International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 2804-2815
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

A Study on the Evolution of Digital Media Technologies and Their Effect on Information Security Practices

Huilong Li*

PhD candidate, International College, Krirk University, Bangkok, Thailand, 10220
* **Corresponding Author Email:** lhl@imac.edu.cn - **ORCID:** 0009-0002-9614-2865

Article Info:

DOI: 10.22399/ijcesen.1864
Received : 11 February 2025
Accepted : 12 April 2025

Keywords :

Digital Media Technologies,
Information Security Practices,
Cyber Threats,
Encryption Methods,
Social Media Vulnerabilities,
Holistic Security Frameworks.

Abstract:

Digital media technologies transformed communication systems through exceptional advancement rates. Rapid technological progress transformed how we collaborate with others alongside information distribution practises. Modern technology provided easier connectivity and performance optimization but introduced extensive problems with infrastructure security. The study investigates how digital media technologies relate to information security by analysing storage procedures across systems and encryption protocols and social media network development patterns. A total of 280 participants were utilised in the study to evaluate both critical security hazards and educational requirements as well as existing defence systems. Research findings indicate an immediate requirement to create an integrated security framework connecting technology innovation to regulatory action and behavioural guidance to minimise risks. Through this research organisations receive targeted recommendations that enhance their security frameworks during their digital transformation phase.

1. Introduction

Digital media tools emerged from the development of digital media technologies which brought fundamental changes to human social connections through self-interactions and organisational data-sharing practices [1]. People currently use digital media platforms extensively since they serve as vital lifelines for daily activities and streaming and collaborative tools play a vital role in modern digital media development [2]. Digital media technologies have introduced new standards regarding connection and innovation which help organisations enhance their performance levels and enable immediate access to real-time information [3].

Digital transformation introduces critical security challenges which threaten existing information protection methods. As digital media expands its reach the number of possible digital threat entry points grows which enables cybercriminals to discover and exploit system vulnerabilities. Data theft and phishing attacks and ransomware incidents and unauthorised network intrusions have increased in frequency [4]. The same platforms which users use for digital engagement also function simultaneously as emergency points where risk actors target private information. Homework productivity increases with real-time collaboration tools and cloud applications but widespread adoption leads organisations to encounter fresh security threats which break compliance rules and endanger end-user privacy [5].

The successful adoption of digital media requires robust information security systems that provide flexible protection measures across daily organisational operations. The challenges from modern technologies move too swiftly for traditional security models to effectively address them according to Susanto [6]. The protection of digital media requires advanced security techniques that defence against modern threats while they grow and transform. Academic research relevant to digital media development engages heavily in the study of security measure connectivity and adjustment standards [7].

The combination of cybersecurity and digital media fields lacks systematic investigation although researchers have studied each field discretely. The analysis between digital media innovation and information security approach modifications remains an understudied field of research. Research on this unexplored area generates foundational insights necessary to safeguard digital assets

alongside preserving user confidence in modern systems [8]. A quantitative research approach underpins this investigation which examines digital media's impact on information security practice patterns. The study combines analysis of vulnerabilities with investigations into security incidents coupled with assessments of existing protective methods. The study presents empirical recommendations for fortifying digital security infrastructure that emerge from identified patterns.

2. Literature Review

The quick expansion of contemporary digital media technologies produces significant transformations within human communication methods alongside information propagation and collaborative activities. The advancements in digital technology produce new growth options yet develop vulnerabilities that risk both individual safety and company protection. The current study analyzes existing research on the relationship between digital media technologies and information security practices. This research investigates cyber threats along with adaptive security upgrades as well as considerations of user awareness and knowledge gaps.

2.1 Theoretical Frameworks and Methodological Approaches

Security technology adoption research bases its understanding on both the Technology Acceptance Model (TAM) and Diffusion of Innovations (DOI) frameworks according to studies. The adoption process of AI-based threat detection systems was evaluated by Rodriguez and his team (2021) through TAM theory research methods while Singh and Patel (2020) investigated blockchain security technology expansion using DOI theory principles [9].

2.2 The Proliferation of Cyber Threats

The widespread implementation of digital media technology directly resulted in massive growth of cyber threats which now confront all of society. Social media platforms provide digital channels for cybercriminals to access user data. When users share personal details on sites like Facebook Instagram and LinkedIn they increase the risk of being targets for phishing and baiting during social engineering attacks. Hackers use this data to trick victims into giving away critical system information access for malware-controlled systems [10]. Streaming platforms represent recent attractive entry points hackers use to exploit digital services. These platforms depend on robust network capacity which becomes a liability that hackers exploit through Distributed Denial-of-Service attacks to disrupt services and cause financial impact as Bellovin explained [11]. Cloud-based collaboration tools such as Google Workspace and Microsoft Teams present risks that include both unauthorized data access and leaks alongside substandard endpoint protection [12]. The rising Internet of Things (IoT) platforms are enabling these security weaknesses. Current IoT systems present multiple security risks from which botnets along with ransomware attacks can take advantage. The combination between smart house products and industrial sensor systems has established numerous routes through which malicious actors can start their online assaults.

