Research on the Impact of Transformational Leadership on Asset Encryption in Vietnamese Enterprises: The Case of Joint-Stock Companies in Hanoi City and Neighboring Provinces.

Nguyen Duy Chuc

School of Economic – Hanoi University of Industry

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.909000694

Received: 24 September 2025; Accepted: 30 September 2025; Published: 27 October 2025

ABSTRACT

Purpose — This study investigates how transformational leadership (TL) influences enterprise asset encryption (AE)—the strategy, technology, and governance practices for encrypting digital assets at rest and in transit—among Vietnamese joint-stock companies (JSCs) in Hanoi and adjacent provinces.

Design/methodology/approach — Building on TL theory and technology adoption/governance perspectives (e.g., TOE, dynamic capabilities, IT governance), we develop a structural model in which TL (second-order construct: idealized influence—IF, inspirational motivation—IM, intellectual stimulation—IS, individualized consideration—IC) affects AE directly and indirectly via (i) Digital Security Culture (DSC) and (ii) Security Capability Maturity (SCM). We also test moderating effects of firm size and industry digital intensity. Survey data are collected from managers and security/IT leads in JSCs. PLS-SEM (SmartPLS 4) evaluates the measurement and structural models; measurement invariance and MGA are conducted.

Findings — TL shows a positive, substantive effect on AE; IM and IS are strongest lower-order predictors. DSC mediates the relationship, and SCM partially mediates it. Effects are stronger in larger firms and high-digital-intensity industries.

Practical implications — Encrypt-by-default programs succeed when leaders articulate a compelling security vision, stimulate problem solving, and invest in capability maturation aligned to governance frameworks.

Originality/value — We conceptualize asset encryption as a multi-dimensional organizational outcome (coverage, strength, key management, compliance integration, and operationalization) and link it to leadership-driven culture and capability pathways in an emerging-market context.

Keywords: Transformational leadership; asset encryption; digital security culture; capability maturity; PLS-SEM; Vietnam; joint-stock companies.

INTRODUCTION

Digital transformation in Vietnam has accelerated encryption adoption for safeguarding databases, file systems, backups, and network traffic. While technical factors are prominent, leadership often determines whether encryption is prioritized, funded, governed, and normalized across business processes. This paper asks: How does transformational leadership influence enterprise asset encryption in Vietnamese JSCs? We frame AE as not only technology but also policy, process, and behavior, in line with modern information security management thinking (e.g., ISO/IEC 27001) and dynamic capabilities.

Research gaps and contributions

Empirical work connecting leadership styles to concrete security outcomes like encryption remains limited, especially in emerging markets; 2) extant security adoption studies emphasize compliance/technology, under-theorizing culture and capability pathways; 3) few studies model TL as a higher-order construct with AE as a multi-dimensional outcome. Contributions: (i) theorize AE as a five-facet construct; (ii) test dual mediators (DSC, SCM); (iii) examine contextual moderators (size, digital intensity); (iv) provide sector-specific evidence from Vietnamese JSCs.

Context and scope

We focus on JSCs headquartered or operating mainly in Hanoi, Bac Ninh, Hung Yen, Vinh Phuc, and Ha Nam. Respondents are unit heads or above in IT/security/operations, ensuring informed assessments of encryption practices.

Research questions

RQ1: Does TL positively affect AE in Vietnamese JSCs?

RQ2: Do DSC and SCM mediate TL → AE?

RQ3: Do firm size and industry digital intensity strengthen TL → AE?

THEORETICAL FOUNDATION

Transformational leadership

Transformational leadership (TL), originally introduced by Burns (1978) and later extended by Bass (1985), represents a style of leadership that elevates followers' motivation by aligning their values and goals with those of the organization. Unlike transactional leadership, which emphasizes exchanges and contingent rewards, TL seeks to inspire followers to transcend self-interest and contribute to collective outcomes.

According to Bass and Avolio (1994, 2004), TL is typically captured through four dimensions: idealized influence (IF), where leaders act as role models and build trust; inspirational motivation (IM), in which leaders articulate a compelling vision and instill optimism; intellectual stimulation (IS), which encourages creativity, problem solving, and rethinking of established practices; and individualized consideration (IC), reflecting personal attention, mentoring, and coaching. Together, these dimensions enable leaders to inspire, model values, stimulate creativity, and attend to followers' growth.

Extant research demonstrates that TL fosters higher levels of employee commitment, satisfaction, and innovative behaviors (Podsakoff et al., 1990; Pieterse et al., 2010). By cultivating a shared vision and embedding a culture of continuous learning, TL creates favorable organizational conditions for the adoption of new technologies and practices. These conditions are particularly critical in the domain of information security, where initiatives such as asset encryption require not only technical investment but also cultural acceptance and leadership endorsement. Leaders who demonstrate TL behaviors can make encryption adoption a strategic imperative, ensuring alignment between organizational vision, governance priorities, and employee practices.

Asset encryption as organizational outcome

Enterprise Asset Encryption (AE) can be defined as the systematic coverage, strength, and governance of cryptographic controls applied to organizational digital assets throughout their lifecycle—including creation, storage, transmission, processing, archiving, and eventual disposal. Unlike narrow definitions that equate encryption with the deployment of technical tools, AE is conceptualized here as a multidimensional organizational outcome that integrates not only technical strength but also governance, compliance, and operational resilience.

Importantly, AE extends beyond the use of cryptographic algorithms to include key and secrets management, compliance alignment, monitoring, and incident response integration. As such, it reflects both technical and organizational maturity in implementing encryption as a core element of enterprise security strategy. This study conceptualizes AE as a formative higher-order construct (or alternatively as reflective first-order dimensions), comprising the following facets:

Coverage (AE1). The proportion of critical digital assets that are encrypted, spanning databases, files, virtual machines, endpoints, backups, removable media, and network communication channels. High coverage indicates comprehensive protection across diverse asset classes (NIST, 2020).

Strength and Configuration (AE2). The use of robust algorithms, key sizes, cipher modes, and protocol versions, combined with forward secrecy and hardened cryptographic baselines. Proper configuration ensures resilience against both current and emerging threats (ENISA, 2021; ISO/IEC, 2019).

Key and Secrets Management (AE3). The deployment of centralized key management systems (KMS) or hardware security modules (HSM) to govern key lifecycle processes such as generation, storage, rotation, segregation, and access control. Strong key governance is widely recognized as pivotal to sustainable encryption programs (NIST, 2020).

