The Influence of Information Security Management and Digital Intensity on Firm Performance in Thai Listed Companies

Kanoknate Prempree[1] and Patsakorn Singto[2]*

[1]Department of Accounting, Faculty of Business Administration, Rajamangala University of Technology Rattanakosin, Bangkok, 10100, Thailand

[2]Department of Business Information Technology, Faculty of Business Administration, Rajamangala University of Technology Rattanakosin, Bangkok, 10100, Thailand

* Corresponding author. E-mail address: patsakorn.s@rmutr.ac.th

Received: 21 November 2025; Revised: 19 February 2026; Accepted: 20 March 2026; Available online: 23 March 2026

Abstract

The adoption of digital technologies in organizational processes varies according to strategic objectives, while simultaneously introducing potential risks and security vulnerabilities. Consequently, effective information and technology security management has become increasingly critical. In parallel, organizations that recognize the strategic value of digital technologies are more likely to invest appropriately in technological resources to enhance performance and sustain long-term organizational competitiveness. This study aims to (1) examine the effect of information security management on firm performance, (2) investigate the influence of digital intensity on firm performance, and (3) explore the impact of perceived digital usefulness on digital intensity. A structured questionnaire was employed as the primary data collection instrument. The sample comprised 768 firms listed on the Stock Exchange of Thailand, from which 191 valid responses were obtained, representing a response rate of 24.87%. The results indicate that information security management positively influences firm performance ($p < .05$), digital intensity has a significant positive effect on firm performance ($p < .01$), and perceived digital usefulness positively affects digital intensity ($p < .05$). These findings suggest that firms with well-established information security management systems are more likely to achieve superior performance outcomes. In addition, organizations that perceive digital technologies as beneficial tend to adopt a broader range of digital tools and integrate them more deeply into operational processes, thereby improving efficiency and strengthening overall firm performance. Collectively, the results highlight the strategic role of digital capability and security governance in driving organizational value creation.

Keywords: Information Security Management, Digital Intensity, Perceived Digital Usefulness, Firm Performance, Thai Listed Companies

Introduction

Recently in Thailand, national digital development initiatives and institutional frameworks promoting technology utilization have encouraged firms to integrate digital systems into core business processes in order to remain competitive in an increasingly technology-intensive environment (Digital Economy Promotion Agency, 2022). These policy and market forces have led organizations—particularly medium- and large-scale enterprises—to invest extensively in digital technologies such as enterprise systems, cloud infrastructure, artificial intelligence, analytics platforms, and integrated digital services over the past five years. According to National Statistics, the magnitude and pace of this transformation. According to the Digital Economy Promotion Agency, Thailand's digital industry has expanded markedly, with total industry value growth increasing from approximately 3.88% in 2023 to 23.35% in 2024 (Digital Economy Promotion Agency, 2023). These figures indicate that digital transformation in Thailand is not incremental but structural, reflecting the rapid integration of digital technologies across software, digital services, and hardware sectors. Such expansion

demonstrates that digital capabilities are increasingly embedded within organizational operations and strategic decision-making, thereby amplifying both opportunities for value creation and exposure to cyber-related risks. Digital transformation has become a defining structural force reshaping organizational competitiveness, strategic management, and value creation in contemporary economies. Government-driven digital economy policies, together with rapidly evolving consumer behavior toward online platforms, mobile services, and data-driven interactions, have accelerated digital adoption across industries worldwide. For Thailand's economy, publicly listed firms generate substantial economic value and exert systemic influence on national markets; their digital transformation trajectories are of particular strategic importance. However, while digitalization creates opportunities for innovation, efficiency, and growth, it simultaneously exposes firms to new categories of risk, especially cybersecurity threats, operational disruptions, reputational damage, and data governance challenges. In response, firms implement structured information security management practices—such as access control policies, risk management procedures, data protection protocols, and continuous monitoring systems—to safeguard digital assets.

As discussed above, firms respond to digital transformation by investing in advanced technologies and strengthening information security management practices. At the same time, organizations operate under the fundamental objective of enhancing economic value and achieving long-term sustainability. Within this strategic context, a critical research question emerges: to what extent do digital transformation investments, together with cybersecurity safeguards, contribute to measurable firm performance? Prior research has consistently highlighted the strategic significance of digital technologies, though findings vary across national contexts and methodological approaches. Goi et al. (2023), using survey data from firms in Eastern European markets, found that digital technology adoption enhances strategic management effectiveness by improving information transparency, decision speed, and coordination efficiency. Lee et al. (2021), employing multiple case studies across low- and high-technology industries in Malaysia, identified leadership support, technological readiness, and organizational competence as critical drivers of successful digital adoption, emphasizing that transformation outcomes depend heavily on organizational capabilities rather than technology alone. Similarly, Nwankpa and Datta (2017), drawing on combined survey and archival data from firms in developed economies, demonstrated that Digital Business Intensity positively influences perceived organizational performance when firms effectively balance exploratory and exploitative uses of information technology resources. Collectively, these studies confirm that digital technologies can enhance organizational outcomes, yet they also reveal important limitations in the existing literature. First, most prior studies examine digital adoption, technological capability, or strategic performance as separate constructs rather than as interrelated components of an integrated performance framework. Second, empirical evidence has been concentrated largely in developed or technologically advanced economies, leaving emerging market contexts comparatively underexplored. Third, although digital integration increases organizational exposure to cyber risks, relatively few studies incorporate governance mechanisms such as information security management into models explaining firm performance. Consequently, while existing scholarship recognizes that digital technologies influence organizational outcomes, there remains limited empirical understanding of how technological integration and structured security governance jointly shape economic value creation. This gap is particularly evident in the context of publicly listed companies in emerging economies such as Thailand. Firms listed on the Stock Exchange of Thailand generally exhibit higher levels of digital maturity, more advanced technological infrastructure, and stricter governance requirements than smaller enterprises. They

also face elevated cyber risk exposure due to their visibility, asset scale, and regulatory obligations. These characteristics make the listed firms an especially relevant empirical setting for examining whether digital intensity and information security management function as complementary strategic capabilities that enhance performance outcomes.

