 The Dual Antecedents: Internal Resources, Leadership, and External Pressure

This study, therefore, proposes that RC, TMC, and EIP represent three distinct but complementary antecedents that must pass through SCC to shape ISME. RC provides the material and human capacity for security work; TMC provides the internal authority and prioritization that activates that capacity; and EIP provides the external legitimacy pressure that channels organizational attention toward security practice [23, 24]. Because organizations differ substantially in size, security-team maturity, and organizational age, this study further examines whether these relationships hold uniformly or vary across organizational contexts [25].

1.5 Research Objectives and Questions

This study aims to develop and test an integrated resource-based and institutional framework linking organizational antecedents to information security management effectiveness through the mediating role of security culture and competency. Read against the sustainable development agenda, the framework addresses the same concern as SDG target 16.6, the development of effective and accountable institutions, and SDG target 9.1, the reliability and resilience of the infrastructure on which economic activity now depends. Specifically, it addresses the following research questions:

RQ1: Do resource capability, top management commitment, and external institutional pressure influence information security management effectiveness through security culture and competency?

RQ2: Does external institutional pressure moderate the relationship between security culture and competency and information security management effectiveness?

RQ3: Do these structural relationships differ across organizations of different security-team size and organizational tenure?

RQ4: What configurations of resource capability, top management commitment, external institutional pressure, and security culture lead to high versus low firm competitiveness?

1.6 Theoretical and Practical Contributions

This study makes three contributions. First, it integrates resource-based and institutional theory within a single structural model of information security management, rather than treating them as competing explanations. Second, it identifies security culture and competency as the capability-conversion mechanism that transforms resources, leadership commitment, and institutional pressure into measurable security effectiveness. Third, by combining covariance-based structural equation modeling with configurational fsQCA, this study demonstrates that effective security management can be achieved through multiple, equally valid organizational configurations rather than a single universal

formula [26, 27]. Practically, the findings offer managers and policymakers a differentiated roadmap: organizations should not assume that resource investment alone yields security effectiveness, nor that regulatory compliance is sufficient without internal culture-building.

1.7 Structure of the Paper

The remainder of this paper proceeds as follows. Section 2 reviews the theoretical foundations of resource-based and institutional explanations of information security management. Section 3 develops the hypotheses and conceptual model. Section 4 describes the methodology. Followed by empirical results in Section 5. The findings will be discussed within section 6 before presenting conclusions, contributions, and limitations in Section 7.

2. Literature Review and Theoretical Background

2.1 Information Security Management Effectiveness as an Organizational Outcome

Information security management effectiveness (ISME) is defined as the extent to which security practice in an organization mitigates risk, reduces losses and creates business value through secure operations [28, 29]. Early information systems security research treated effectiveness largely as a function of technical control implementation [30]. More recent work has reframed ISME as a socio-organizational outcome shaped jointly by resources, governance, and culture, reflecting the recognition that technology alone cannot resolve security risk without organizational commitment and behavioral change [5, 8]. This reframing motivates the present study's focus on organizational antecedents rather than purely technical determinants of effectiveness.

2.2 Resource-Based View and Resource Capability

The resource-based view (RBV) argues that heterogeneous, valuable, and difficult-to-imitate resources are a primary source of sustained advantage and superior performance [11, 31]. Applied to information technology and security, RBV scholars have shown that IT and security-specific resources, skilled personnel, dedicated budgets, and infrastructure, constitute a resource capability (RC) that enables effective risk management [12, 32]. Dynamic capabilities extend this argument by emphasizing that resources must be continuously reconfigured to remain effective under changing threat conditions [33, 34]. However, resource-based explanations alone have been criticized for underspecifying the organizational processes through which resources are converted into outcomes [35], which is precisely the gap this study addresses by positioning security culture as the conversion mechanism.

2.3 Institutional Theory and External Institutional Pressure

The institutional perspective offers a robust link between information security management and the governance agenda of sustainable development. SDG target 16.6 highlights the importance of effective, accountable, and transparent institutions. In this vein, coercive, mimetic, and normative pressures

explain the way in which these institutional expectations influence individual organisations. Recent studies in this journal have also explored this connection from two directions, one mapping the cybersecurity research base in internal auditing [61] and one examining digital transformation risk in logistics and supply chains [60]. Institutional theory suggests that organizations adopt practices to gain legitimacy in the institutional environment, often without regard to the technical efficiency of the practices [15, 36]. External institutional pressure (EIP) [37, 38] is jointly defined as coercive pressure from regulators, mimetic pressure from industry peers, and normative pressure from professional standards. EIP has been shown to drive investments in security and the adoption of policies based on customer demands, supplier requirements, and government regulations regarding information security [16, 39]. Prior studies have proved that institutional pressure acts as a complement, not a substitute, to internal resource-based mechanisms, which motivates the integrated framework proposed in this paper [13, 17].

2.4 Top Management Commitment as an Internal Governance Mechanism

Top management commitment (TMC) reflects the extent to which organizational leadership prioritizes security, allocates resources, and monitors security performance [14]. TMC has consistently been identified as a critical antecedent of both security policy compliance and security culture, because leadership behavior signals organizational priorities to employees and shapes resource allocation decisions [9, 10, 40]. If there is no visible leadership commitment, security initiatives risk will be treated as a peripheral IT function rather than a core organizational priority [41].

2.5 Security Culture and Competency as a Capability-Conversion Mechanism

Security culture and competency (SCC) captures the shared assumptions, values, skills, and behavioral norms that embed security considerations into everyday organizational routines [19]. Unlike formal policy, which specifies what employees should do, security culture reflects what employees actually value and practice [20, 21]. Prior research demonstrates that security culture mediates the relationship between organizational antecedents, such as training, awareness programs, and governance structures, and behavioral or effectiveness outcomes [22, 42, 61]. This study extends that logic by testing SCC as the mediating mechanism between RC, TMC, EIP, and ISME within a single integrated model, addressing calls for research that connects resource-based and institutional antecedents through an intervening organizational-capability variable [43, 44].

2.6 Boundary Conditions: Organizational Size, Tenure, and Configurational Complexity

Because the strength of resource-based and institutional mechanisms is likely to vary with organizational maturity, this study also examines security-team size and organizational tenure as boundary conditions, following measurement-invariance and multi-group analysis (MGA) procedures established in prior cross-group comparative research [25]. In addition, because covariance-based

methods such as structural equation modeling assume symmetric, additive relationships, this study complements the SEM analysis with fuzzy-set qualitative comparative analysis (fsQCA), which captures equifinal, conjunctural, and asymmetric configurations of antecedents leading to firm competitiveness [26, 27, 45]. This combination follows recent methodological guidance recommending the pairing of symmetric and configurational analyses in information systems research [46].

3. Research Framework and Hypotheses Development

3.1 Resource Capability and Security Culture and Competency

Resource capability (RC) reflects the availability of skilled information security personnel, dedicated financial resources, and adequate IT infrastructure for security work [12, 32]. Under the viewpoint of RBV, organizations that possess greater security-specific resources should be better positioned to cultivate a strong security culture, because trained personnel and adequate infrastructure provide the practical means to embed security values into daily routines [9]. Therefore, the resource capability should directly reflect on the cultural and competency dimension of the organization's security posture, laying the foundation for a more robust and consistent set of behavioral norms.

H1: Resource capability positively influences security culture and competency.

3.2 Top Management Commitment and Security Culture and Competency

Top management commitment (TMC) captures leadership's strategic prioritization of security, visible policy sponsorship, and active monitoring of security performance [14]. Leadership behavior is a powerful signal that shapes what employees perceive as organizationally valued; when top management visibly commits to security, employees are more likely to internalize security as a shared value rather than a bureaucratic requirement [13, 40]. Because culture is fundamentally a socially transmitted set of values, TMC is expected to be one of its strongest internal drivers.

H2: Top management commitment positively influences security culture and competency.

3.3 External Institutional Pressure and Security Culture and Competency

External institutional pressures (EIP) [15, 16] exist as organizations feel compelled to show regulators, business partners, customers and industry norms legitimate security practice. Besides inspiring single compliance acts, persistent institutional pressure can gradually reshape organizational values and practices when firms internalize external expectations into daily routines, a process consistent with normative and mimetic isomorphism [37, 38]. Firms facing stronger external pressure should therefore develop a more robust security culture as they adapt to survive scrutiny from partners and regulators.

H3: External institutional pressure positively influences security culture and competency.