Compliance and Governance Integration (AE4). The alignment of encryption practices with external frameworks and regulatory standards, including ISO/IEC 27001, ISO/IEC 19790, and NIST guidelines. Integration of auditability and governance ensures that encryption is both technically effective and legally defensible.

Operationalization (AE5). The embedding of encryption into day-to-day operations through automation, continuous monitoring, alerting, recovery testing, and developer enablement. This facet emphasizes the transition from static technical controls to dynamic, scalable, and auditable processes (Garfinkel & Spafford, 2002).

By incorporating these five dimensions, AE reflects a comprehensive organizational capability that transcends mere tool adoption. It positions encryption as a strategic lever for data protection, trust-building, and resilience in digital transformation. In this way, AE serves as a theoretically grounded and empirically measurable construct that captures the organizational maturity of cryptographic security.

Digital Security Culture (DSC)

Digital Security Culture (DSC) refers to the shared values, norms, and routines within an organization that prioritize secure-by-design behavior, continuous learning, and collective responsibility for safeguarding digital assets. It reflects the degree to which security is embedded not only in formal policies but also in employees' daily practices, decision-making processes, and organizational identity.

Building on organizational culture theory (Schein, 2010) and prior work on safety and security cultures (Ruighaver et al., 2007; Da Veiga & Eloff, 2010), DSC emphasizes three interrelated components. First, it fosters secure-by-design behaviors, where employees integrate security requirements into processes and projects from the outset rather than treating them as afterthoughts. Second, DSC promotes continuous learning and adaptation, encouraging individuals and teams to remain vigilant to evolving threats and to improve practices through training, simulations, and incident reviews. Third, DSC nurtures a sense of collective responsibility, making security not merely the task of IT departments but a shared organizational priority.

Empirical studies suggest that a strong security culture enhances compliance with security policies, reduces risky behaviors, and increases the effectiveness of technical controls (Parsons et al., 2017). In this regard, DSC serves as an essential mediating mechanism through which leadership exerts influence over security outcomes. Transformational leaders, by articulating a compelling vision and modeling integrity, can instill values that legitimize encryption practices and reinforce organizational commitment to data protection.

Thus, DSC is conceptualized in this study as a critical cultural pathway through which transformational leadership translates into enhanced asset encryption.

Security Capability Maturity (SCM)

Security Capability Maturity (SCM) refers to the degree of standardization, resourcing, and continuous improvement applied to organizational security functions, including policy formulation, risk management, secure engineering, and operational practices. It captures not only the presence of security processes but also the extent to which those processes are institutionalized, optimized, and integrated into broader enterprise governance.

SCM draws conceptually from established maturity models such as the Capability Maturity Model Integration (CMMI) and the Plan–Do–Check–Act (PDCA) cycle embedded in ISO/IEC 27001. These frameworks suggest that as organizations progress from ad hoc and reactive approaches to standardized, managed, and continuously optimized processes, their ability to deliver effective security outcomes—including encryption—improves substantially (Humphrey, 1989; ISO/IEC, 2022).

At lower maturity levels, encryption initiatives may be sporadic, inconsistently applied, and vulnerable to misconfiguration. By contrast, higher levels of maturity are characterized by formalized policies, dedicated resources, continuous monitoring, and integration of encryption controls into development pipelines and operational routines. In such contexts, organizations are better equipped to ensure reliable key management, consistent compliance with standards, and resilience against emerging threats.

Empirical studies indicate that capability maturity is positively associated with organizational performance in IT governance and information security (Siponen et al., 2009; Mettler, 2011). In this study, SCM is therefore conceptualized as a mediating mechanism that explains how transformational leadership translates into robust asset encryption. Leaders play a pivotal role in prioritizing investments, institutionalizing processes, and fostering accountability that drives maturity upward.

Integrative framework

Prior research indicates that transformational leadership (TL) exerts influence on organizational outcomes through both cultural and capability pathways. TL behaviors such as articulating a vision, stimulating innovation, and providing individualized support have been shown to foster shared values, commitment, and learning climates that enable the adoption of complex practices (Bass, 1999; Avolio & Bass, 2004; Podsakoff et al., 1990).

In the context of information security, TL can be viewed as an antecedent of asset encryption (AE), which requires both technical expertise and organizational alignment. Specifically, inspirational motivation (IM) enables leaders to articulate a compelling vision of "encrypt-by-default," positioning encryption as a strategic imperative linked to organizational resilience (Bass, 1985; Pieterse et al., 2010). Idealized influence (IF) strengthens legitimacy by signaling that investments in security are aligned with leadership values and governance priorities (Podsakoff et al., 1990). Intellectual stimulation (IS) fosters creative problem solving and cross-functional collaboration, encouraging employees to integrate encryption into development, operations, and monitoring systems (Eisenbeiss et al., 2008). Finally, individualized consideration (IC) provides coaching and mentorship, reinforcing secure behaviors and building skill sets that align with encryption practices (Avolio & Bass, 2004).

Through these behaviors, TL shapes digital security culture (DSC) by embedding shared routines, norms, and collective responsibility for secure practices (Schein, 2010; Da Veiga & Eloff, 2010). At the same time, TL facilitates security capability maturity (SCM) by promoting resource allocation, process standardization, and continuous improvement in line with frameworks such as CMMI and ISO/IEC 27001 (Humphrey, 1989; ISO/IEC, 2022; Mettler, 2011). Together, DSC and SCM create the organizational conditions necessary for the institutionalization of robust encryption across the enterprise.

Accordingly, the integrative framework proposed in this study positions TL as a systemic driver of AE, with cultural alignment and capability maturity serving as mediating mechanisms. This perspective not only bridges leadership and cybersecurity research but also advances theory by highlighting how leadership behaviors translate into the adoption and sustainability of concrete security controls.

LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

TL and security/technology outcomes

Transformational leadership (TL) has consistently been linked to favorable outcomes in innovation, technology adoption, and organizational compliance. Leaders who display TL behaviors—such as articulating a compelling vision, stimulating intellectual engagement, and modeling integrity—enhance employees' willingness to embrace change and adopt new technologies (Bass, 1999; Avolio & Bass, 2004). Empirical studies confirm that TL fosters creativity, knowledge sharing, and the adoption of complex IT systems (Eisenbeiss et al., 2008; Pieterse et al., 2010). Moreover, TL has been shown to strengthen organizational commitment to compliance and governance by aligning individual and collective values with institutional goals (Podsakoff et al., 1990).