To resolve the research question, drawing on the Resource-Based View (Barney, 1991), this study conceptualizes Information Security Management (ISM) as an intangible strategic capability that strengthens the value derived from digital investments. Rather than treating ISM as a purely compliance-oriented function, RBV suggests that well-developed security governance structures may constitute firm-specific resources that are valuable, rare, and difficult to imitate. At the same time, Digital Intensity is conceptualized through an integration-depth framework, capturing the extent to which digital technologies are embedded across organizational processes. By integrating RBV with insights from the Technology Acceptance Model (Davis, 1989), this study further examines how perceived usefulness of digital technologies contributes to higher levels of digital intensity, thereby linking managerial cognition with firm-level strategic capability formation. Accordingly, the objectives of this research are twofold: first, to examine the influence of Information Security Management and Digital Intensity on firm performance among companies listed on the Stock Exchange of Thailand; and second, to investigate the relationship between perceived usefulness of digital technologies and digital intensity. Using survey data from listed firms analyzed through regression and ANOVA techniques, this study seeks to provide empirical evidence on the mechanisms through which digital capability and governance discipline contribute to organizational value creation. This research makes several contributions. Theoretically, it advances digital transformation scholarship by integrating ISM and Digital Intensity within a single performance model, addressing the absence of empirical studies that examine these constructs jointly. It also extends RBV by demonstrating that information security management can function as a strategic resource that enhances firm performance in digitally intensive environments. Furthermore, by linking perceived usefulness to digital integration, the study broadens technology adoption theory beyond individual-level behavioral intention to encompass organization-level capability development. From a managerial perspective, the findings suggest that digital investment alone is insufficient to generate sustainable performance gains; organizations must align technological integration with structured security governance and managerial recognition of digital value. By focusing on Thai listed companies, this study provides nuanced, context-specific evidence from an emerging market. These findings offer critical insights for policymakers and executives navigating digital transformation within rapidly evolving institutional frameworks.

Information Security Management

Information security management is critical for organizations that utilize digital technologies in their operations, as such firms accumulate substantial volumes of sensitive data, including customer information, intellectual property, and strategic assets that support operational capability and competitive advantage. Information security management refers to the systematic process of protecting vital information and related systems from internal and external threats. Its core objectives consist of three dimensions: (1) confidentiality, which ensures that data are accessible only to authorized users; (2) integrity, which safeguards information from unauthorized alteration or damage; and (3) availability, which guarantees that authorized users can access systems and retrieve data when required (Yee & Zolkipli, 2021). Implementing robust data security measures not only prevents potential damage arising from security breaches but also generates organizational benefits,

including regulatory compliance, enhanced reputation, stakeholder trust, minimized financial loss from data theft, reduced operational disruption, and lower system recovery costs. A widely recognized framework for managing information security is the Information Security Management System (ISMS), particularly the ISO/IEC 27001 standard, which provides structured procedures for identifying, assessing, and mitigating risks associated with data security incidents (Nowicka et al., 2024). Effective implementation requires a comprehensive governance approach encompassing strategic policy formulation by top management, risk assessment frameworks, technological investment, employee training, and continuous monitoring of security practices. Prior empirical evidence indicates that top management support is a critical determinant of effective information security governance (Pigola et al., 2025).

Digital Intensity

The adoption of digital technologies varies across organizations in both scope and depth. Some firms integrate digital technologies across all operational units, whereas others deploy them selectively within specific departments. The level of digital adoption depends on organizational characteristics, strategic objectives, and technological readiness. Prior research has attempted to classify organizations according to their degree of digital intensity. Indicators commonly used include investment in digital hardware and software, procurement of information and communication technology (ICT) products and services, utilization of robotics, number of ICT specialists, and proportion of sales conducted through online channels. Based on such indicators, organizations have been categorized into four levels of digital intensity: low, medium-low, medium-high, and high (Calvino et al., 2018). Similarly, another study assessed digital intensity among European firms using indicators such as business internet usage, enterprise resource planning (ERP) adoption, online sales, Internet of Things (IoT) applications, social media utilization, customer relationship management (CRM) systems, cloud computing, and artificial intelligence implementation. Firms were classified into four categories: very low, low, high, and very high digital intensity (European Union, 2022). More broadly, digital intensity can be defined as the extent to which organizations invest in and utilize digital technologies—including analytics, big data, cloud platforms, social media, and mobile technologies—to enhance organizational capabilities and strengthen competitiveness (Nwankpa & Datta, 2017).

Perceived Digital Usefulness

Perceived usefulness is defined as the degree to which an individual believes that using a particular system enhances job performance (Davis, 1989). The adoption of digital technologies provides multidimensional benefits for organizations. Firms increasingly leverage digital tools to achieve competitive advantage, improve operational efficiency, streamline business processes, enhance communication effectiveness, reduce marketing costs, increase productivity, accelerate revenue growth, and expand into global markets (Goi et al., 2023). Prior studies consistently demonstrate that digital adoption improves operational efficiency and effectiveness. For instance, the use of financial technology applications and digital marketing platforms among small and medium-sized enterprises has been shown to reduce operational time and costs while improving customer service quality (Saleh et al., 2025). Similarly, the implementation of enterprise resource planning and supply chain management systems enhances financial performance (Fauzi, 2021). Digital twin technologies applied in product design enable large-scale customer data analysis, facilitating faster product development cycles and reducing both time and cost (Lo et al., 2021). In addition, customer relationship management systems contribute to increased

customer loyalty (Khan et al., 2020). Collectively, these findings suggest that when organizations perceive digital technologies as useful, they are more likely to adopt and integrate them into business processes.

Firm Performance

Firm performance, influenced by a combination of internal and external variables, is typically evaluated by the degree to which a company achieves its set strategic targets (Fauzi, 2021). Performance can be assessed using both qualitative and quantitative indicators (AlMulhim, 2021). Common performance measures include profitability and market value (Nwankpa & Datta, 2017). Within the context of digital transformation, performance indicators are generally categorized into financial and non-financial dimensions (Jongwanich & Kohpaiboon, 2024). Financial indicators include revenue growth, operating cost reduction (Kahrovic & Avdovic, 2023), net profit and operating profit (Nasiri et al., 2022), return on investment and market capitalization (Kang et al., 2022), as well as earnings and sales growth (AlMulhim, 2021). Non-financial indicators include market share, customer satisfaction, employee satisfaction, productivity, digital market expansion, platform utilization, and digital product development (AlMulhim, 2021; Kahrovic & Avdovic, 2023). Operational outcomes such as cost efficiency, processing speed, and service quality represent key performance indicators (Saleh et al., 2025). Furthermore, outcomes from digital utilization may be classified into four dimensions: process efficiency, employee outcomes, customer outcomes, and financial value creation (Marcolivio & Wade, 2023).