3.4 Security Culture and Competency and Information Security Management Effectiveness

Building on the capability-conversion logic outlined in Section 2.5, this study proposes that security culture and competency (SCC) is the proximal driver of information security management effectiveness (ISME). RC, TMC and EIP provide inputs, resources, leadership signals and external expectations. At the same time, SCC is the embedded organizational capability that transforms these inputs into actual security practices, including employee skills, incident-reporting behavior, cross-departmental coordination, and regulatory compliance [19, 22]. Organizations with a stronger security culture should therefore exhibit more effective technology implementation, risk reduction, and business value from security investment.

H4: Security culture and competency positively influences information security management effectiveness.

3.5 Resource Capability and Information Security Management Effectiveness

In addition to its indirect effect through SCC, resource capability may influence ISME directly. Adequate staffing, budget, and infrastructure can enable effective technology implementation and risk reduction independently of cultural embedding, for example, mature security tooling and incident-response infrastructure can reduce losses even before broader cultural change takes hold [12, 32]. This direct path recognizes that some effectiveness gains are realized through the immediate operational deployment of resources rather than through their cultural conversion.

H5: Resource capability positively influences information security management effectiveness.

3.6 Top Management Commitment and Information Security Management Effectiveness

Top management commitment may also influence ISME directly, insofar as leadership decisions, approving security budgets, mandating specific controls, and monitoring outcomes, translate into effectiveness without requiring a fully developed security culture as an intermediate step [10, 14]. This direct path is included to test whether leadership commitment matters beyond its role in shaping culture.

H6: Top management commitment positively influences information security management effectiveness.

3.7 External Institutional Pressure and Information Security Management Effectiveness

Similarly, external institutional pressure may directly shape ISME through compliance-driven adoption of specific controls, audits, and certifications mandated by regulators or partners, independent of whether such pressure has yet been internalized into organizational culture [16, 24]. This direct path captures the compliance-oriented, rather than culture-mediated, channel through which institutional pressure can shape effectiveness.

H7: External institutional pressure positively influences information security management effectiveness.

3.8 The Moderating Role of External Institutional Pressure

Finally, this study examines whether the strength of the SCC–ISME relationship depends on the level of external institutional pressure. Two competing logics are plausible. On one hand, institutional pressure could amplify the effectiveness-generating power of security culture by aligning external legitimacy demands with internal cultural capability, so that culturally strong organizations facing high pressure translate culture into effectiveness particularly efficiently. On the other hand, when institutional pressure is high, organizations may respond with compliance-driven, checklist-oriented behaviors that partially substitute for organically developed culture, weakening the incremental contribution of SCC to ISME [37, 39]. Because both directions are theoretically defensible, this study tests the interaction without a directional prediction.

H8: External institutional pressure moderates the relationship between security culture and competency and information security management effectiveness.

Figure 1 depicts the proposed conceptual model: RC, TMC, and EIP are modeled as antecedents of SCC (H1–H3) and as antecedents of ISME through both indirect (via SCC, H4) and direct paths (H5–H7); the $SCC \times EIP$ interaction term is modeled as a moderator of the SCC–ISME path (H8). This structure allows the model to simultaneously test capability-conversion (mediation) and compliance-driven (direct-effect and moderation) logics within a single framework, consistent with the sample-based analytical structure used in comparable structural equation modeling studies of consumer and organizational behavior [47, 48].

4. Research Methodology

4.1 Research Design and Data Collection

This study adopted a quantitative, survey-based research design to test the hypothesized relationships among resource capability, top management commitment, external institutional pressure, security culture and competency, and information security management effectiveness. A survey design was appropriate because the constructs of interest, perceived resource adequacy, leadership commitment, institutional pressure, cultural embedding, and effectiveness, are best captured through the perceptions of managers and employees directly involved in organizational security practice [10].

The research context is organizational information security management in Vietnam, a rapidly digitizing emerging market where firms face uneven regulatory maturity and heterogeneous security investment across sectors [5]. Respondents were required to hold managerial or security-relevant roles, or otherwise possess direct familiarity with their organization's information security practices, to ensure that responses reflected informed organizational assessments rather than uninformed impressions.

A structured questionnaire was distributed to managers and employees across organizations varying in size, ownership structure, sector, and security-team maturity. The final valid sample comprised 358 organizations. Consistent with the sampling approach common in organizational survey research, a purposive/convenience sampling strategy targeted respondents with verifiable security-related responsibilities [49]. The questionnaire included two sections: the first captured organizational demographic characteristics (size, revenue, sector, ownership, security-team size, organizational tenure, and framework adoption); the second measured the theoretical constructs using multi-item scales adapted from established literature. All items were assessed on a seven-point Likert scale ranging from 1 ("strongly disagree") to 7 ("strongly agree"), consistent with common practice in organizational behavior and information systems research [48].

4.2 Measurement Development

Resource Capability (RC) was measured using five items capturing the availability of information security experts, financial resources, IT infrastructure, and the effective use of advanced IT tools for security purposes, adapted from RBV-based IT capability research [12, 32].

Top Management Commitment (TMC) was measured by using seven items which reflects the strategic importance placed on information security, policy development, management responsibility, direct involvement, investment support, forward-looking vision, and performance monitoring [14].

Security Culture and Competency (SCC) was measured using seven items capturing employee security skills, training, incident sharing and reporting, employee contribution to improvement, cross-departmental coordination, regulatory compliance, and organizational commitment to security [19, 20].

External Institutional Pressure (EIP) was measured using ten items reflecting pressure from suppliers and business partners, industry-wide practices, customer requirements, government regulation, and participation in government security programs [15, 16].

Information Security Management Effectiveness (ISME) was measured using eight items capturing technology, policy, and planning implementation, reduction of security losses and risks, and the business value, profitability, and competitive advantage generated through secure operations [28, 29].

4.3 Pilot Study and Data Screening

A pilot test was conducted with a small sample of security and IT managers to assess item clarity and contextual relevance prior to full-scale distribution. Following the main data collection, responses were screened for completeness, straight-lining, and inconsistent answering patterns; incomplete or low-

quality responses were excluded before analysis, yielding the final sample of 358 valid organizational responses.

4.4 Common Method Bias Assessment

Because all constructs were measured through a single questionnaire administered to the same respondents, common method bias (CMB) was a relevant concern [50]. Procedural remedies included assuring respondent anonymity, separating predictor and criterion items within the questionnaire, and using neutral, non-leading item wording. Discriminant validity was established through the heterotrait-monotrait ratio reported in Section 5.2. Discriminant validity speaks to the distinctness of the constructs rather than to shared method variance, so the procedural remedies above carry the weight of the assessment here, and the possibility of common method bias cannot be excluded.

4.5 Data Analysis Procedure

Data were analyzed using a multi-stage covariance-based structural equation modeling (CB-SEM) approach in AMOS with maximum likelihood (ML) estimation, following the analytical logic recommended for theory-testing structural models [47, 51].

First, the measurement model was assessed through confirmatory factor analysis (CFA). Internal consistency reliability was evaluated using Cronbach's alpha and composite reliability (CR), computed from standardized factor loadings following Bagozzi and Yi [52]; convergent validity was assessed via standardized factor loadings and average variance extracted (AVE); discriminant validity was examined using the heterotrait-monotrait ratio (HTMT) criterion [53, 54].

Second, the structural model was estimated to test the hypothesized paths (H1–H7), with model fit evaluated using the chi-square/degrees-of-freedom ratio (CMIN/df), comparative fit index (CFI), and Tucker-Lewis index (TLI) [55].

Third, the moderating effect of external institutional pressure on the SCC–ISME relationship (H8) was tested by incorporating an $SCC \times EIP$ interaction term into the structural model.

Fourth, mediation was assessed using the variance accounted for (VAF) approach, and robustness of all structural paths was verified through bootstrapping with 5,000 resamples and bias-corrected 95% confidence intervals [56].

Fifth, prior to multi-group comparison, measurement invariance (configural and metric) was established, followed by structural invariance testing [25]. Organizations were then split into two grouping schemes, security-team size (small, fewer than five members, versus medium-to-large, five or more) and organizational tenure (younger, ten years or less, versus mature, more than ten years), and multi-group analysis (MGA) compared structural paths across groups. Chow tests were additionally conducted to formally test whether regression coefficients differed significantly between groups for the SCC and ISME structural equations [57].

Finally, fuzzy-set qualitative comparative analysis (fsQCA) was conducted as a complementary configurational analysis, calibrating RC, TMC, EIP, and SCC as fuzzy-set conditions and firm competitiveness as the configurational outcome. Following standard fsQCA procedures, truth tables were constructed with a frequency cutoff of three cases and a consistency cutoff of 0.85, and both high- and low-outcome configurations were analyzed using the intermediate solution [26, 45, 58, 59]. Because fsQCA identifies equifinal and conjunctural configurations rather than net effects, it complements the linear, additive assumptions of CB-SEM by revealing whether multiple, qualitatively distinct combinations of antecedents can equally produce high firm competitiveness [27, 46].