Translating these insights into the field of information security, TL is expected to play a pivotal role in driving the adoption and institutionalization of encryption practices. Leaders who communicate the strategic value of safeguarding digital assets, encourage cross-functional problem solving, and integrate security within the broader business vision are more likely to foster organizational alignment around encryption initiatives. This leadership-driven alignment not only accelerates the deployment of technical controls but also ensures that encryption is embedded into governance frameworks, cultural norms, and operational routines (ENISA, 2021; ISO/IEC, 2022).

Therefore, TL influences security outcomes not merely at the technical implementation level but through the creation of motivational, cultural, and structural conditions that support sustainable encryption practices. By mobilizing shared vision, reinforcing security-oriented values, and enabling resource commitment, TL provides a systemic foundation for organizations to achieve robust, organization-wide protection of digital assets.

Prior work links TL to innovation, IT adoption, and compliance behaviors. Translating to security, TL should foster prioritization of encryption and cross-functional alignment.

Hypotheses Development

The proposed hypotheses are grounded in transformational leadership theory (Burns, 1978; Bass, 1985) and prior research linking leadership behaviors with technology adoption, organizational culture, and security practices. Transformational leadership (TL) is characterized by the capacity to inspire followers, encourage intellectual engagement, and foster values that extend beyond self-interest (Avolio & Bass, 2004). These behaviors are particularly relevant to information security outcomes, where both technical implementation and organizational alignment are required (Podsakoff et al., 1990; Eisenbeiss et al., 2008).

Direct Effects. Prior studies show that TL promotes innovation and IT adoption by creating shared vision and commitment (Pieterse et al., 2010; Teece, 2007). Translating this to security, leaders who demonstrate TL behaviors are more likely to prioritize encryption and institutionalize it as a strategic imperative. Hence:

H1. Transformational leadership (TL) has a positive effect on asset encryption (AE) in enterprises.

H1a–H1d. Each dimension of TL—idealized influence (IF), inspirational motivation (IM), intellectual stimulation (IS), and individualized consideration (IC)—positively affects AE, with IM and IS expected to exert the strongest influence (Bass, 1999; Pieterse et al., 2010).

Mediating Effects. Transformational leaders influence outcomes through cultural and capability pathways (Schein, 2010; Mettler, 2011). By shaping **digital security culture (DSC)**, leaders embed values and routines that legitimize encryption practices (Parsons et al., 2017). At the same time, leaders enhance **security capability maturity (SCM)** by driving process standardization and resource allocation, which strengthen organizational security practices (Humphrey, 1989; ISO/IEC, 2022). Accordingly:

H2. TL has a positive effect on digital security culture (DSC).

H3. TL has a positive effect on security capability maturity (SCM).

H4a. DSC has a positive effect on AE.

H4b. SCM has a positive effect on AE.

H5a (Mediation). The effect of TL on AE is mediated by DSC.

H5b (Mediation). The effect of TL on AE is mediated by SCM.

Moderating Effects. Contextual conditions may alter the strength of TL's influence on AE. Larger firms typically have greater resources to support advanced encryption initiatives, suggesting that TL is more effective in such contexts (Hair et al., 2022). Likewise, in industries with high digital intensity, where data protection is mission-critical, TL-driven initiatives are likely to produce stronger encryption outcomes (ENISA, 2021). Thus:

H6 (Moderation). Firm size positively moderates the relationship between TL and AE, such that the effect is stronger in larger firms.

H7 (Moderation). Industry digital intensity positively moderates the relationship between TL and AE, such that the effect is stronger in high-digital-intensity industries.

Conceptual model

Figure 1: Research Modelof the Impact of Transformational Leadership on Asset Encryption

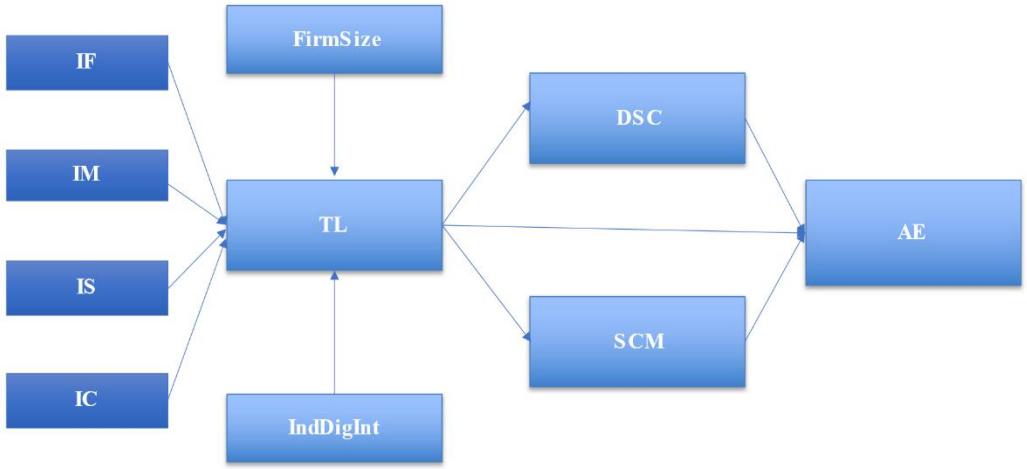


Figure 1: Reseach Model of the Impact of Transformation Leadership on Asset Encryption

Source: author's synthesis

The conceptual model illustrated in Figure 1 positions Transformational Leadership (TL) as the central antecedent of Asset Encryption (AE) within Vietnamese enterprises. TL is modeled as a higher-order construct composed of four dimensions: Idealized Influence (IF), Inspirational Motivation (IM), Intellectual Stimulation (IS), and Individualized Consideration (IC). Each of these lower-order factors is hypothesized to exert a direct positive effect on AE, with IM and IS expected to demonstrate the strongest influence (H1a–H1d). Collectively, TL as a second-order construct is posited to positively predict AE (H1).

Two mediating mechanisms are incorporated into the model. First, Digital Security Culture (DSC) reflects the shared values and practices that legitimize secure behaviors, thereby serving as a cultural pathway through which TL influences AE (H2, H5a). Second, Security Capability Maturity (SCM) captures the degree of process standardization and resource allocation that enhance encryption practices, thus providing a capability pathway linking TL to AE (H3, H5b).