To contextualize the present study within the existing literature, Table 1 systematically compares the variables and principal findings of relevant prior research.

Table 1 Previous research

Authors	Variable	Results
AlMulhim (2021)	Digital transformation. Smart technology. Performance.	Digital transformation encourages using smart technology. Smart technology enhances the positive relationship of digital transformation and performance.
Bolodeoku et al. (2022)	Perceived usefulness of technology. Employee satisfaction. Employee productivity.	A higher level of perceived usefulness of technology contributes to improved employee satisfaction and productivity.
Fauzi (2021)	Using enterprise resource planning (ERP systems). Financial performance. Non-financial performance.	Implementing an ERP system positively affects a firm's financial and non-financial performance.
Goi et al. (2023)	Digital transformation. Digital investment. Strategic priorities. Operation efficiency. Competitiveness.	The adoption of technology drives strategic transformation in organizational operations and resource management, thereby fostering sustainable competitive advantages.
Jiang et al. (2025)	Digital technology adoption. Enterprise investment efficiency.	Digital technology adoption enhances enterprise investment efficiency.
Jongwanich and Kohpaiboon (2024)	ICT adoption. ICT depth. Financial performance; income, profits.	ICT adoption positively impacts on financial performance. ICT depth more positive impacts on income than profits.

Table 1 (Cont.)

Authors	Variable	Results
Kahrovic and Avdovic (2023)	Digital technology. Firm performance.	The adoption of digital technology positively affects firm performance.
Kang et al. (2022).	Information security intellectual property. Firm performance.	Information security intellectual property is positively related to firm performance in term of return on investment and market capitalization.
Kashada et al. (2018)	Perceived usefulness. Perceived of ease of use. User awareness. Information technology infrastructure. Top management support. Digital Learning Technology adoption (DLT).	User awareness, perceived usefulness, and perceived ease of use had a positive significant indirect effect on successful adoption of the digital learning technology adoption through their impact on top management support. Information technology infrastructure showed a positive significant direct effect on the successful adoption of the DLT.
Khan et al. (2020)	Using customer relationship management. Company reputation. Customer loyalty.	Customer relationship management such as communication, service and customer trust, and company reputation positively impact customer loyalty.
Kong et al. (2015)	Information security activities. Service transaction stability. Organizational performance.	An increasing of information security activities results higher service transaction stability and leading more organizational performance.
Kongsumpao (2024)	Perceive of usefulness. Perceive of ease. Perceive of risk. Operational efficiency.	Perceive of usefulness, perceive of ease, and perceive of risk have positive impact on operational efficiency of electronic tax system in the revenue department of Thailand.
Lo et al. (2021)	Digital twin. Product design and development.	Digital twin provides a real time information and in-dept data that increase the efficient of design and developing product, production, and innovation.
Moshi et al. (2024)	Perceived usefulness. Perceived ease of use. Awareness. Big data adoption readiness.	Awareness of big data is the main driver for perceived usefulness and perceived ease of use. Ease of use and usefulness are essential predictors of big data adoption readiness. Perceived usefulness is the core determinants of big data adoption readiness.
Nwankpa and Datta (2017)	Digital business Intensity. Performance.	The digital business intensity has positive influence on performance.
Nasiri et al. (2022)	Digital orientation. Digital intensity. Digital maturity. Performance.	The digital maturity which are the continuous improvement of technology encourage the positive relationship between the digital intensity and performance.
Saleh et al. (2025)	Digital technology adoption level (Digital payment, Fintech application, Digital marketing). Operational efficiency (Cost reduction, Time efficiency improvement, Customer service quality improvement).	The level of digital technology adoption has a positive relationship with operational efficiency. Digital payment systems, fintech applications, and digital marketing positively affect operational efficiency.

Table 1 (Cont.)

Authors	Variable	Results
Sudaryanto et al. (2023)	Perceived usefulness. Perceived ease of use. Digital competence. Technology readiness. Technology adoption.	Perceived usefulness and perceived ease of use is positively relative technology adoption. Technology readiness and digital competence do not significantly affect technology adoption.
Tewamba et al. (2019).	Information security management system. IT capability. Firm Performance	Information security management system has positively effects on performance. Information security management system has positively impact on performance through IT capability.

Research Model

Based on the preceding literature review, the conceptual framework guiding this study is presented in Fig. 1. The model proposes that Information Security Management (ISM) and Digital Intensity (DI) influence Firm Performance (FP), while Perceived Digital Usefulness (PDU) affects Digital Intensity