5. Results

5.1 Sample Characteristics

Table 1 presents the organizational profile of the 358 valid responses. Organizations were predominantly small to mid-sized (41.6% with 1–49 employees; 29.9% with 50–249 employees), and 64.2% reported an information security team of fewer than five members. State-owned organizations represented the largest ownership category (62.6%), and the construction and real estate sector was the most represented industry (32.7%), followed by information technology and telecommunications (19.8%). Regarding organizational age, 29.6% of firms had operated for more than 20 years, while 16.2% were younger than five years. Only 20.4% of organizations reported ISO/IEC 27001 adoption, and 22.3% reported no formal information security framework.

Table 1
Organizational Characteristics of Respondents (N = 358)

Variable	Category	Frequency	Percentage (%)
Organization size	1–49 employees	149	41.6
	50–249 employees	107	29.9
	250–999 employees	58	16.2
Information security team size	< 5	230	64.2
	5–10	65	18.2
	11–20	31	8.7
	21–50	17	4.7
	50	15	4.2
Annual business revenue	< 3 billion	47	13.1
	3–50 billion	143	39.9
	50–300 billion	40	11.2
	300 billion	43	12.0
	Don't know	85	23.7
Organizational age	< 5 years	58	16.2
	5–10 years	93	26.0
	11–20 years	101	28.2
	20 years	106	29.6
Ownership structure	State-owned	224	62.6
	Private	41	11.5
	Foreign-owned	31	8.7
	Mixed	62	17.3
Managerial position	No	140	39.1
	Yes	218	60.9
Tenure	< 1 year	49	13.7
	1–5 years	156	43.6
	6–10 years	58	16.2

Variable	Category	Frequency	Percentage (%)
	10 years	95	26.5
Region	Southern Vietnam	207	57.8
	Central Vietnam	29	8.1
	Northern Vietnam	122	34.1
Industry sector	Information Technology and Telecommunications	71	19.8
	Finance and Banking	17	4.7
	Manufacturing and Industrial	34	9.5
	Retail and Consumer Goods	17	4.7
	Healthcare and Pharmaceuticals	19	5.3
	Construction and Real Estate	117	32.7
	Education and Training	45	12.6
	Other	38	10.6
Information security framework adoption	ISO/IEC 27001	73	20.4
	ISO/IEC 27017 (Cloud Security)	64	17.9
	ISO/IEC 27018 (Cloud Privacy)	47	13.1
	PCI DSS	44	12.3
	NIST CSF	41	11.5
	COBIT	31	8.7
	ITIL	43	12.0
	No framework adopted	80	22.3
	Unknown	181	50.6
	Other	2	0.6
Business type	B2B (Business to Business)	193	53.9
	B2C (Business to Consumer)	158	44.1
	C2C (Consumer to Consumer)	38	10.6
	B2G (Business to Government)	46	12.8
	Other_type	25	7.0

5.2 Measurement Model Assessment

The measurement model was assessed through exploratory and confirmatory factor analysis, internal consistency reliability, convergent validity, and discriminant validity. As shown in Table 2, Cronbach's alpha values ranged from .915 (RC) to .947 (TMC), and composite reliability (CR) ranged from .913 to .943, indicating strong internal consistency across all five constructs. Average variance extracted (AVE) values ranged from .572 (EIP) to .700 (TMC), all exceeding the .50 threshold and confirming satisfactory convergent validity [54]. Standardized CFA factor loadings ranged from .671 to .886 across constructs, indicating that all indicators strongly represented their intended latent variables.

Table 2
Measurement Model Summary

Construct	Cronbach's α	Composite Reliability (CR)	Average Variance Extracted (AVE)
Resource Capability (RC)	.915	.913	.679
Top Management Commitment (TMC)	.947	.943	.700
Security Culture and Competency (SCC)	.929	.916	.611
External Institutional Pressure (EIP)	.938	.930	.572
Information Security Management Effectiveness (ISME)	.944	.931	.630

Discriminant validity was assessed using the heterotrait–monotrait ratio (HTMT). As shown in Table 3, all HTMT values were below the conservative threshold of .85 [53], with the highest value observed between SCC and ISME (HTMT = .799), followed by RC and TMC (HTMT = .872, marginally above the more conservative .85 cutoff but below the liberal .90 threshold often applied in organizational-level survey research). Overall, the measurement model demonstrated satisfactory reliability, convergent validity, and discriminant validity, supporting the subsequent structural model assessment.

Table 3
Discriminant Validity Results (HTMT Criterion)

Construct	RC	TMC	SCC	EIP	ISME
RC	–				
TMC	.872	–			
SCC	.676	.714	–		
EIP	.667	.654	.794	–	
ISME	.675	.707	.799	.780	–

5.3 Structural Model Assessment

The structural model was estimated using CB-SEM with ML estimation. Overall model fit was acceptable (CMIN/df = 2.568, CFI = .919, TLI = .911), confirming that the proposed structural model adequately represented the observed data [55].

As reported in Table 4, TMC had a significant positive effect on SCC ($\beta = .386$, $p < .001$), supporting H2, and EIP had a strong positive effect on SCC ($\beta = .587$, $p < .001$), supporting H3. In contrast, RC did not significantly predict SCC ($\beta = -.071$, $p = .438$), so H1 was not supported. SCC significantly predicted ISME ($\beta = .393$, $p < .001$), supporting H4 and confirming the central capability-conversion mechanism proposed in this study.

Regarding direct effects on ISME, RC had a significant positive effect ($\beta = .236$, $p = .008$), supporting H5, and EIP had a significant positive effect ($\beta = .260$, $p < .001$), supporting H7. However, TMC did not significantly predict ISME directly ($\beta = .052$, $p = .562$), so H6 was not supported. The SCC $\times$ EIP interaction term showed a negative and non-significant effect on ISME ($\beta = -.061$, $p = .065$), so H8 is not supported.

The model explained 69.5% of the variance in SCC ($R^2 = .695$) and 73.3% of the variance in ISME ($R^2 = .733$), indicating strong explanatory power.

Table 4
Structural Model Results and Model Fit Indices

Hypothesis	Path	Standardized β	p-value	Result
H1	RC $\rightarrow$ SCC	– .071	.438	Not supported
H2	TMC $\rightarrow$ SCC	.386	< .001	Supported
H3	EIP $\rightarrow$ SCC	.587	< .001	Supported
H4	SCC $\rightarrow$ ISME	.393	< .001	Supported
H5	RC $\rightarrow$ ISME	.236	.008	Supported
H6	TMC $\rightarrow$ ISME	.052	.562	Not supported
H7	EIP $\rightarrow$ ISME	.260	< .001	Supported
H8	SCC $\times$ EIP $\rightarrow$ ISME	– .061	.065	Not supported (marginal)
R ² (SCC)	.695			
R ² (ISME)	.733			
Model fit: CMIN/df = 2.568; CFI = .919; TLI = .911				

5.4 Moderation Analysis

Moderation analysis was conducted to test H8, which proposed that external institutional pressure (EIP) moderates the relationship between security culture and competency (SCC) and information security management effectiveness (ISME). The interaction term (SCC $\times$ EIP) was entered into the structural model alongside the main effects of SCC and EIP on ISME, following standard latent-interaction procedures in CB-SEM [51].

As reported in Table 5, the SCC $\times$ EIP interaction on ISME was negative and not significant (β = – .061, SE-implied p = .065), falling short of the conventional .05 threshold. H8 is therefore not supported. The main effects of both SCC (β = .393, p < .001) and EIP (β = .260, p < .001) on ISME are individually strong and positive, and the interaction estimate is negative and close to zero, so the data give no evidence that either condition amplifies the other. Whether the two operate as mild substitutes at high levels, as the negative sign would suggest, cannot be settled at this significance level and is taken up in Section 6.4.

Table 5
Moderation Analysis Results (H8: SCC × EIP → ISME)

Term	Standardized β	p-value	95% Bootstrap CI	Conclusion
SCC (main effect) → ISME	.393	< .001	not applicable (see Table 7)	Significant
EIP (main effect) → ISME	.260	< .001	not applicable (see Table 7)	Significant
SCC × EIP (interaction) → ISME	– .061	.065	not applicable (see Table 7)	Marginal, not supported at $p < .05$

Figure 2 presents a response-surface ("rocky") plot built directly from the respondent-level dataset (N = 358): each observed ISME composite score is plotted against that respondent's standardized EIP and SCC values, and the surface is generated by linear interpolation across this empirical point cloud (with the original 358 observations overlaid as scatter points for transparency), rather than from the fitted SEM coefficients alone. The irregular, multi-peaked terrain therefore reflects genuine between-respondent variability in ISME at similar EIP/SCC combinations – measurement noise, unmodeled covariates, and individual differences that a smooth model-implied plane would otherwise conceal. Despite this raw irregularity, the broad gradient of the surface is consistent with the SEM results: ISME is visibly lowest in the low-EIP/low-SCC region and highest where both predictors are elevated, and a supplementary OLS check on the observed composites ($ISME \sim EIP + SCC + EIP \times SCC$) corroborates the same directional pattern reported in Table 5 (EIP $\beta = .395$, SCC $\beta = .451$, interaction $\beta = -.028$, ns; $R^2 = .637$), reinforcing that the near-zero interaction in H8 is not an artifact of aggregation. Section 6.4 discusses the theoretical implications of this near-substitution pattern in detail.