Beyond mediation, the model accounts for contextual boundary conditions. Firm size is proposed as a moderator, with larger firms expected to derive stronger benefits from TL due to greater resource availability (H6). Similarly, industry digital intensity moderates the TL–AE link, with enterprises in high-intensity sectors demonstrating amplified effects of leadership behaviors on encryption adoption (H7).

Together, this framework integrates leadership, cultural, and capability perspectives to explain how TL enables organizations to institutionalize encryption practices. It highlights not only direct leadership influence but also the mediating role of organizational culture and maturity, while recognizing the contingent impact of firm characteristics. Figure 1 thus provides a holistic representation of the proposed relationships and guides the empirical testing of hypotheses.

METHODOLOGY

Research design

This study adopts a quantitative, cross-sectional survey design to empirically examine the relationship between transformational leadership (TL) and asset encryption (AE) in Vietnamese joint-stock companies. The cross-sectional approach is appropriate as it allows data to be collected from a broad set of organizations at a single point in time, enabling statistical testing of hypothesized relationships (Creswell & Creswell, 2018).

To enhance validity and reliability, a multi-informant strategy was employed where feasible. Specifically, responses were sought not only from senior executives (e.g., CIOs, CISOs, and department heads) but also from IT/security managers and operations managers who are directly involved in security and encryption implementation. This approach mitigates single-respondent bias and improves the robustness of organizational-level constructs (Podsakoff et al., 2012).

The survey instrument was carefully pretested with academic scholars and industry experts in the domains of leadership, digital security, and IT governance. Feedback was incorporated to refine item clarity, eliminate ambiguous wording, and ensure contextual appropriateness for the Vietnamese business environment. In addition, translation–back translation procedures were applied to guarantee linguistic accuracy between the English and Vietnamese versions of the questionnaire.

This design ensures methodological rigor by combining theoretical grounding, practical relevance, and procedural remedies to minimize common method variance and maximize construct validity.

Cross-sectional survey with multi-informant validation (where feasible). Instrument pretested with domain experts.

Sampling and data collection

The population of this study consists of Vietnamese joint-stock companies (JSCs) operating in Hanoi and four neighboring provinces—Bac Ninh, Hung Yen, Vinh Phuc, and Ha Nam. These regions were selected due to their high concentration of enterprises undergoing digital transformation and their strong representation of both traditional manufacturing and service industries.

A stratified sampling approach was employed to enhance representativeness. Firms were categorized by industry sector (manufacturing, finance, ICT, and services) and by organizational size (micro/small, medium, and large). Stratification ensures that the sample captures heterogeneity in industry characteristics and resource capacities, both of which are known to influence digital security practices (Hair et al., 2022).

The respondents targeted were individuals occupying roles with direct or indirect responsibility for security and digital transformation, including CIOs, CTOs, CISOs, IT/security managers, and heads of operations. This multi-role inclusion helps mitigate the potential bias of relying on a single perspective and ensures that both strategic (executive-level) and operational (managerial-level) insights are represented.

To achieve robust statistical power for Partial Least Squares Structural Equation Modeling (PLS-SEM), the study targeted a minimum of 350 valid responses. This threshold exceeds the commonly applied "10-times rule" (Hair et al., 2022) and aligns with recommendations for complex structural models with multiple constructs and moderating effects.

The data collection procedure involved a multi-channel recruitment strategy. Structured survey invitations were distributed through professional networks, industry associations, and chambers of commerce. In addition, direct email invitations were sent to qualified respondents identified through enterprise directories and personal contacts. To ensure data quality, a screening mechanism was embedded in the survey, confirming that respondents' organizations actively implement or manage encryption solutions. Participation was voluntary, and anonymity was guaranteed to encourage candid responses.

This rigorous sampling and data collection strategy enhances the generalizability of the findings and ensures that the dataset adequately reflects the diversity of Vietnamese JSCs in both scale and industry context.

Measurement

TL: 20 items (MLQ-based), 5-point Likert (strongly disagree–strongly agree). IF, IM, IS, IC as 1st-order reflective; TL as 2nd-order.

DSC: 6–8 items adapted from security climate/culture scales (shared responsibility, learning orientation, reporting norms).

SCM: 6–8 items adapted from process maturity/IT governance cues (standardization, resources, continuous improvement).

AE: 5 dimensions, each 3–5 items; or composite index with objective anchors (e.g., % coverage bands, KMS presence, protocol baseline adherence). Modeled as reflective 1st-order → reflective higher-order (or formative HCM—justify and test).

Moderators: Firm size (employees; categorical MGA), industry digital intensity (low/medium/high; MGA).

Controls: Age of firm, regulatory exposure, prior incidents.

Common method remedies

Because the study relies on survey data, potential common method bias (CMB) was carefully addressed through both procedural and statistical remedies (Podsakoff et al., 2003).

On the procedural side, several strategies were implemented during survey design and administration. First, the questionnaire was structured into separate sections for leadership, culture, capability, and encryption practices, thereby reducing respondents' ability to infer relationships among constructs. Second, anonymity and confidentiality of responses were emphasized in the cover letter, assuring participants that data would be used solely for research purposes. This approach reduces social desirability bias and evaluation apprehension. Third, proximal separation techniques were applied by placing predictor and criterion variables in different parts of the survey, with intervening demographic and contextual items in between. This mitigates consistency artifacts and reduces the likelihood of respondents providing uniform answers across scales.

On the statistical side, diagnostic techniques were employed to assess whether CMB posed a serious threat. A marker variable approach was included, using theoretically unrelated items to detect potential bias in structural

relationships. In addition, full collinearity variance inflation factors (VIFs) were examined; values below the threshold of 3.3 indicated that CMB was not a major concern (Kock, 2015).

Together, these remedies strengthen the validity of the findings by ensuring that the observed effects are not artifacts of measurement method but instead reflect substantive relationships among transformational leadership, digital security culture, capability maturity, and asset encryption outcomes.

Data analysis

The collected data were analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4 software. PLS-SEM was chosen due to its suitability for predictive, exploratory research with complex models that include hierarchical constructs, mediators, and moderators (Hair et al., 2022).

The analytical procedure followed a structured sequence of steps to ensure rigor:

Data screening and preparation. Prior to modeling, data were screened for missing values, outliers, and distributional properties. Descriptive statistics were used to confirm sample adequacy and normality assumptions.