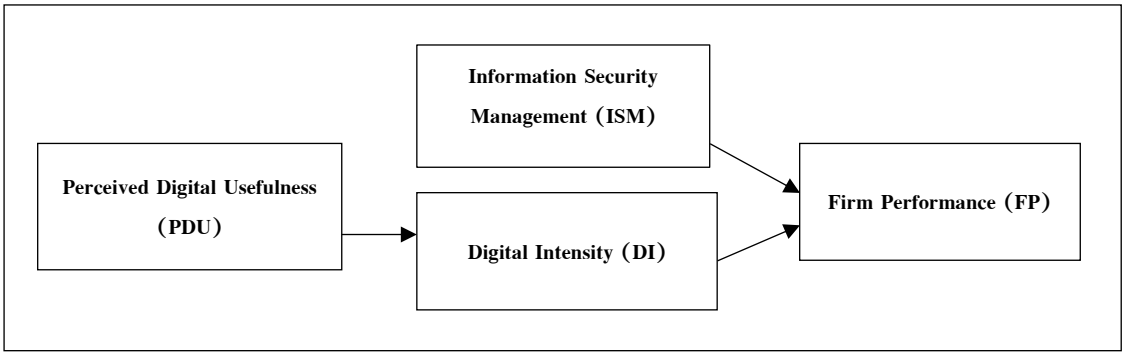

Figure 1 Research Model

Hypotheses Development

Information Security Management and Firm Performance

The adoption of digital technologies and the storage of information as a strategic organizational resource increase exposure to data security risks, particularly concerning financial data and stakeholder information. Effective information security management is therefore essential for mitigating cyber threats and preventing negative impacts on firm performance. Well-implemented ISM enhances business continuity, strengthens stakeholder trust, reduces potential financial losses, and ultimately improves organizational performance. From a Resource-Based View perspective, ISM can be conceptualized as an intangible strategic capability that functions as a valuable organizational resource enhancing firm performance. Empirical evidence supports this view. For instance, Kong et al. (2015) found that effective ISM improves service transaction stability and enhances firm performance. Likewise, Kang et al. (2022) demonstrated that protecting intellectual property through information security practices positively influences organizational performance. Accordingly, the following hypothesis is proposed:

Hypothesis 1: Information security management positively influences firm performance.

Digital Intensity and Firm Performance

The implementation of digital technologies across business operations enhances efficiency by reducing costs, shortening processing time, improving responsiveness, and increasing customer satisfaction, thereby contributing to superior firm performance. Previous research consistently shows that digital adoption improves organizational efficiency and employee satisfaction (Goi et al., 2023). Empirical evidence suggests that the integration of smart technologies serves as a critical driver for enhancing firm performance (AlMulhim, 2021). In addition, the use of social networks, robotics, cloud computing, and artificial intelligence contributes to improved financial outcomes and operational efficiency (Kahrovic & Avdovic, 2023). Empirical evidence further indicates that higher levels of digital intensity directly enhance firm performance (Nwankpa & Datta, 2017), and that this positive effect is strengthened when organizations continuously upgrade digital capabilities (Nasiri et al., 2022). Moreover, enterprise resource planning implementation has been shown to improve both financial and non-financial performance outcomes (Fauzi, 2021). Therefore, the following hypothesis is proposed:

Hypothesis 2: Digital intensity positively influences firm performance.

Perceived Digital Usefulness and Digital Intensity

The adoption of digital technologies depends not only on infrastructure readiness but also on users' perceptions of their usefulness. According to the Technology Acceptance Model, performance expectancy—defined as the belief that technology use enhances job performance—is a key determinant of both intentions to use and actual technology usage behavior (Venkatesh et al., 2003). Prior research indicates that perceived usefulness positively influences the adoption of digital learning technologies, particularly when supported by top management (Kashada et al., 2018). Similarly, studies in accounting education show that perceived usefulness increases adoption of artificial intelligence tools (Sudaryanto et al., 2023). Evidence from public sector auditing further demonstrates that perceived usefulness drives readiness to adopt big data technologies (Moshi et al., 2024). These findings suggest that perceived usefulness plays a pivotal role in facilitating digital adoption. Therefore, the following hypothesis is proposed:

Hypothesis 3: Perceived digital usefulness positively influences digital intensity.

Materials and Methods

Population and samples

The population of this study comprised firms across multiple industries listed on the Stock Exchange of Thailand (SET). Listed firms were selected because they are typically medium- to large-sized enterprises with substantial capacity to invest in digital technologies and because they represent diverse industry sectors, thereby supporting broader inference within the listed-firm context. The population frame was obtained from the official SET registry, which listed 913 firms at the time of sampling. The required sample size was determined using Cochran's (1977) formula for continuous data: $n = (Z^2_{\alpha} S^2)/e^2$(Cochran, 1977). A 95% confidence level was adopted ($Z = 1.96$). Following common practice in survey planning, the variance parameter was expected as $S^2=2$, and the expected mean was set at 2 for precision planning. The acceptable margin of error was defined as 5% of the assumed mean, yielding $e=0.10$. Substituting these parameters produced a required sample size of $n = (1.96)^2(2)/(0.10)^2 = 768$. Accordingly, 768 firms were selected for data collection. A probability

sampling approach was applied using simple random sampling with a random number table. Questionnaires were distributed to all sampled firms.

Data collection

A structured questionnaire was employed as the primary data collection instrument. The designated key informants were directors or managers of information technology (IT) departments. A single-informant research design, in which IT directors or senior IT managers served as organizational representatives, was adopted to obtain firm-level measures of Information Security Management (ISM), Digital Intensity (DI), and Firm Performance (FP). This approach is justified by the strategic role of chief information officers and senior IT executives—referred to in this study as IT directors—who are responsible for aligning digital initiatives with organizational objectives, ensuring compliance requirements, and creating value through technology-enabled transformation. These executives typically participate in strategic planning, lead cross-functional coordination, and oversee technology investment decisions. Moreover, by engaging in board-level discussions, they help direct the governance processes that drive strategic development and stakeholder-focused value delivery (Aguilar Alonso et al., 2009). Given their involvement in strategy and reporting, IT leaders possess the holistic insight required to assess digital security governance and implementation outcomes. They are thus ideally situated to offer informed perspectives on firm-level digital performance. A total of 768 questionnaires were distributed via postal mail. Data collection was conducted over two months from April to May 2024. In total, 191 questionnaires were returned and verified as complete and usable for analysis, resulting in a response rate of 24.87%.

Measurement

All constructs were measured using a five-point Likert-type scale, where 1 indicates the lowest level, and 5 indicates the highest level of agreement or extent. Measurement items were adapted from prior studies and refined to fit the Thai business context. Table 2 presents the operational definitions and measurement indicators for each variable.

Table 2 Operational definition and measurement

Variable	Operational definition	Measurement indicators	Reference
Perceived Digital Usefulness	Organization perceives the efficiency and effectiveness of business activities derived from the utilization of digital technology contribute to enhancing organizational success.	Improve decision-making, improve collaboration and communication, real-time tracking. Improve data accessibility from anywhere and at any time. Automate tasks and processes. Minimize human error. Better understand of customer requirement, more direct interfaces with customers, Increased productivity.	Garg et al. (2024)
Digital Intensity	The degree of technological investment and the diversity of digital adoption within organizational processes.	The investment in hardware and software. The expenses of technology services and supplies. Number of technological in business process.	Calvino et al. (2018); European Union (2022)

Table 2 (Cont.)