5.5 Mediation Analysis

Mediation was examined using the variance accounted for (VAF) approach [56]. As shown in Table 6, EIP influenced ISME partially through SCC (indirect effect = .231, VAF = 47.05%), and TMC influenced ISME only through SCC (indirect effect = .152, VAF = 74.88%), since the direct TMC path to ISME was not significant. In contrast, RC's relationship with ISME showed no meaningful mediation through SCC (VAF = 13.46%), consistent with RC's non-significant path to SCC; the relationship between RC and ISME is therefore best characterized as a direct effect rather than a culturally mediated one.

Table 6
Mediation Analysis Results

Relationship	Total Effect	Direct Effect	Indirect Effect	VAF (%)	Conclusion
EIP → SCC → ISME	.491	.260	.231	47.05	Partial mediation
TMC → SCC → ISME	.203	.052	.152	74.88	Partial mediation
RC → SCC → ISME	.208	.236	– .028	13.46	No mediation

5.6 Robustness Check

Bootstrap resampling (5,000 resamples, bias-corrected 95% CI) confirmed the structural results (Table 7). Paths from TMC → SCC, EIP → SCC, SCC → ISME, RC → ISME, and EIP → ISME were robust, with confidence intervals excluding zero. Paths from RC → SCC and TMC → ISME were not robust, consistent with their non-significant estimates in the main structural model. These same bootstrap intervals underpin the main-effect rows reported in Table 5's moderation summary.

Table 7
Bootstrap Robustness Assessment (5,000 resamples, bias-corrected 95% CI)

Path	β	95% CI	p-value	Result
RC → SCC	– .053	[–.211, .092]	.438	Not robust
TMC → SCC	.315	[.170, .469]	< .001	Robust
EIP → SCC	.621	[.431, .851]	< .001	Robust
SCC → ISME	.544	[.362, .774]	< .001	Robust
RC → ISME	.246	[.030, .490]	.008	Robust
TMC → ISME	.059	[–.214, .288]	.562	Not robust
EIP → ISME	.381	[.160, .620]	< .001	Robust

5.7 Measurement Invariance, Chow Test, and Multi-Group Analysis

Prior to multi-group comparison, measurement invariance was established for both grouping schemes. As shown in Table 8, metric invariance was supported for security-team size ($\Delta\chi^2 = 31.064$, $\Delta df = 32$, $p = .514$) and organizational tenure ($\Delta\chi^2 = 22.257$, $\Delta df = 32$, $p = .900$), and structural invariance was likewise supported for both groupings ($p = .008$ and $p = .002$, respectively, with $\Delta IFI \leq .003$ in all cases), confirming that cross-group comparisons are meaningful [25].

Table 8
Measurement and Structural Invariance Tests

Grouping Variable	Invariance Level	$\Delta\chi^2$	Δdf	p-value	ΔIFI	Decision
Security team size	Metric	31.064	32	.514	.002	Supported
Security team size	Structural	20.809	8	.008	.002	Supported
Organizational tenure	Metric	22.257	32	.900	.002	Supported
Organizational tenure	Structural	24.852	8	.002	.002	Supported

Chow tests formally confirmed group heterogeneity [57]: the SCC equation differed significantly across security-team size ($F = 3.310$, $df = 4,350$, $p = .011$) and organizational tenure ($F = 3.630$, $df = 4,350$, $p = .006$), and the ISME equation likewise differed significantly across both groupings ($F = 2.221$, $p = .041$; $F = 2.270$, $p = .037$, respectively), confirming that a single pooled model would misrepresent at least one subgroup's structural relationships.

Table 9
Chow Test Results

Model	Grouping	F-statistic	df1	df2	p-value	Conclusion
SCC = RC + TMC + EIP	Security team size	3.310	4	350	.011	Significant difference
ISME = RC+TMC + EIP+SCC + SCC×EIP	Security team size	2.221	6	346	.041	Significant difference
SCC = RC + TMC + EIP	Organizational tenure	3.630	4	350	.006	Significant difference
ISME = RC+TMC + EIP+SCC + SCC×EIP	Organizational tenure	2.270	6	346	.037	Significant difference

MGA results (Table 10) show that in organizations with small security teams (< 5 members), TMC strongly predicted SCC ($\beta = .489$, $p < .001$) and EIP strongly predicted ISME directly ($\beta = .385$, $p < .001$); in medium-to-large security teams (≥ 5 members), EIP became the dominant predictor of SCC ($\beta = .732$, $p < .001$), SCC's effect on ISME nearly doubled ($\beta = .636$ versus $\beta = .268$), and the SCC $\times$ EIP interaction turned significantly negative ($\beta = -.133$, $p = .030$). A parallel pattern emerged across organizational tenure: TMC significantly predicted SCC only in mature organizations ($\beta = .565$, $p < .001$, versus $\beta = .210$, $p = .079$ in younger firms), while EIP's effect on SCC was stronger among younger organizations ($\beta = .756$ versus $\beta = .443$).

Table 10
Multi-Group SEM Results

Hypothesis	Small Team (β/p)	Medium–Large Team (β/p)	Younger Org. (β/p)	Mature Org. (β/p)
RC → SCC	– .085 / .449	– .099 / .533	– .093 / .448	– .085 / .517
TMC → SCC	.489 / <.001	.285 / .071	.210 / .079	.565 / <.001
EIP → SCC	.465 / <.001	.732 / <.001	.756 / <.001	.443 / <.001
SCC → ISME	.268 / <.001	.636 / <.001	.321 / .002	.384 / <.001
RC → ISME	.203 / .043	.086 / .620	.143 / .176	.337 / .016
TMC → ISME	.132 / .213	.070 / .687	.165 / .100	– .023 / .879
EIP → ISME	.385 / <.001	.079 / .528	.354 / .001	.226 / .006
SCC × EIP → ISME	.027 / .517	– .133 / .030	– .144 / .003	– .003 / .953

5.8 Fuzzy-Set Qualitative Comparative Analysis (fsQCA)

Complementing the symmetric SEM findings, fsQCA identified five configurations of RC, TMC, EIP, and SCC associated with high firm competitiveness (Table 11; solution coverage = .891, solution consistency = .822). Two configurations—the Resource–Leadership Capability Path (RC present, TMC present) and the Resource–Institutional Capability Path (RC present, EIP present)—showed the highest raw coverage (.740 and .717, respectively), indicating that resource capability combined with either leadership commitment or institutional pressure is a particularly prevalent route to competitiveness. Notably, the Security Culture Compensation Path (SCC present, RC absent) demonstrates that a strong security culture can compensate for limited resource capability, consistent with the mediation results in Section 5.5.

Table 11
Configurational Paths to High Firm Competitiveness

Configuration	RC	TMC	EIP	SCC	Raw Coverage	Unique Coverage	Consistency
Leadership–Institutional Compensation		●	⊗		.447	.009	.843
Security Culture Compensation	⊗			●	.451	.028	.881
Institutional–Leadership Compensation		⊗	⊗		.457	.018	.870
Resource–Leadership Capability	●	●			.740	.013	.893
Resource–Institutional Capability	●		●		.717	.018	.923
Solution coverage = .891; Solution consistency = .822							

Four configurations were associated with low firm competitiveness (Table 12; solution coverage = .909, solution consistency = .815), and in every configuration, the simultaneous absence of at least two antecedents—most often EIP or SCC combined with RC or TMC—characterized weak-competitiveness firms, reinforcing the asymmetric, conjunctural insight that competitiveness erodes not from any single missing factor but from the joint absence of complementary capabilities and pressures.

Table 12
Configurational Paths to Low Firm Competitiveness

Configuration	RC	TMC	EIP	SCC	Raw Coverage	Unique Coverage	Consistency
Security Culture–Institutional Compensation			⊗	⊗	.790	.033	.883
Leadership–Security Culture Compensation		⊗		⊗	.779	.013	.886
Institutional–Resource Compensation	⊗		●		.761	.009	.891
Resource–Leadership Compensation	⊗	⊗			.782	.021	.867
Solution coverage = .909; Solution consistency = .815							

Note

● = presence of condition; ⊗ = absence of condition; blank = condition may be present or absent ("don't care"). Results are based on the intermediate solution; frequency cutoff = 3; consistency cutoff = .85.