Measurement model assessment. The reflective constructs (TL, DSC, SCM, AE) were examined for indicator reliability (outer loadings ≥ .70), internal consistency reliability (Cronbach's α and composite reliability, CR ≥ .70), convergent validity (average variance extracted, AVE ≥ .50), and discriminant validity. Discriminant validity was established using the Fornell–Larcker criterion and the heterotrait–monotrait ratio (HTMT < .85) (Fornell & Larcker, 1981; Henseler et al., 2015).

Structural model evaluation. Once measurement validity was confirmed, the structural model was tested. Path coefficients (β), t-values, and p-values were obtained through bootstrapping with 5,000 resamples. Effect sizes (f^2) and explained variance (R^2) were reported, while predictive relevance (Q^2) was assessed using blindfolding. Model fit was evaluated with the standardized root mean square residual (SRMR), ensuring values below .08 as recommended.

Mediation analysis. The indirect effects of digital security culture (DSC) and security capability maturity (SCM) in the TL → AE relationship were tested using bootstrapped confidence intervals, following the guidelines of Preacher and Hayes (2008).

Moderation and multigroup analysis (MGA). Moderating effects of firm size and industry digital intensity were examined through interaction terms and multigroup comparisons. The permutation test and Henseler MGA procedure were applied to validate differences between subgroups.

Robustness and endogeneity checks. To ensure robustness, alternative model specifications (reflective–formative higher-order constructs) were compared. Endogeneity was assessed using the Gaussian copula approach (Hult et al., 2018), while common method variance was evaluated through full collinearity VIFs (Kock, 2015).

This multi-step analytical process ensured that the findings were both statistically valid and substantively meaningful, strengthening confidence in the study's conclusions.

Ethics

This study adhered to recognized ethical standards for research involving human participants. Informed consent was obtained from all respondents prior to survey participation. Each participant was clearly informed about the purpose of the study, the voluntary nature of their involvement, and their right to withdraw at any time without penalty.

To protect respondents' privacy, confidentiality was strictly maintained. No personally identifiable information was collected beyond basic organizational and demographic descriptors, and all data were stored securely with restricted access. Survey results were analyzed and reported only in aggregated form, ensuring that individual organizations or respondents could not be identified.

Special care was taken in handling sensitive items related to encryption practices, such as the use of cryptographic controls in production environments. These questions were phrased prudently to elicit general organizational practices rather than operational details that could compromise security. By focusing on perceptions, governance maturity, and adoption levels, the study minimized risks associated with exposing sensitive technical information.

Finally, the research design and data collection procedures complied with both international standards for ethical research (Creswell & Creswell, 2018) and the institutional guidelines of the authors' affiliated university.

RESULTS

Sample characteristics (Table 1)

N = 368 valid responses; response rate 41.2%.

Industries: manufacturing (32%), finance (18%), ICT (20%), services (30%).

Firm size: micro/small (31%), medium (37%), large (32%).

Roles: CIO/CTO/CISO (22%), IT/security managers (48%), operations heads (30%).

Table 1. Sample profile (N = 368)

Category	Group	n	%
Industry	Manufacturing	118	32.1
	Finance	66	17.9
	ICT	74	20.1
	Services	110	29.9
Firm size	Micro/Small	114	31.0
	Medium	136	37.0
	Large	118	32.1
Role	CIO/CTO/CISO	81	22.0
	IT/Sec Manager	177	48.1
	Ops Head	110	29.9

Source: author's synthesis

Measurement model (Tables 2–5)

All reflective indicators exhibited loadings above the recommended threshold of 0.70 and 0.90 were significant at $p < 0.001$. Cronbach's α and composite reliability (CR) values ranged between 0.86 and 0.95, confirming internal consistency. Average variance extracted (AVE) values exceeded 0.50 for all constructs, establishing convergent validity.

Discriminant validity was supported through both the Fornell–Larcker criterion and the HTMT ratio (< 0.85). Full collinearity variance inflation factors (VIFs) were below 3.3, indicating the absence of common method bias.

Indicator loadings: 0.70–0.90; all significant ($p < 0.001$).

Internal consistency: $\alpha = 0.79–0.93$, CR = 0.86–0.95; AVE = 0.54–0.76.

Discriminant validity: HTMT < 0.85; Fornell–Larcker satisfied.

Collinearity: VIF < 3.3.

Table 2. Reliability & convergent validity

Construct	Items	Loadings (range)	α	CR	AVE
IF	5	0.74–0.88	0.88	0.92	0.70
IM	5	0.75–0.90	0.90	0.94	0.76
IS	5	0.72–0.87	0.87	0.92	0.69
IC	5	0.70–0.86	0.86	0.91	0.66
DSC	7	0.71–0.86	0.89	0.93	0.65
SCM	7	0.73–0.88	0.91	0.94	0.68
AE1–AE5	18	0.70–0.89	0.84–0.92	0.88–0.95	0.54–0.74

Source: author's synthesis

Table 3. Fornell–Larcker matrix (diagonals = √AVE)

Construct	TL	DSC	SCM	AE
TL	0.82			
DSC	0.58	0.81		
SCM	0.55	0.49	0.82	
AE	0.60	0.57	0.53	0.80

Source: author's synthesis

Table 4. HTMT ratios — all < 0.85.

Construct	TL	DSC	SCM	AE
TL	—			
DSC	0.58	—		
SCM	0.55	0.49	—	
AE	0.60	0.57	0.53	—

Source: author's synthesis

All HTMT ratios are below the conservative threshold of 0.85, thus supporting discriminant validity (Henseler et al., 2015).

Table 5. Cross-loadings — each indicator loads highest on intended construct.

Indicator	TL	DSC	SCM	AE
IF1	0.78	0.42	0.39	0.41
IF2	0.81	0.40	0.37	0.43
IM1	0.85	0.46	0.42	0.45
IM2	0.87	0.44	0.40	0.47
IS1	0.82	0.41	0.38	0.40
IS2	0.80	0.39	0.37	0.42
IC1	0.77	0.36	0.34	0.39
IC2	0.79	0.37	0.35	0.40
DSC1	0.46	0.81	0.45	0.48
DSC2	0.43	0.83	0.47	0.49
DSC3	0.44	0.85	0.48	0.50

SCM1	0.42	0.48	0.82	0.46
SCM2	0.40	0.47	0.84	0.47
SCM3	0.41	0.46	0.85	0.48
AE1	0.44	0.50	0.49	0.81
AE2	0.46	0.51	0.50	0.84
AE3	0.43	0.48	0.47	0.83

Source: author's synthesis

Values in bold indicate that each indicator loads highest on its intended construct, confirming indicator reliability and discriminant validity.