Variable	Operational definition	Measurement indicators	Reference
		Automation systems facilitate interdepartmental integration within organizations. Automated information exchange and linkage with business partners. Number of information technology professional.	
Information Security Management	Protecting sensitive data and information systems from internal and external threats.	Access control by investigated right accessing network. Permission level of accessing information system. Installation of updated security software. Password standard form is strong and unique for high security.	National Institute of Standards and Technology (2020)
Firm Performance	An achievement of firm objectives and goal both financial and non-financial.	Efficient business processes: reduce time, cost, resource, and error; rapidly response to the problem; improved time to develop and launch a new product. Employee satisfaction: flexible time and workplace. Customer satisfaction: increasing new customer; customer repurchased. Financial value added: total revenue increasing; online revenue increasing.	Marcolivio and Wade (2023)

Instrument Validity and Reliability

Measurement quality was evaluated in terms of validity and reliability. Convergent validity was assessed using factor loadings to verify the extent to which indicators of each construct captured the same underlying concept. Factor loadings of 0.60 or higher indicate adequate convergent validity (Hair et al., 2010). Construct reliability was verified using Cronbach's alpha to assess internal consistency. This measure ensured that items within each construct were homogeneous and consistently captured the intended underlying theoretical concepts. Cronbach's alpha values exceeding 0.70 are generally considered acceptable, indicating satisfactory reliability (Hair et al., 2010). As reported in Table 3, all factor loadings met or exceeded 0.60, supporting convergent validity. Cronbach's alpha values for all constructs were at least 0.70, indicating acceptable reliability. Overall, the instrument demonstrated adequate measurement quality for subsequent statistical analyses.

Table 3 Validity and Reliability of Measurement

Variables	Number of Items	KMO	Factor loading	Cronbach's Alpha
ISM	5	.81	.65 - .88	.83
DI	6	.86	.76 - .88	.89
PDU	5	.73	.68 - .76	.75
FP	8	.78	.64 - .81	.78

Data Analysis Techniques

Data analysis proceeded in several stages. First, Pearson correlation analysis was conducted to examine bivariate relationships among study variables. Second, regression analyses were performed to test the hypothesized relationships: ISM and DI predicting FP (H1–H2), and PDU predicting DI (H3). Third, hierarchical cluster analysis (Ward's method) was used to classify firms into digital intensity groups. Finally, one-way ANOVA was conducted to compare firm performance across the identified digital intensity clusters, providing robustness checks for the DI–FP relationship.

Results

Data Screening and Assumption Testing

The study employed Pearson correlation and regression analysis. From the 768 sampled firms, 191 responses were obtained (24.87%). Before regression analysis, the dataset was screened for outliers using box plots of residuals. Four outlying observations were detected and removed to reduce the risk of model distortion (Kutner et al., 2008), resulting in a final analytical sample of 187 observations for assumption testing and inferential analysis. Regression assumptions were assessed as follows. First, normality of residuals was examined using the Kolmogorov–Smirnov test, yielding a statistic of 0.065 with $p > .5$, indicating no evidence of non-normality (Vanichbuncha, 2010). Second, multicollinearity was evaluated using variance inflation factors (VIF). All VIF values were below 10, suggesting no serious multicollinearity (Hair et al., 2010). Third, homoscedasticity was assessed using the Brown–Forsythe test, which yielded a statistic of 0.068 with $p > .5$, supporting constant error variance (Kutner et al., 2008). Finally, linearity was evaluated by plotting residuals against predicted values, showing residual dispersion approximately parallel to the horizontal axis, consistent with linear relationships (Kutner et al., 2008).

Correlation Analysis

As shown in Table 4, ISM and DI were positively and significantly correlated with FP at the 0.01 level. In addition, PDU exhibited a positive and statistically significant correlation with DI at the 0.05 level.

Table 4 Correlation analysis

Variable	ISM	DI	PDU	FP
ISM				
DI	.123			
PDU	.310**	.149*		
FP	.235**	.576**	.543**	
$\bar{X}$	4.48	2.92	4.22	3.71
S.D.	.55	.85	.52	.53

* $p < .05$, ** $p < .01$

Hypothesis Testing

H1–H2: ISM and DI ⟶ Firm Performance. To test Hypotheses 1 and 2, firm performance was regressed on ISM and DI.

Table 5 The influence of Information Security Management and Digital Intensity on Firm Performance

Dependent variable	Unstandardized Coefficients		Standardized Coefficients	t	p-value
	b	Std. Error	β		
Constant	1.967	.270	-	7.273	< .01
ISM	.162	.058	0.166	2.801	< .05
DI	.348	.037	0.556	9.354	< .01
Dependent variable: Firm performance					
R^2 = .36, Adjust R^2 = .353, Model sig. < .01					

The overall model was statistically significant ($p < .01$) and produced an adjusted R^2 of 0.353, indicating that ISM and DI jointly explain 35.3% of the variance in firm performance. This level of explanatory power is substantial for survey-based organizational research and suggests meaningful predictive relevance.

As reported in Table 5, ISM had a positive unstandardized coefficient (b = 0.162, $p < .05$), Hypothesis 1 is supported. DI also had a positive unstandardized coefficient (b = 0.348, $p < .01$), Hypothesis 2 is supported. In terms of relative effect strength, the standardized coefficients indicate that DI ($\beta = 0.556$) exerts a stronger positive influence on firm performance than ISM ($\beta = 0.166$). This pattern implies that deeper integration of digital technologies is a dominant driver of performance gains among Thai listed firms, while ISM provides an additional, statistically significant contribution.

H3: Perceived Digital Usefulness ⟶ Digital Intensity. To test Hypothesis 3, digital intensity was regressed on perceived digital usefulness.