Figure 3 translates Tables 11 and 12 into configurational roadmaps, tracing each combination of conditions through to its outcome. The high-competitiveness roadmap shows two resource-anchored routes (Resource–Leadership Capability and Resource–Institutional Capability, raw coverage .740 and .717) alongside three lower-coverage compensation routes in which an absent condition is offset by another present one—most notably the Security Culture Compensation path, where SCC substitutes for an absent RC. The low-competitiveness roadmap, by contrast, shows every route requiring the joint absence of at least two conditions, visually reinforcing that weak competitiveness is a conjunctural failure rather than a single missing ingredient.

6. Discussion

This study set out to explain how internal resources, leadership commitment, and external institutional pressure shape information security management effectiveness (ISME), and whether security culture and competency (SCC) serves as the mechanism converting these antecedents into effective practice. The findings reveal a more differentiated picture than a simple "more resources, more effectiveness" narrative: institutional and leadership forces build culture, resources act more directly, and the relative importance of each mechanism shifts with organizational maturity.

6.1 Institutional Pressure and Leadership, Not Raw Resources, Build Security Culture

The most striking structural finding is that resource capability did not significantly predict security culture (H1 not supported), while top management commitment and external institutional pressure both did (H2 and H3 supported, with EIP the stronger driver, $\beta = .587$). This extends institutional theory into the security-culture domain by showing that culture is fundamentally a socially and externally shaped phenomenon rather than a byproduct of budget or headcount [15, 16]. Consistent with normative and mimetic isomorphism, organizations appear to internalize security values in response to partner requirements, customer expectations, and regulatory scrutiny more readily than in response to simply having more security staff or infrastructure [37]. This finding qualifies RBV-based accounts of security management: resources matter, but they do not by themselves cultivate the shared values and behavioral norms that constitute culture [19].

6.2 Security Culture as the Capability-Conversion Bridge

SCC emerged as a strong, significant predictor of ISME (H4 supported, $\beta = .393$) and transmitted the whole of the TMC effect (74.88% VAF) and part of the EIP effect (47.05% VAF). This confirms the central theoretical proposition that culture functions as the conversion mechanism through which leadership commitment and institutional pressure become embedded, effectiveness-generating practice, rather than remaining abstract managerial intentions or compliance gestures [21, 22]. Leadership commitment,

in particular, had almost no direct effect on ISME (H6 not supported) but a strong indirect effect through SCC—top managers cannot simply mandate effectiveness; their commitment must first translate into a lived security culture before performance gains materialize, echoing prior evidence that culture and awareness programs mediate the link between governance-level antecedents and security-behavioral outcomes [22, 42]. This pattern has implications for governance beyond information security. SDG target 16.6 highlights both effectiveness and accountability, and these findings show that the two do not always develop together. Senior management's stated commitment alone did not lead to better security outcomes; improvements were associated only when this commitment was translated into everyday organisational practices. Therefore, accountability that remains limited to formal authority may not be sufficient to achieve the effectiveness required by SDG target 16.6.

6.3 Resource Capability's Direct, Culture-Independent Path

In contrast to TMC and EIP, RC influenced ISME directly (H5 supported, $\beta = .236$) with no meaningful mediation through SCC (VAF = 13.46%). This suggests that some resource-driven effectiveness gains—for example, deploying adequate infrastructure or specialized personnel to execute technical controls—are realized operationally, independent of whether a broader cultural shift has occurred [12, 32]. Practically, this means resource investment still pays off, but through a narrower, more mechanical channel than leadership- or pressure-driven culture-building. The direct relationship between resource capability and effectiveness indicates that material investment still plays a key role. Under SDG target 9.1, sustainable infrastructure is expected to be reliable and resilient, rather than simply large in scale. And, the findings also support this perspective. Human, financial, and technical resources contributed to better outcomes even there is not having any changes in organisational culture. This suggests that dependable digital operations can be achieved through two distinct pathways rather than relying on cultural change alone.

6.4 Institutional Pressure as a Weak and Possibly Counterproductive Moderator

The SCC $\times$ EIP interaction on ISME was only marginally significant and negative ($\beta = -.061$, $p = .065$), offering, at best, weak support for H8. The coefficient is negative rather than positive, which runs against the amplification logic set out in Section 3.8, but an estimate of this size at this p-value cannot carry a directional interpretation. Two readings therefore remain open, and the present data do not separate them. Institutional pressure may add little once security culture is already well developed, or heavy external scrutiny may push organizations toward compliance-oriented routines that sit alongside an organically developed culture rather than reinforcing it [39]. Testing the second reading calls for a design that measures compliance behaviour separately from cultural strength, which the present cross-sectional survey does not do.

6.5 Organizational Maturity as a Genuine Boundary Condition

The Chow tests and MGA results demonstrate that the model is not a "one-size-fits-all" account. In organizations with small security teams, TMC was the dominant lever for building SCC; in medium-to-large teams, EIP dominated and SCC's effect on ISME nearly doubled, while the SCC × EIP interaction turned significantly negative, suggesting that once teams reach sufficient scale, institutional pressure and culture begin to substitute rather than reinforce one another. A similar maturation pattern appeared across organizational tenure: TMC mattered only in mature firms, while EIP was the stronger cultural driver in younger organizations, plausibly because younger firms lack the internal legitimacy and established leadership routines that older organizations have accumulated [25]. These findings extend RBV and institutional theory by showing that the relative weight of internal versus external mechanisms is itself a function of organizational life-stage and team maturity, not a fixed structural constant.

6.6 Equifinality: Multiple Configurational Routes to Competitiveness

The fsQCA results complement and extend the SEM findings by revealing that high firm competitiveness can be achieved through at least five distinct configurations, not a single optimal path [26, 45]. Notably, the Security Culture Compensation Path shows that strong SCC can offset weak RC, empirically corroborating the mediation finding that culture, not raw resources, is the more consequential lever. Conversely, the low-competitiveness configurations each involve the joint absence of at least two complementary antecedents, indicating that competitiveness erosion is conjunctural rather than attributable to any single missing ingredient [27]. Together, the symmetric SEM and asymmetric fsQCA results paint a coherent, mutually reinforcing picture: culture is the mechanism, but organizations can arrive at effective, competitive security postures via more than one legitimate combination of resources, leadership, and institutional pressure [46]. A more specific implication can be drawn from the configurational findings. SDG target 8.2 identifies technological upgrading as an important pathway to higher productivity. The compensation pattern suggests that this upgrading involves organisational changes as well as technological improvements. In one of the five configurations linked to high competitiveness, a strong security culture was able to compensate for limited resource capability. However, this relationship should be viewed as secondary because competitiveness in this study is measured through perceptions rather than actual economic performance.

7. Conclusion

This study examined how resource capability, top management commitment, and external institutional pressure shape information security management effectiveness, and whether security culture and competency mediates these relationships. The findings show that leadership commitment and institutional pressure, not raw resources, are the primary forces that build security culture, and that culture, in turn, is the strongest predictor of effectiveness. Resource capability instead operates through a separate, direct, culture-independent path. These relationships are not organizationally uniform: Chow tests and multi-group analysis confirm that security-team size and organizational tenure reshape which mechanisms dominate, and fsQCA shows that multiple configurations of these antecedents can equally

produce high firm competitiveness. Overall, effective information security management is best understood not as a compliance outcome purchased with budget, but as a culturally embedded, contingently configured organizational capability. These findings also extend the relevance of information security management to sustainable development by highlighting its governance, continuity, and competitiveness implications, aligning most closely with the concerns of SDG targets 16.6, 9.1, and 8.2.

7.1 Contributions

This study offers three theoretical contributions. First, it integrates the resource-based view and institutional theory within a single structural model of information security management, moving beyond the tendency of prior research to examine internal resources [12, 32] and external institutional pressure [15, 16] as separate explanatory traditions. By jointly estimating RC, TMC, and EIP as antecedents within one model, this study clarifies their relative and complementary contributions, showing, notably, that institutional and leadership mechanisms dominate culture formation while resources operate more independently.

Second, this study identifies security culture and competency as the capability-conversion mechanism that transforms leadership commitment and institutional pressure into measurable effectiveness. Prior security research has often treated culture as an outcome in its own right [19, 20] or as a background contextual factor; this study instead positions SCC as a formal structural mediator with quantified variance-accounted-for contributions (74.88% for TMC, 47.05% for EIP), providing a more precise account of how "soft" managerial and institutional forces become "hard" organizational performance.