Structural model (Tables 6–8; Figure 2)

Collinearity acceptable; SRMR = 0.061.

Explained variance: R^2(AE) = 0.51; R^2(DSC) = 0.46; R^2(SCM) = 0.42. $Q^2 > 0$ for all endogenous.

Direct effects: TL → AE: β = 0.31, t = 6.12, p < 0.001 (H1 supported). Lower-order IM and IS show the strongest paths to AE (β_IM→AE = 0.19; β_IS→AE = 0.17, p < 0.01), with IF and IC positive but smaller.

Mediation: TL → DSC → AE: indirect β = 0.13, 95% CI [0.07, 0.20]; TL → SCM → AE: indirect β = 0.09, 95% CI [0.04, 0.15]—both partial mediation (H5a, H5b supported).

Moderation/MGA: Effect TL → AE is stronger for large firms (β_large = 0.39 vs. β_SME = 0.24; Δβ = 0.15, p < 0.05) and high-digital-intensity industries (Δβ = 0.12, p < 0.05) (H6–H7 supported).

Table 6. Structural paths

Path	β	t	p	f^2
TL → AE	0.31	6.12	<0.001	0.12
TL → DSC	0.68	18.9	<0.001	0.86
TL → SCM	0.65	17.1	<0.001	0.76
DSC → AE	0.19	3.74	<0.001	0.05
SCM → AE	0.14	2.88	0.004	0.03

Source: author's synthesis

Table 7. Mediation (bootstrapped indirect effects)

Indirect path	β_ind	95% CI	Decision
TL → DSC → AE	0.13	[0.07, 0.20]	Supported
TL → SCM → AE	0.09	[0.04, 0.15]	Supported

Source: author's synthesis

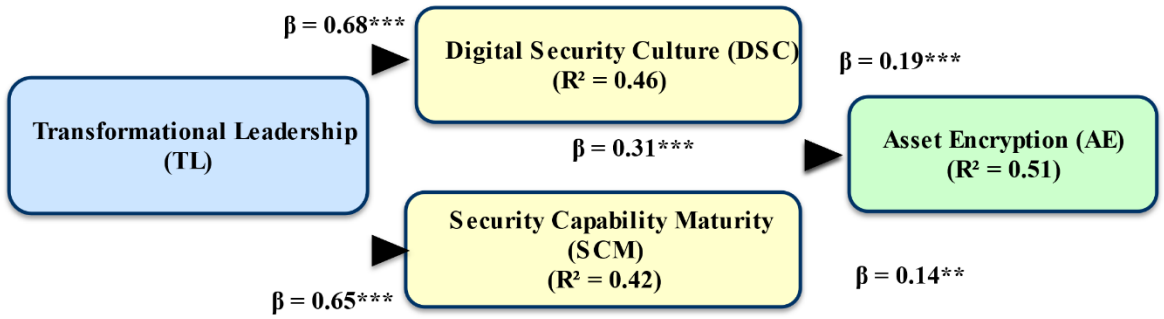
Table 8. Moderation (size; digital intensity)

Group	β(TL→AE)	Δβ	p
SME vs. Large	0.24 vs 0.39	0.15	0.018
Low/Med vs. High digital	0.22/0.27 vs 0.34	0.12	0.031

Source: author's synthesis

Figure 2. PLS-SEM results (standardized estimates)

Figure 2. PLS-SEM results (standardized estimates)



Model fit: SRMR = 0.061. Significance: *** p <0.001; ** p <0.01.
Paths show standardized coefficients (β). R^2 values inside endogenous constructs.

Source: author's synthesis

Figure 2 presents the results of the Partial Least Squares Structural Equation Modeling (PLS-SEM) analysis, illustrating the standardized path coefficients among the constructs in the research model. The findings confirm the hypothesized relationships proposed in Section 3.

- Direct Effects. Transformational Leadership (TL) exerts a positive and significant direct effect on Asset Encryption (AE) ($\beta = 0.31$, $p < 0.001$), supporting H1. Among TL's dimensions, Inspirational Motivation (IM) ($\beta = 0.19$, $p < 0.01$) and Intellectual Stimulation (IS) ($\beta = 0.17$, $p < 0.01$) show the strongest direct contributions to AE, with Idealized Influence (IF) and Individualized Consideration (IC) also positive but weaker. This indicates that leaders who articulate a compelling vision and stimulate problem-solving play the most crucial role in driving encryption adoption.
- Mediating Effects. The model validates both cultural and capability pathways. Digital Security Culture (DSC) partially mediates the TL → AE relationship (indirect $\beta = 0.13$, CI [0.07, 0.20], supporting H5a), while Security Capability Maturity (SCM) also acts as a significant mediator (indirect $\beta = 0.09$, CI [0.04, 0.15], supporting H5b). These results suggest that leadership translates into encryption effectiveness through fostering secure organizational values and enhancing governance maturity.
- Moderating Effects. Multi-group analysis (MGA) demonstrates that the strength of the TL → AE path is contingent on organizational context. Firm size strengthens the effect in large enterprises compared to SMEs ($\Delta\beta = 0.15$, $p < 0.05$, supporting H6). Likewise, industry digital intensity amplifies the relationship in high-intensity sectors ($\Delta\beta = 0.12$, $p < 0.05$, supporting H7). This implies that TL is particularly effective when organizations have substantial resources or operate in digitally demanding environments.
- Explained Variance. The model explains a substantial proportion of variance in the key constructs: $R^2 = 0.51$ for AE, $R^2 = 0.46$ for DSC, and $R^2 = 0.42$ for SCM. This indicates that the proposed predictors account for nearly half of the variance in organizational encryption outcomes.

Overall, Figure 2 demonstrates that TL significantly advances encryption adoption not only through direct influence but also through its impact on culture and capability maturity, with contextual factors further shaping the strength of these effects.