Table 6 Relationship between Perceived Digital Usefulness and Digital Intensity

Dependent variable	Unstandardized		Standardized Coefficients	t	p-value
	b	Std. Error	β		
Constant	1.890	.509	-	3.717	< .01
PDU	.245	.120	.149	2.047	< .05
Dependent variable: Digital intensity					
R^2 = .022, Adjust R^2 = .017, Model sig. < .05					

The model was statistically significant ($p < .05$) and yielded $R^2 = 0.022$, indicating that PDU explains 2.2% of the variance in digital intensity. Although the explanatory power is modest, small R^2 values are common in social science research when behavioral or perceptual predictors are used and when outcomes are influenced by multiple unobserved factors (Helland, 1987; Ozili, 2022). Importantly, the objective of this analysis was to test whether PDU is a statistically meaningful predictor of DI, rather than to maximize predictive variance.

As shown in Table 6, PDU had a positive unstandardized coefficient (b = 0.245, $p < .05$), indicating that higher perceived usefulness is associated with higher digital intensity. Therefore, Hypothesis 3 is supported.

Additional Analysis: Cluster Analysis and ANOVA

To provide further evidence for the DI-FP relationship and align additional analyses with the research objectives, cluster analysis and ANOVA were conducted.

Observations were classified into digital intensity groups using hierarchical cluster analysis (Ward's method), based on the indicator "investment in equipment and software." The 187 observations were classified into four groups representing distinct digital intensity levels, as shown in Table 7.

Table 7 Digital intensity groups

Digital intensity group	Mean of Digital intensity	Number of cases	%
High	4.29	17	9.09
Middle-High	3.46	63	33.69
Low-Middle	2.87	52	27.81
Low	1.93	55	29.41
Total		187	100

Table 8 Result of One-way ANOVA analysis

	Digital intensity group				F-statistic	p-value
	High	Middle-High	Low-Middle	Low		
FP	4.38	3.85	3.68	3.38	27.177	< .01

A one-way ANOVA was performed to examine whether firm performance differs across these groups. The results indicate statistically significant differences in mean firm performance across the four digital intensity clusters ($p < .01$). Specifically, firms with high digital intensity exhibited the highest mean performance (M = 4.38), followed by medium-high (M = 3.85), low-medium (M = 3.68), and low digital intensity (M = 3.38). These results provide convergent support for the regression findings, strengthening confidence that higher digital intensity is associated with superior firm performance.

Discussion

The findings of this study both confirm and extend existing scholarship on digital transformation and firm performance. Consistent with prior empirical research, the results demonstrate that Information Security Management (ISM) significantly enhances organizational performance. This supports earlier findings by Tewamba et al. (2019) and Pigola et al. (2025), who showed that effective information security systems contribute to overall organizational outcomes through coordinated technical, human, and organizational mechanisms. Likewise, the present results corroborate Kang et al. (2022), who reported that intellectual property-related information security strengthens firm performance by safeguarding strategic assets and enabling value creation. Similarly, the positive relationship between Digital Intensity and firm performance aligns with studies indicating that deeper digital integration is associated with superior organizational outcomes (Nwankpa & Datta, 2017; Nasiri et al., 2022; AlMulhim, 2021; Fauzi, 2021). These studies collectively suggest that the adoption of digital technologies—such as ERP systems, data analytics, AI, cloud computing, and digital platforms—enhances operational efficiency, reduces costs, accelerates processes, and improves revenue generation. The present findings reinforce this perspective by demonstrating that digital technologies embedded in business processes yield performance benefits. However, beyond confirming prior research, this study extends the literature in several meaningful ways. Previous studies typically examined digital capability or information security independently, whereas this research integrates ISM and Digital Intensity within a single explanatory

framework. This unified modeling approach reveals their relative strategic influence and indicates that digital transformation outcomes are shaped not merely by technology adoption but by the interaction between technological intensity and ISM capability. The stronger standardized effect observed for Digital Intensity suggests that performance gains arise when digital technologies are systematically embedded across organizational functions rather than adopted in isolated or superficial ways. In addition, the study advances technology adoption research by empirically linking the perceived usefulness of digital technology to organizational-level outcomes through Digital Intensity. Earlier work grounded in technology acceptance theory primarily focused on individual behavioral intention or adoption readiness (Kashada et al., 2018; Moshi et al., 2024; Sudaryanto et al., 2023). By contrast, the present findings demonstrate a sequential mechanism in which perceived digital usefulness enhances digital intensity, which in turn improves firm performance. This progression broadens the explanatory scope of adoption theory from individual cognition to strategic organizational capability formation.

The findings must also be interpreted within the institutional and technological context of publicly listed firms in Thailand. Recently, Thailand has undergone rapid digital expansion supported by national digital economy initiatives, infrastructure investment, and increasing technological penetration across industries. Yet this rapid digitalization has also increased organizational exposure to cyber risks, including data breaches, ransomware attacks, and operational disruptions. Within such an environment, information security management becomes more than a technical safeguard—it functions as a strategic mechanism for managing cyber risk and preserving organizational legitimacy. Listed companies operate under stringent disclosure requirements, corporate governance standards, regulatory oversight, and stakeholder accountability expectations. Compliance with data protection and cybersecurity regulations places additional emphasis on structured information security practices. Under these conditions, firms that institutionalize ISM capabilities are better positioned to maintain investor confidence, safeguard intangible assets, and mitigate reputational risk. The empirical evidence from this study supports this interpretation by demonstrating that ISM directly contributes to performance outcomes. At the same time, the significant effect of Digital Intensity underscores the structural role of IT infrastructure maturity. Thai-listed firms typically possess more advanced technological infrastructures than smaller enterprises, enabling them to deploy enterprise systems, analytics platforms, and digital service architectures. However, the findings indicate that technological availability alone does not guarantee a competitive advantage. Performance improvements occur when digital technologies are deeply integrated into organizational processes, decision-making systems, and strategic operations. Taken together, these results suggest that digital transformation in Thailand is not solely technology-driven but ISM-dependent. Organizations that synergize high digital intensity with robust security governance achieve superior performance, as this alignment allows for the efficient conversion of technological investments into sustainable strategic value.