Third, by pairing CB-SEM with fsQCA, this study demonstrates empirically that information security effectiveness and firm competitiveness can be achieved through multiple, equifinal configurations of antecedents rather than a single universally optimal formula, extending recent methodological calls to combine symmetric and configurational analysis in information systems research [26, 27, 46]. This configurational insight has direct managerial value: it indicates that organizations lacking one antecedent (for example, limited resources) can still achieve competitiveness by compensating through another (for example, strong security culture), rather than concluding that security effectiveness is unattainable without uniformly high scores across every antecedent.

Practically, the findings suggest that managers and policymakers should prioritize leadership visibility and constructive engagement with institutional pressure (regulation, partner requirements, industry standards) as the primary levers for building security culture, rather than assuming that budget and staffing increases alone will produce a security-conscious organization. Because the effective mechanisms differ by security-team size and organizational tenure, differentiated strategies, rather than a uniform playbook, are warranted across organizations at different maturity stages. Such approaches can enhance organizational accountability, ensure secure and dependable digital operations, and

promote competitive sustainability in progressively interconnected business landscapes. At the level of an individual organization, that is the practical form taken by the concerns of SDG targets 16.6 and 9.1.

7.2 Limitations and Future Research Directions

This study has several limitations. The cross-sectional design precludes strong causal claims about how security culture develops over time; longitudinal designs could clarify the temporal sequencing among leadership commitment, institutional pressure, and cultural change. Reliance on self-reported managerial perceptions introduces potential social desirability bias, and future studies could triangulate survey data with objective security-incident records. The sample is concentrated in Vietnamese organizations with a large construction-sector presence, limiting generalizability to other institutional and cultural contexts; cross-national replication would help establish boundary conditions. A further caveat concerns measurement, because the heterotrait-monotrait ratio between resource capability and top management commitment reached .872, above the conservative .85 threshold, so the non-significant path from resource capability to security culture should be read with the overlap between those two constructs in mind. Finally, the non-significant SCC × EIP interaction warrants further investigation, potentially examining additional moderators such as digital supply-chain integration or sector-specific regulatory intensity, and future research could extend the fsQCA outcome to directly measured security-incident reduction rather than perceived competitiveness.

Declarations

Ethics approval and consent to participate.

Ethical approval for the original study was granted by the RMIT University BL CHEAN's COB Research Ethics Board (Project number 25540). All procedures performed in this study were in accordance with the ethical standards of the institutional research committee and with the 1964 Helsinki Declaration and its later amendments. Informed consent was obtained from all participants prior to participation, and all responses were collected and analysed anonymously.

Consent for publication.

Not applicable.

Competing interests.

The authors declare no competing interests. One of the guest editors of this Collection is a co-author of this manuscript and was not involved in the peer-review or editorial decision process for this submission.

Funding.

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability. The anonymised survey dataset supporting the findings of this study is available from the corresponding author upon reasonable request. The data are not publicly available because they contain information that could compromise the confidentiality of participating organisations.

Author Contribution

Author contributions: H.T.T. contributed to conceptualization, supervision, investigation, data curation, writing – original draft, and visualization. N.T.G.N. contributed to conceptualization, methodology, supervision, validation, and writing – review and editing. K.N.P.N. contributed to formal analysis, methodology, validation, writing – review and editing, and project administration. B.N.N.D. contributed to investigation, methodology, data curation, literature review, and supporting the original draft. L.T.H.T. contributed to investigation, data curation, validation, visualization, and writing – review and editing. L.N.P.D. contributed to conceptualization, validation, and writing – review and editing. C.H.L. contributed to formal analysis, methodology, and validation. U.L.T.P. contributed to conceptualization, validation, writing – review and editing, and project administration. All authors reviewed and approved the final manuscript.

References

1. Boyson S. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*. 2014;34(7):342–53. <https://doi.org/10.1016/j.technovation.2014.02.001>.
2. Ghadge A, Weiß M, Caldwell ND, Wilding R. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Manage*. 2020;25(2):223–40. <https://doi.org/10.1108/SCM-10-2018-0357>.
3. Colicchia C, Creazza A, Menachof DA. Managing cyber and information risks in supply chains: Insights from an exploratory analysis. *Supply Chain Manage*. 2019;24(2):215–40. <https://doi.org/10.1108/SCM-09-2017-0289>.
4. Pandey S, Singh RK, Gunasekaran A, Kaushik A. Cyber security risks in globalized supply chains: Conceptual framework. *J Global Oper Strategic Sourc*. 2020;13(1):103–28. <https://doi.org/10.1108/JGOSS-05-2019-0042>.
5. Von Solms R, Van Niekerk J. From information security to cyber security. *Computers Secur*. 2013;38:97–102. <https://doi.org/10.1016/j.cose.2013.04.004>.
6. Siponen M, Willison R. Information security management standards: Problems and solutions. *Inf Manag*. 2009;46(5):267–70. <https://doi.org/10.1016/j.im.2008.12.007>.
7. Baskerville R, Dhillon G. Information systems security strategy: A process view. In: Straub D, Goodman S, Baskerville R, editors. *Information security policies, processes, and practices*. M.E.

- Sharpe; 2008. pp. 15–45.
8. Soomro ZA, Shah MH, Ahmed J. Information security management needs more holistic approach: A literature review. *Int J Inf Manag.* 2016;36(2):215–25. <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>.
 9. Chang SE, Ho CB. Organizational factors to the effectiveness of implementing information security management. *Industrial Manage Data Syst.* 2006;106(3):345–61. <https://doi.org/10.1108/02635570610653498>.
 10. Kankanhalli A, Teo H-H, Tan BCY, Wei K-K. An integrative study of information systems security effectiveness. *Int J Inf Manag.* 2003;23(2):139–54. [https://doi.org/10.1016/S0268-4012\(02\)00105-6](https://doi.org/10.1016/S0268-4012(02)00105-6).
 11. Barney J. Firm resources and sustained competitive advantage. *J Manag.* 1991;17(1):99–120. <https://doi.org/10.1177/014920639101700108>.
 12. Bharadwaj AS. A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Q.* 2000;24(1):169–96. <https://doi.org/10.2307/3250983>.
 13. Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decis Sci.* 2012;43(4):615–60. <https://doi.org/10.1111/j.1540-5915.2012.00361.x>.
 14. Knapp KJ, Marshall TE, Rainer RK, Ford FN. Information security: Management's effect on culture and policy. *Inform Manage Comput Secur.* 2006;14(1):24–36. <https://doi.org/10.1108/09685220610648355>.
 15. DiMaggio PJ, Powell WW. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *Am Sociol Rev.* 1983;48(2):147–60. <https://doi.org/10.2307/2095101>.
 16. Cavusoglu H, Cavusoglu H, Son J-Y, Benbasat I. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Inf Manag.* 2015;52(4):385–400. <https://doi.org/10.1016/j.im.2014.12.004>.
 17. Angst CM, Block ES, D'Arcy J, Kelley K. When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Q.* 2017;41(3):893–916. <https://doi.org/10.25300/MISQ/2017/41.3.09>.
 18. Ifinedo P. Information systems security policy compliance: An empirical study of the effects of socialisation, external influence, and specificity. *Computers Secur.* 2014;46:43–55. <https://doi.org/10.1016/j.cose.2014.06.006>.
 19. Da Veiga A, Eloff JHP. A framework and assessment instrument for information security culture. *Computers Secur.* 2010;29(2):196–207. <https://doi.org/10.1016/j.cose.2009.09.002>.
 20. Da Veiga A, Martins N. Information security culture and information protection culture: A validated assessment instrument. *Comput Law Secur Rev.* 2015;31(2):243–56. <https://doi.org/10.1016/j.clsr.2015.01.005>.