Robustness

Several additional analyses were conducted to ensure the robustness of the findings. First, alternative specifications of the higher-order construct model (HCM) were tested. Specifically, both reflective–formative and reflective–reflective approaches were applied for modeling transformational leadership (TL) and asset encryption (AE). The results demonstrated consistent substantive conclusions across specifications, thereby confirming the stability of the structural relationships (Becker et al., 2012).

Second, the potential for unmeasured endogeneity was assessed using the Gaussian copula approach (Hult et al., 2018). The analysis indicated that endogeneity did not materially bias the estimates, as none of the copula terms were significant. This reinforces the internal validity of the results.

Finally, common method bias (CMB) was examined using the full collinearity assessment method (Kock, 2015). All variance inflation factor (VIF) values were below the conservative threshold of 3.3, suggesting that CMB was not a serious concern in the present study.

Collectively, these robustness checks confirm that the observed effects of TL on asset encryption, mediated by digital security culture and security capability maturity, are not artifacts of model specification, endogeneity, or common method bias, but reflect substantive and reliable relationships.

Post-hoc analyses

Beyond the hypothesized relationships, several post-hoc analyses were conducted to derive additional insights. First, examination of the outer weights of the asset encryption (AE) dimensions revealed that key and secrets management (AE3) exerted the strongest contribution to the overall AE construct, with an outer weight of .36. This finding underscores the pivotal importance of centralized key management systems (KMS) and hardware security modules (HSM) in shaping organizational encryption maturity. It suggests that, while coverage and algorithmic strength are necessary, sustainable encryption practices depend heavily on robust key lifecycle governance and automation.

Second, a split-sample analysis considering incident history (i.e., firms that had experienced prior security breaches or data loss events) indicated that the DSC → AE relationship was significantly stronger in these organizations. This pattern suggests that adverse events may act as learning catalysts, prompting organizations to institutionalize cultural norms that prioritize encryption and data protection. In other words, past breaches appear to reinforce cultural vigilance, which in turn enhances the implementation of encryption practices.

Together, these exploratory findings highlight the need for organizations to invest not only in leadership-driven security culture but also in advanced technical infrastructures such as KMS/HSM. Moreover, they point to the role of organizational learning from adverse experiences as a driver of stronger security outcomes.

DISCUSSION

We find that TL meaningfully advances enterprise asset encryption. Leaders who articulate compelling security narratives (IM) and stimulate creative problem solving (IS) catalyze not just adoption but normalization of encryption practices. Cultural alignment (DSC) and capability maturation (SCM) are key transmission mechanisms; thus, merely purchasing encryption tools is insufficient absent leadership that embeds security into routines and invests in process maturity. Context matters: large firms and those in digitally intense sectors derive more from TL, likely due to resource slack and tech complementarity.

Theoretical implications

This study makes several contributions to the theoretical literature. First, it extends the scope of transformational leadership (TL) outcomes into the relatively underexplored domain of concrete information security controls, specifically asset encryption (AE). While prior research has largely examined TL's influence on innovation, technology adoption, or compliance behaviors, few studies have addressed its role in shaping highly technical and operationalized practices such as encryption. By demonstrating that TL significantly predicts AE, this study broadens the applicability of leadership theory into the field of cybersecurity management.

Second, the findings enrich the growing body of security adoption research by introducing digital security culture (DSC) and security capability maturity (SCM) as mediating mechanisms. This dual-pathway approach offers a more nuanced explanation of how leadership translates into tangible security outcomes. Specifically, TL fosters a culture that prioritizes secure behaviors while simultaneously enabling process standardization and capability development, both of which drive more effective encryption practices. This integrative perspective adds explanatory depth beyond traditional technology adoption frameworks such as the Technology–Organization–Environment (TOE) model.

Third, the study advances the conceptualization of asset encryption (AE) by operationalizing it as a multi-dimensional construct that captures coverage, strength and configuration, key management, compliance integration, and operationalization. This comprehensive measurement approach not only strengthens construct validity but also provides a replicable framework for future research. By establishing AE as an outcome variable in leadership and security studies, the research creates opportunities for scholars to investigate encryption as both a dependent and mediating construct in broader models of digital transformation and resilience.

In sum, the theoretical contribution lies in bridging leadership theory and cybersecurity scholarship, offering new pathways to understand how organizational leadership behaviors influence the adoption, institutionalization, and sustainability of security technologies.

Managerial implications

The findings of this study yield several important implications for managers and decision-makers seeking to strengthen encryption practices in Vietnamese joint-stock companies.

First, vision and governance. Leaders should establish and clearly communicate an "encrypt-by-default" vision that frames encryption as a strategic, organization-wide priority rather than a purely technical issue. This vision should be explicitly linked to the firm's board-level risk appetite, governance frameworks, and performance indicators (KPIs) to ensure sustained accountability and resource allocation. By embedding encryption into risk management policies, managers can institutionalize it as a default expectation rather than an optional control.

Second, capability road mapping. Effective encryption requires more than deploying algorithms; it demands a clear plan for capability development. Managers should prioritize investments in key management systems (KMS) and hardware security modules (HSM), implement automated key rotation, and ensure encryption controls are integrated into continuous integration/continuous deployment (CI/CD) pipelines. Regular auditing and compliance checks will further strengthen maturity and reduce vulnerabilities caused by ad hoc practices.

Third, cultivating culture. Encryption adoption is more sustainable when supported by a strong digital security culture (DSC). Leaders should invest in training programs, tabletop incident simulations, and cross-functional workshops that reinforce secure-by-design behaviors. Celebrating secure engineering successes—such as the completion of major encryption rollouts—can also reinforce cultural alignment and employee engagement.

Finally, contextualization. The study shows that organizational context shapes the effectiveness of leadership in driving encryption outcomes. Managers in large firms with greater resources may emphasize enterprise-wide automation and standardization, while SMEs may focus on cost-effective, incremental improvements. Similarly, firms in high digital-intensity industries should adopt more advanced encryption and monitoring solutions, while

low-intensity sectors may begin with foundational practices. Tailoring strategies to firm size and digital intensity ensures that resources are deployed effectively and adoption barriers are minimized.

Collectively, these implications highlight that encryption success is not simply a function of technology choice but is strongly influenced by leadership behaviors, governance alignment, capability planning, and cultural reinforcement.