This study makes several important contributions to theory. First, it advances digital transformation research by conceptualizing Information Security Management as a strategic organizational resource rather than merely an operational or compliance-oriented function. In line with the resource-based view (Barney, 1991), ISM can be interpreted as an intangible capability that enhances resilience, strengthens stakeholder trust, and enables firms to capture value from digital investments. This reconceptualization broadens the theoretical understanding of cybersecurity within organizational performance models. Second, the study extends technology adoption theory by demonstrating that digital awareness influences firm performance indirectly through Digital Intensity. By empirically validating the pathway from perceived usefulness to technological integration and ultimately to

performance outcomes, this research shifts the analytical focus from individual adoption behavior to organization-level strategic impact. Third, the research provides contextual enrichment to the digital transformation literature by offering empirical evidence from an emerging market setting in Thailand. Much prior work has been conducted in advanced economies with mature institutional environments. By examining Thai listed firms operating within evolving regulatory frameworks and heterogeneous technological conditions, this study highlights the importance of governance-oriented digital strategies in transitional economies. From a managerial standpoint, the findings indicate that executives should treat information security governance as an integral component of digital strategy rather than as a technical afterthought. Integrating ISM into strategic planning, risk management, and employee capability development can significantly enhance organizational performance. From a policy perspective, the results underscore the importance of strengthening national digital governance frameworks and cybersecurity standards to support sustainable digital transformation across industries. Overall, the evidence suggests that, within the context of Thai listed firms, investment in IT infrastructure alone is insufficient to generate sustained competitive advantage. Instead, superior performance emerges from the synergistic interaction between digital intensity, executive awareness of digital value, and robust information security governance. These findings position digital transformation as a strategic organizational capability shaped by both technological integration and institutional governance mechanisms.

Conclusion and Suggestions

This study investigated the impact of Information Security Management and Digital Intensity on organizational performance, while further exploring the link between the perceived usefulness of digital technologies and the level of digital adoption among SET-listed companies. The analysis was based on questionnaire data obtained from 191 valid organizational respondents and evaluated using regression and ANOVA techniques. The findings underscore that effective digital transformation should be understood as a multidimensional strategic process that integrates technological capability, managerial cognition, and governance discipline to generate sustained organizational value. The study makes several contributions to the literature. It advances information security research by reframing ISM as a strategic organizational resource rather than merely a compliance-oriented function, highlighting its role in strengthening competitiveness, supporting long-term sustainability, and enhancing firm value. In addition, the research offers an integrative perspective that connects previously distinct streams of scholarship by simultaneously examining digital adoption, security management, and organizational performance within a unified analytical framework. This synthesis provides a more comprehensive understanding of how digital capabilities and governance practices jointly shape organizational outcomes in contemporary digital environments.

This study should be interpreted in light of several design limitations. First, the sample is restricted to firms listed on the Stock Exchange of Thailand. Although listed companies offer an appropriate context for examining digital transformation and information security due to their formal governance structures and regulatory obligations, this sampling frame limits external validity. The findings may not generalize to small and medium-sized enterprises or privately held firms, which often differ in resources, technological capacity, and governance practices. Future studies should expand this scope to include a diverse array of industries, thereby enhancing the generalizability of the findings and providing a more granular understanding of how digital

capabilities drive performance across different sectors. Second, the study relied on a single-informant survey design using IT executives or equivalent senior technology managers as respondents. While such individuals possess relevant organizational knowledge, this approach may introduce informant bias and subjective interpretation. Subsequent studies could improve measurement robustness by employing multi-informant designs or integrating perceptual survey data with objective performance indicators. Finally, future research should expand the analytical scope by incorporating additional governance and performance dimensions. Examining the role of IT governance in shaping financial outcomes—such as return on technology investment, digital revenue intensity, and productivity gains—would provide deeper insight into how digital strategies translate into measurable economic value. Addressing these limitations would strengthen methodological rigor and advance a more nuanced and generalizable understanding of digital transformation, information security management, and organizational performance across diverse institutional contexts.

Acknowledgements

The authors gratefully acknowledge Rajamangala University of Technology Rattanakosin for financial support provided through a research grant.

Author Contributions

Kanoknate Prempree: Conceptualization, formal analysis, investigation, methodology, writing-original draft, writing-review & editing

Patsakorn Singto: Conceptualization, formal analysis, investigation, methodology, writing-original draft, writing-review & editing

Conflict of Interests

All authors declare that they have no conflicts of interest.

Funding

Rajamangala University of Technology Rattanakosin.

Declaration of Generative AI and AI-assisted Technologies

During the preparation of this manuscript, the authors used ChatGPT to assist with language editing. After using this tool, the authors carefully reviewed and revised the manuscript and accept full responsibility for the final version of the publication.

References

Almulhim, A. F. (2021). Smart supply chain and firm performance: The role of digital technologies. *Business Process Management Journal*, *27*(5), 1353-1372. https://doi.org/10.1108/BPMJ-12-2020-0573

Alonso, I. A., Verdún, J. C., & Caro, E. T. (2009). IT, senior executives and board of directors contribute to the success of the business: Implicates on the IT demand process life cycle. In *Proceedings of the Fourth International Conference on Computer Sciences and Convergence Information Technology* (pp. 149-156). IEEE. https://doi.org/10.1109/ICCIT.2009.288

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99-120. https://doi.org/10.1177/014920639101700108

Bolodeoku, P. B., Igbinoba, E., Salau, P. O., Chukwudi, C. K., & Idia, S. E. (2022). Perceived usefulness of technology and multiple salient outcomes: The improbable case of oil and gas workers. *Heliyon*, *8*(4), 1-8. https://doi.org/10.1016/j.heliyon.2022.e09322

Calvino, F., Criscuolo, C., Squicciarini, M., & Marcolin, L. (2018). *A taxonomy of digital intensive sectors.* OECD Publishing. https://doi.org/10.1787/f404736a-en

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. https://doi.org/10.2307/249008

Digital Economy Promotion Agency. (2023). *Digital industry 2023 (Final Report).* https://www.depa.or.th/storage/app/media/file/Digital%20Industry%202023%20Final01.pdf

Digital Economy Promotion Agency. (2022). *Digital economy promotion master plan phase 2 (2023-2027).* https://www.depa.or.th/en/master-plan-digital-economy/master-plan-for-digital-economy-66-67

European Union. (2022, August 26). *How digitalized are the EU's enterprises?* Eurostat. https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20220826-1

Fauzi, T. (2021). Impact of enterprise resource planning systems on management control systems and firm performance. *Uncertain Supply Chain Management*, *9*(3), 745-754. https://doi.org/10.5267/j.uscm.2021.4.003

Garg, P., Gupta, B., Sar, A., Graham, G., & Shore, A. (2024). Development and validation of an instrument to measure the perceived benefits of digitalization in manufacturing. *IEEE Transactions on Engineering Management*, *71*(4), 8288-8306. https://doi.org/10.1109/TEM.2024.3390434

Goi, V., Ahieieva, I., Mamonov, K., Pavliuk, S., & Dligach, A. (2023). The Impact of digital technologies on the companies' strategic management. *Economic Affairs*, *68*(2), 1291-1299. https://doi.org/10.46852/0424-2513.2.2023.33

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis* (7th ed.). Pearson.