21. Ashenden D. (2008). Information security management: A human challenge? *Information Security Technical Report*, 13(4), 195–201. <https://doi.org/10.1016/j.istr.2008.10.006>
22. Chen Y, Ramamurthy K, Wen K-W. Impacts of comprehensive information security programs on information security culture. *J Comput Inform Syst*. 2015;55(3):11–9. <https://doi.org/10.1080/08874417.2015.11645767>.
23. Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Q*. 2010;34(3):523–48. <https://doi.org/10.2307/25750690>.
24. Herath T, Rao HR. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decis Support Syst*. 2009;47(2):154–65. <https://doi.org/10.1016/j.dss.2009.02.005>.
25. Steenkamp J-BEM, Baumgartner H. Assessing measurement invariance in cross-national consumer research. *J Consum Res*. 1998;25(1):78–107. <https://doi.org/10.1086/209528>.
26. Fiss PC. Building better causal theories: A fuzzy set approach to typologies in organizational research. *Acad Manag J*. 2011;54(2):393–420. <https://doi.org/10.5465/amj.2011.60263120>.
27. Woodside AG. Moving beyond multiple regression analysis to algorithms: Calling for adoption of a paradigm shift from symmetric to asymmetric thinking in data analysis and crafting theory. *J Bus Res*. 2013;66(4):463–72. <https://doi.org/10.1016/j.jbusres.2012.12.021>.
28. Straub DW, Welke RJ. Coping with systems risk: Security planning models for management decision making. *MIS Q*. 1998;22(4):441–69. <https://doi.org/10.2307/249551>.
29. Whitman ME, Mattord HJ. Principles of information security. 7th ed. Cengage Learning; 2021.
30. Dhillon G, Backhouse J. Current directions in IS security research: Towards socio-organizational perspectives. *Inform Syst J*. 2001;11(2):127–53. <https://doi.org/10.1046/j.1365-2575.2001.00099.x>.
31. Wernerfelt B. A resource-based view of the firm. *Strateg Manag J*. 1984;5(2):171–80. <https://doi.org/10.1002/smj.4250050207>.
32. Melville N, Kraemer K, Gurbaxani V. Information technology and organizational performance: An integrative model of IT business value. *MIS Q*. 2004;28(2):283–322. <https://doi.org/10.2307/25148636>.
33. Teece DJ. Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strateg Manag J*. 2007;28(13):1319–50. <https://doi.org/10.1002/smj.640>.
34. Teece DJ, Pisano G, Shuen A. Dynamic capabilities and strategic management. *Strateg Manag J*. 1997;18(7):509–33. [https://doi.org/10.1002/\(SICI\)1097-0266\(199708\)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z](https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%3C509::AID-SMJ882%3E3.0.CO;2-Z).
35. Eisenhardt KM, Martin JA. Dynamic capabilities: What are they? *Strateg Manag J*. 2000;21(10–11):1105–21. [https://doi.org/10.1002/1097-0266\(200010/11\)21:10/11%3C1105::AID-SMJ133%3E3.0.CO;2-E](https://doi.org/10.1002/1097-0266(200010/11)21:10/11%3C1105::AID-SMJ133%3E3.0.CO;2-E).

36. Meyer JW, Rowan B. Institutionalized organizations: Formal structure as myth and ceremony. *Am J Sociol.* 1977;83(2):340–63. <https://doi.org/10.1086/226550>.
37. Oliver C. Strategic responses to institutional processes. *Acad Manage Rev.* 1991;16(1):145–79. <https://doi.org/10.5465/amr.1991.4279002>.
38. Scott WR. *Institutions and organizations: Ideas, interests, and identities.* 4th ed. SAGE; 2013.
39. Kwon J, Johnson ME. Proactive versus reactive security investments in the healthcare sector. *MIS Q.* 2014;38(2):451–71. <https://doi.org/10.25300/MISQ/2014/38.2.06>.
40. Puhakainen P, Siponen M. Improving employees' compliance through information systems security training: An action research study. *MIS Q.* 2010;34(4):757–78. <https://doi.org/10.2307/25750704>.
41. Dutta A, McCrohan K. Management's role in information security in a cyber economy. *Calif Manag Rev.* 2002;45(1):67–87. <https://doi.org/10.2307/41166154>.
42. Flores WR, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers Secur.* 2014;43:90–110. <https://doi.org/10.1016/j.cose.2014.03.004>.
43. Karyda M, Kiountouzis E, Kokolakis S. Information systems security policies: A contextual perspective. *Computers Secur.* 2005;24(3):246–60. <https://doi.org/10.1016/j.cose.2004.08.011>.
44. Williams SP, Hardy CA, Holgate JA. Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electron Markets.* 2013;23(4):341–54. <https://doi.org/10.1007/s12525-013-0137-3>.
45. Ragin CC. *Redesigning social inquiry: Fuzzy sets and beyond.* University of Chicago Press; 2008. <https://doi.org/10.7208/chicago/9780226702797.001.0001>.
46. Pappas IO, Woodside AG. Fuzzy-set qualitative comparative analysis (fsQCA): Guidelines for research practice in information systems and marketing. *Int J Inf Manag.* 2021;58:102310. <https://doi.org/10.1016/j.ijinfomgt.2021.102310>.
47. Byrne BM. *Structural equation modeling with AMOS: Basic concepts, applications, and programming.* 3rd ed. Routledge; 2016.
48. Hair JF, Black WC, Babin BJ, Anderson RE. *Multivariate data analysis.* 8th ed. Cengage Learning; 2019.
49. Etikan I, Musa SA, Alkassim RS. Comparison of convenience sampling and purposive sampling. *Am J Theoretical Appl Stat.* 2016;5(1):1–4. <https://doi.org/10.11648/j.ajtas.20160501.11>.
50. Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *J Appl Psychol.* 2003;88(5):879–903. <https://doi.org/10.1037/0021-9010.88.5.879>.
51. Kline RB. *Principles and practice of structural equation modeling.* 4th ed. Guilford Press; 2016.
52. Bagozzi RP, Yi Y. On the evaluation of structural equation models. *J Acad Mark Sci.* 1988;16(1):74–94. <https://doi.org/10.1007/BF02723327>.

53. Henseler J, Ringle CM, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *J Acad Mark Sci.* 2015;43:115–35.
<https://doi.org/10.1007/s11747-014-0403-8>.
54. Fornell C, Larcker DF. Evaluating structural equation models with unobservable variables and measurement error. *J Mark Res.* 1981;18(1):39–50. <https://doi.org/10.1177/002224378101800104>.
55. Hu L, Bentler PM. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Struct Equ Model.* 1999;6(1):1–55.
<https://doi.org/10.1080/10705519909540118>.
56. Preacher KJ, Hayes AF. Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behav Res Methods.* 2008;40(3):879–91.
<https://doi.org/10.3758/BRM.40.3.879>.
57. Chow GC. Tests of equality between sets of coefficients in two linear regressions. *Econometrica.* 1960;28(3):591–605. <https://doi.org/10.2307/1910133>.
58. Rihoux B, Ragin CC, editors. *Configurational comparative methods: Qualitative comparative analysis (QCA) and related techniques.* SAGE; 2009. <https://doi.org/10.4135/9781452226569>.
59. Schneider CQ, Wagemann C. *Set-theoretic methods for the social sciences: A guide to qualitative comparative analysis.* Cambridge University Press; 2012.
<https://doi.org/10.1017/CBO9781139004244>.
60. Tran HT, Pham QTT, Nguyen PV. Digital transformation solution implementation risk in logistics and supply chain industry. *Discover Sustain.* 2026;7(1):239. <https://doi.org/10.1007/s43621-026-02603-4>.
61. Tharwat H, Hafez ST, Elgohary IE, Hassanein A. A decade of cybersecurity research in internal auditing: bibliometric mapping and future research agenda. *Discover Sustain.* 2025;6(1):1066.
<https://doi.org/10.1007/s43621-025-02031-w>.