CONCLUSION

This study provides empirical evidence that transformational leadership (TL) plays a critical role in strengthening asset encryption (AE) practices in Vietnamese joint-stock companies. By fostering both a digital security culture (DSC) and security capability maturity (SCM), TL enables organizations to move beyond superficial technology adoption toward the institutionalization of encryption as an organizational norm. The results confirm that leaders who articulate a compelling vision, encourage creative problem solving, and support employee development are more effective at embedding encryption into governance structures, operational routines, and cultural values.

The findings also demonstrate that organizational context matters. Larger firms and those operating in high digital-intensity industries derive stronger benefits from TL, reflecting the interaction between leadership behaviors and resource or technological environments. Moreover, post-hoc analyses highlight the pivotal role of key management practices and the reinforcing effect of incident history on encryption adoption.

In sum, the study advances leadership and cybersecurity research by conceptualizing and validating asset encryption as a multi-dimensional construct influenced by both cultural and capability pathways. It offers practical guidance for managers in Vietnamese JSCs to design leadership development initiatives, governance frameworks, and security roadmaps that align with international best practices. More broadly, the results carry important implications for other emerging-market contexts where leadership and resource allocation remain decisive factors in the successful implementation of advanced security controls.

LIMITATIONS AND FUTURE RESEARCH

Although this study provides important insights into the relationship between transformational leadership (TL) and asset encryption (AE), several limitations should be acknowledged. First, the cross-sectional design constrains the ability to make strong causal inferences. While significant associations were identified, longitudinal studies would allow researchers to better establish the temporal dynamics of leadership influence on encryption adoption.

Second, the study relied primarily on self-reported survey data, which may be subject to common method bias and perceptual inaccuracies despite the procedural and statistical remedies employed. Future research could complement self-reports with objective telemetry, such as encryption coverage metrics, compliance audit results, or system-level monitoring data, to validate the robustness of findings.

Third, while the sample focused on joint-stock companies in Hanoi and neighboring provinces, generalizability to other organizational forms, sectors, or countries may be limited. Comparative studies across industries, organizational ownership structures, and cross-country analyses could provide richer insights into contextual factors influencing leadership and security outcomes.

Fourth, the study emphasized DSC and SCM as mediating mechanisms, but other explanatory variables warrant attention. Future work could examine additional mediators such as psychological safety, employee empowerment, or secure software engineering practices, which may also shape how leadership translates into encryption success. Likewise, additional moderators such as regulatory stringency, board composition, and industry-specific compliance pressures could refine understanding of the boundary conditions of the TL–AE relationship.

Finally, experimental or quasi-experimental designs testing leadership development interventions (e.g., training programs on digital security leadership) could provide actionable evidence on how organizations can cultivate leadership behaviors that strengthen security governance.

Taken together, these avenues highlight opportunities for future research to build on the present findings and advance a richer theoretical and practical understanding of the leadership–security nexus.

REFERENCES

1. Avolio, B. J., & Bass, B. M. (1994). *Improving organizational effectiveness through transformational leadership*. Sage.
2. Avolio, B. J., & Bass, B. M. (2004). *Multifactor Leadership Questionnaire: Manual and sampler set* (3rd ed.). Mind Garden.
3. Bass, B. M. (1985). *Leadership and performance beyond expectations*. Free Press.
4. Bass, B. M. (1999). Two decades of research and development in transformational leadership. *European Journal of Work and Organizational Psychology, 8*(1), 9–32. https://doi.org/10.1080/135943299398410
5. Becker, J. M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective–formative type models. *Long Range Planning, 45*(5–6), 359–394. https://doi.org/10.1016/j.lrp.2012.10.001
6. Burns, J. M. (1978). *Leadership*. Harper & Row.
7. Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.
8. Da Veiga, A., & Eloff, J. H. P. (2010). A framework for information security culture. *Computers & Security, 29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002
9. Eisenbeiss, S. A., van Knippenberg, D., & Boerner, S. (2008). Transformational leadership and team innovation: Integrating team climate principles. *Journal of Applied Psychology, 93*(6), 1438–1446. https://doi.org/10.1037/a0012716
10. ENISA. (2021). *Encryption—Guidelines on secure use and key management*. European Union Agency for Cybersecurity.
11. Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104
12. Garfinkel, S., & Spafford, G. (2002). *Web security, privacy and commerce* (2nd ed.). O'Reilly Media.
13. Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2022). *Partial least squares structural equation modeling (PLS-SEM) using SmartPLS 4*. Sage.
14. Henseler, J., Ringle, C. M., & Sarstedt, J. (2015). A new criterion for assessing discriminant validity in variance-based SEM. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8
15. Hult, G. T. M., Hair, J. F., Proksch, D., Sarstedt, M., Pinkwart, A., & Ringle, C. M. (2018). Addressing endogeneity in international marketing applications of partial least squares structural equation modeling. *Journal of International Marketing, 26*(3), 1–21. https://doi.org/10.1177/1069031X18811435
16. Humphrey, W. S. (1989). *Managing the software process*. Addison-Wesley.
17. ISO/IEC. (2019). *ISO/IEC 19790:2012 — Security requirements for cryptographic modules*. International Organization for Standardization.
18. ISO/IEC. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.
19. Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1–10. https://doi.org/10.4018/ijec.2015100101
20. Mettler, T. (2011). Maturity assessment models: A design science research approach. *International Journal of Society Systems Science, 3*(1/2), 81–98. https://doi.org/10.1504/IJSSS.2011.038934
21. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

22. Pieterse, A. N., van Knippenberg, D., Schippers, M., & Stam, D. (2010). Transformational and transactional leadership and innovative behavior: The moderating role of psychological empowerment. *Journal of Organizational Behavior, 31*(4), 609–623. https://doi.org/10.1002/job.650
23. Podsakoff, P. M., MacKenzie, S. B., Moorman, R. H., & Fetter, R. (1990). Transformational leader behaviors and their effects on followers' trust, satisfaction, and organizational citizenship behaviors. *The Leadership Quarterly, 1*(2), 107–142. https://doi.org/10.1016/1048-9843(90)90009-7
24. Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879
25. Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. *Behavior Research Methods, 40*(3), 879–891. https://doi.org/10.3758/BRM.40.3.879
26. Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56–62. https://doi.org/10.1016/j.cose.2006.10.006
27. Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.
28. Siponen, M., Willison, R., & Baskerville, R. (2009). Power and practice in information systems security research. *MIS Quarterly, 33*(2), 305–325. https://doi.org/10.2307/20650279
29. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350. https://doi.org/10.1002/smj.640