Helland, I. S. (1987). On the interpretation and use of R^2 in regression analysis. *Biometrics*, *43(1)*, 61-69. https://doi.org/10.2307/2531949

Jiang, Q., Zhang, C., & Wei, Q. (2025). Digital technology adoption and enterprise investment efficiency. *Finance Research Letters*, *72*, 106623. https://doi.org/10.1016/j.frl.2024.106623

Jongwanich, J., & Kohpaiboon, A. (2024). *Digital technology adoption & SMEs' financial performance: Evidence from Thailand.* Discussion Paper Series.

Kahrovic, E., & Avdovic, A. (2023). Impact of digital technologies on business performance in Serbia. *Management Journal of Sustainable Business and Management Solutions in Emerging Economies, 28*(2), 37-53. https://doi.org/10.7595/management.fon.2021.0039

Kang, M., Miller, A., Jang, K., & Kim, H. (2022). Firm performance and information security technology intellectual property. *Technological Forecasting and Social Change, 181*, 121735. https://doi.org/10.1016/j.techfore.2022.121735

Kashada, A., Li, H., & Koshadah, O. (2018). Analysis approach to identify factors influencing digital learning technology adoption and utilization in developing countries. *International Journal of Emerging Technologies in Learning, 13*(2), 48-59. https://doi.org/10.3991/ijet.v13i02.7399

Khan, R. U., Salamzadeh, Y., Iqbal, Q., & Yang, S. (2020). The impact of customer relationship management and company reputation on customer loyalty: The mediating role of customer satisfaction. *Journal of Relationship Marketing, 21*(1), 1-26. https://doi.org/10.1080/15332667.2020.1840904

Kong, H., Jung, S., Lee, I., & Yeon, S. (2015). Information security and organizational performance: Empirical study of Korean securities industry. *ETRI Journal, 37*(2), 428-437. https://doi.org/10.4218/etrij.15.0114.1042

Kongsumpao, K. (2024). Information technology acceptance factors affecting performance efficiency in the electronic tax invoice and receipt systems of the revenue department. *Journal of Business Administration and Social Sciences, 7*(1), 12-24. https://so02.tci-thaijo.org/index.php/ibas/article/view/267587

Kutner, M. H., Nachtsheim, C. J., & Neter, J. (2008). *Applied linear regression rodels(4th ed).* McGraw-Hill.

Lee, Y. Y., Falahat, M., & Sia, B. K. (2021). Drivers of digital adoption: A multiple case analysis among low and high-tech industries in Malaysia. *Asia-Pacific Journal of Business Administration, 13*(1), 80-97. https://doi.org/10.1108/APJBA-05-2019-0093

Lo, C. K. M., Chen, C. H., & Zhong, R. Y. (2021). A review of digital twin in product design and development. *Advanced Engineering Informatics, 48*, 101297. https://doi.org/10.1016/j.aei.2021.101297

Marcolivio, M., & Wade, M. R. (2023). *The measurement of digital transformation performance.* IMD.

Moshi, A., Sife, A., & Matto, G. (2024). The effect of awareness on big data adoption readiness in public sector auditing in Tanzania: Assessing TAM model. *Asian Journal of Economics, Business and Accounting, 24*(7), 341-354. https://doi.org/10.9734/ajeba/2024/v24i71414

Nasiri, M., Saunila, M., & Ukko, J. (2022). Digital orientation, digital maturity, and digital Intensity: Determinants of financial success in digital transformation settings. *International Journal of Operations & Production Management, 42*(13), 274-298. https://doi.org/10.1108/IJOPM-09-2021-0616

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5).* https://doi.org/10.6028/NIST.SP.800-53r5

Nowicka, J., Ciekanowski, Z., & Milewska, A. (2024). Information security management as the basis for the functioning of an organization. *European Research Studies Journal, 27*(3), 128-141. https://doi.org/10.35808/ersj/3427

Nwankpa, J. K., & Datta, P. (2017). Balancing exploration and exploitation of IT resources: The influence of digital business intensity on perceived organizational performance. *European Journal of Information Systems, 26*(5), 469-488. https://doi.org/10.1057/s41303-017-0049-y

Ozili, P. K. (2022). *The acceptable R-square in empirical modelling for social science research.* SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4128165

Pigola, A., Costa, P. R, Vils, L., & Meirelles, F. S (2025). Enhancing information security management and performance through social and relational factors: A structural equation modelling approach. *Behaviour & Information Technology, 6*, 1-24. https://doi.org/10.1080/0144929X.2025.2522206

Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka, G. B., Wamba, S. F., & Bahanag, N. N. M. (2019). Effects of information security management systems on firm performance. *American Journal of Operations Management and Information Systems, 4*(3), 99-108. https://doi.org/10.11648/j.ajomis.20190403.15

Saleh, C., Mohamad, S., Talipi, N., & Budiawan, S. (2025). Measuring the impact of digital technology adoption on the operational efficiency of MSMEs in Indonesia. *Amsir Accounting & Finance Journal, 3*(1), 27-34. https://doi.org/10.56341/aafj.v3i1.570

Sudaryanto, M., Hendrawan, M., & Andrian, T. (2023). The effect of technology readiness, digital competence, perceived usefulness, and ease of use on accounting students artificial intelligence technology adoption. *E3S Web of Conferences, 388*, 04055. https://doi.org/10.1051/e3sconf/202338804055

Vanichbuncha, K. (2010). *Statistical analysis for administration and research* (12th ed.). Chulalongkorn University Press.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478. https://doi.org/10.2307/30036540

Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education, 8*(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021