Figures

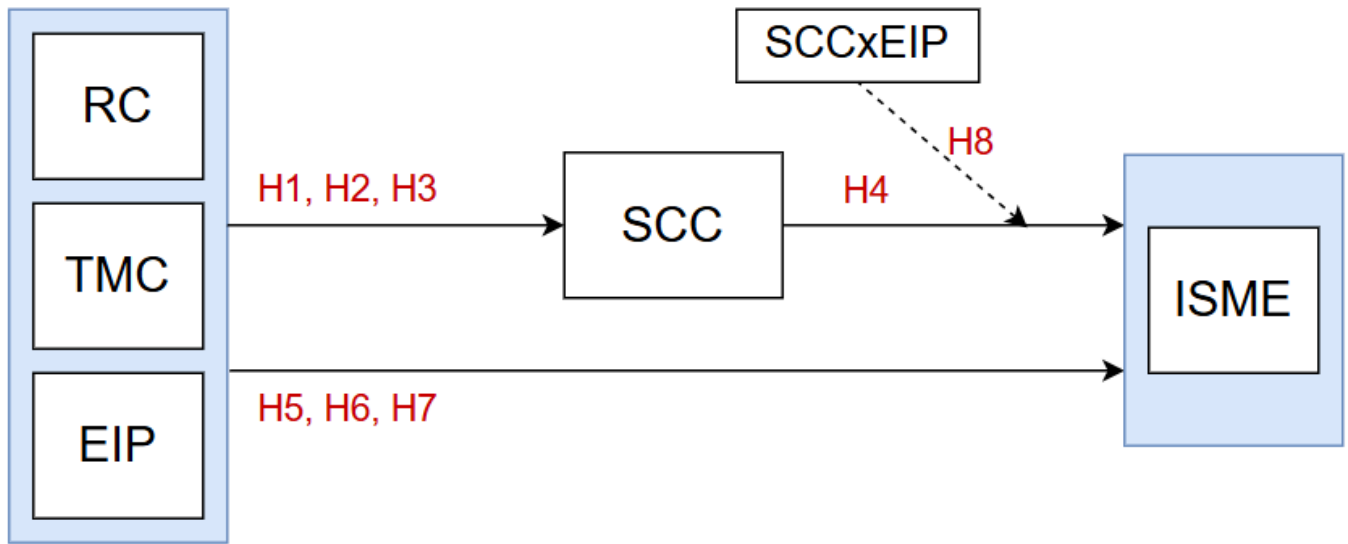


Figure 1

Conceptual Model

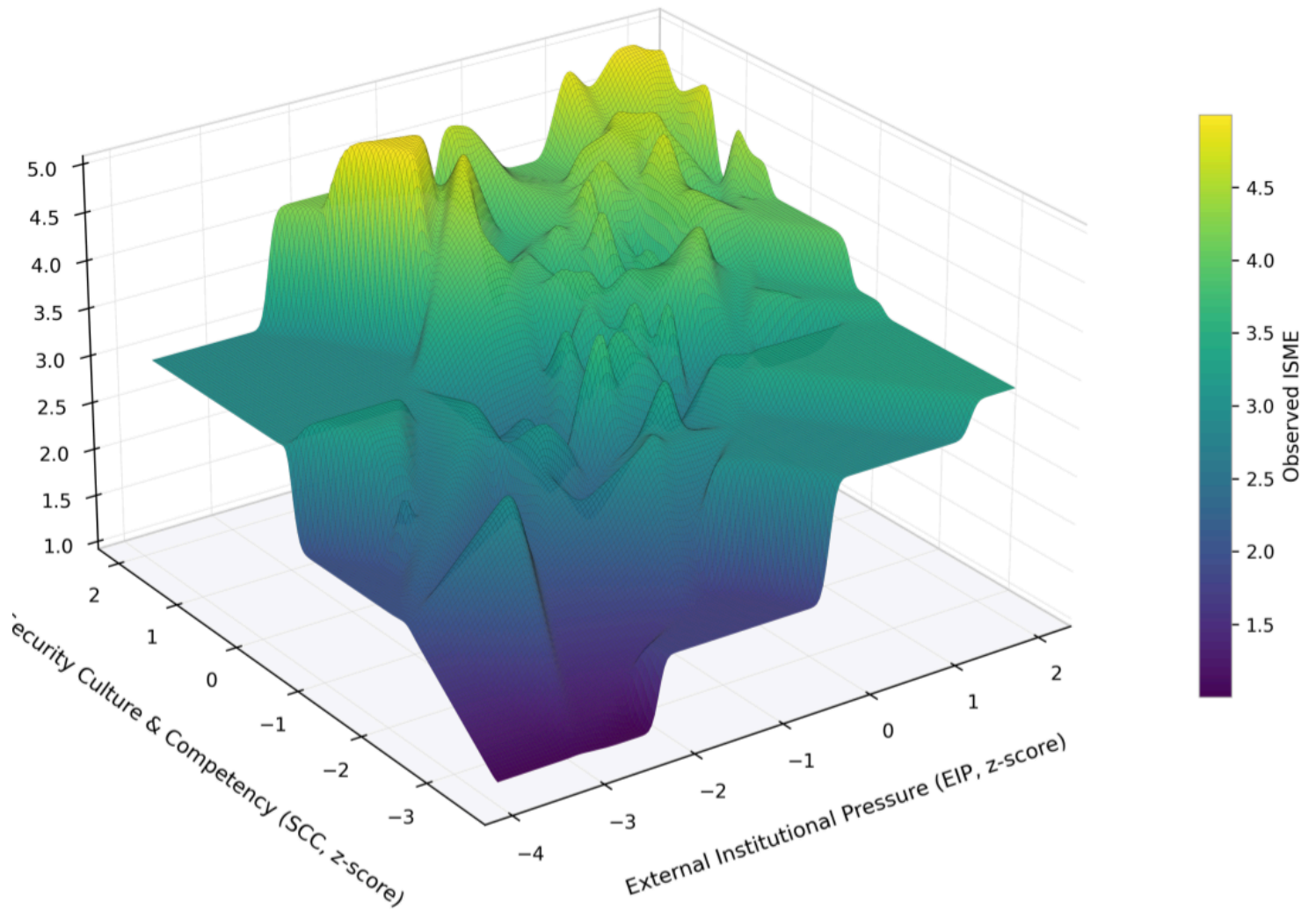


Figure 2

Response-Surface ("Rocky") Plot of Observed Information Security Management Effectiveness across External Institutional Pressure and Security Culture & Competency (N = 358)

Figure 3. fsQCA Configurational Roadmaps

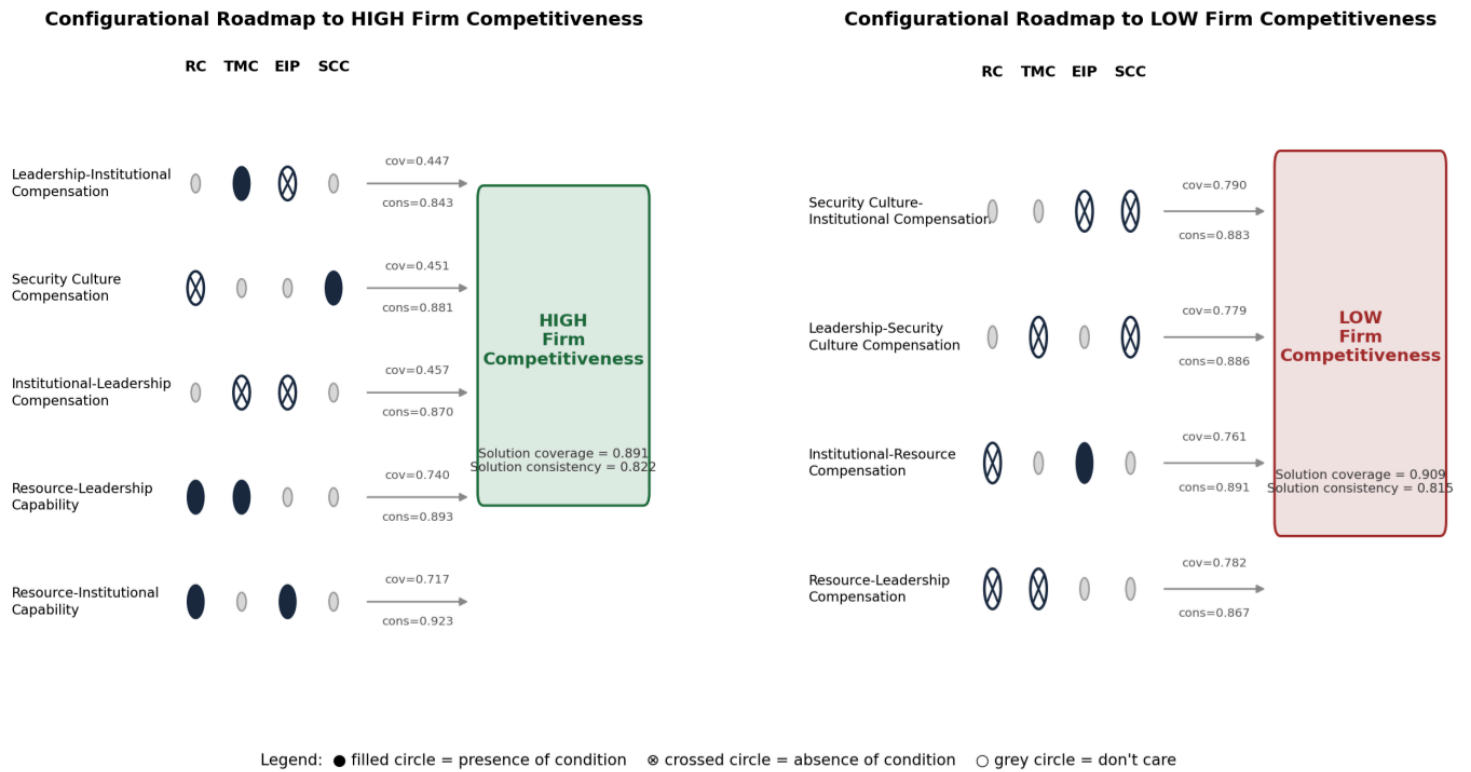


Figure 3

fsQCA Configurational Roadmaps