2.3 Adaptive Security Frameworks

Researchers suggest that adaptive security frameworks are essential to defend against a constantly changing cyber threats. Inherent in security frameworks are abilities that adapt themselves independently both to new threats and modern technical advancements. Due to AI and Machine Learning (AI/ML) integration, security technology needs to be an AI/ML combination which automates threat identification and defense capabilities. Generating future attack forecasts and tracking anomalous behavior is facilitated by extended data sets processed by AI driven instruments that also identify established patterns [13]. Regulatory frameworks for enhancing information security remain the focus of persistent expert analysis. General Data Protection Regulation (GDPR) operates as the standard European Union method to protect privacy and handle data protection obligations. Complex modern threats exceed basic regulatory adherence boundaries. The implementation of successful cybersecurity demands a united approach that connects network infrastructure to operational policies and lawmaking regulations [14]. Blockchain technology proves to enhance the digital media protection system’s capabilities. Blockchain sports offers a protected digital transaction structure for decentralized structure through which intellectual property assets and supply chain components are safeguarded. One of the biggest hindrances for blockchain adoption in information security is the compatibility problem and clear energy usage and scalability performance issues [15]. Finally, the integration of AI / ML powered adaptive security frameworks is essential in responding to constantly changing cyber threats. Besides the automation of threat detection and defense, these frameworks also

facilitate predictive analysis thanks to advanced data processing. Unfortunately, regulatory frameworks like GDPR provide a solid foundation for security; however, this must be enhanced to accommodate a rise of more powerful threats.

2.4 The Role of User Awareness

Entirely successful risk mitigation of digital media technology systems is achieved only through user awareness. In terms of leading factors that trigger security breaches, personnel errors are leading. This reason is that users have weak password protection and fail to defend themselves against phishing attack knowledge and the sensitive details they do not generally protect. Awareness based user education initiatives is leading organizations running user education initiatives to find that they have lower number of security incidents [16]. The Cybersecurity Alliance (2021) discovered organizations that provided extensive training had a **35% lower success rate** for phishing attacks than those which did not offer training. Security awareness programs integrate exercise-based phishing simulations together with practical offline workshops alongside ongoing security threat education [17]. In the past decades, security culture principles were established themselves as widely recognized practice among all industrial branches. However, the construct and development of these security focused cultural mindsets require organizations to continually communicate with their workforce, but need executive support and engaged workforce participation. As this cultural transformation is exited, security transitions into distributed organizational stewardship, exiting traditional IT departmental boundaries [18]. Finally, in order to successfully mitigate risks in digital media technology systems, we need to create awareness in customers and address human error, which still remains the major security breach reason. Investing in user education initiatives such as phishing simulations and hands on workshops substantially reduces incident rates, confirming the importance of training in sealing the vulnerabilities.

2.5 Emerging Technologies and Security Challenges

Artificial intelligence (AI), augmented reality (AR) and virtual reality (VR), in combination, have greatly expanded information security parameters and introduction. When AR technology adds to VR technology, the data capture methods and control mechanisms face special challenges [19]. Biometric information collected by AR/VR devices through eye tracking and facial recognition technologies faces unauthorized access concerns. Data points obtained through observation remain at risk of exploitation by unapproved users enabling/location tracking capabilities and identity theft possibilities. However, even the use of artificial intelligence in an organization brings with it valuable security benefits, but also some serious safety risks. Dual functionality, on the other hand, is exercised by AI systems whereby their detection systems can be turned into powerful malware tools and simultaneously create blockers for detection. At implementing AI in cybersecurity, people are confronted with two-fold ethical requirement came by both the pattern of bias of AI and its transparency [20]. Therefore, the integration of AI, AR, and VR technologies greatly improves information security capabilities, yet presents unique issues. AR and VR devices, with their more sophisticated methods of biometric data collection, present risks of unauthorized access as well as identity theft, underlining the need for tighter data protection. While beneficial to provide security, AI can be dual functional and its detection capabilities can be turned about for malicious means.

2.6 Regional Variations in Security Practices

Due to having well established cybersecurity frameworks, research around digital media technologies, as well as information security, mainly takes place in the North America and European regions [21]. The information security and the combination of obstacles and advantages specific to digital media technology together present problems for developing nations in developing new media of mass information. Due to lack of proper cybersecurity tools along with lack of regulation accompanied by lack of user understanding of security protocols, these areas serve as multiple threats [22]. Digital defense vulnerabilities generate dramatic surges in the insurance of cybersecurity threats so as to make the automation of effective security systems a challenge. Nigeria’s economy is undergoing rapid digital transformation, allowing builders to create security solutions to fit local needs. The need for adaptive security solutions that operate at affordable levels is supported by adoption of digital media technology in these regions. Custom technology solutions to combat the specific regional threats pay better when paired with standard security campaigns directed at local populations [23]. Security issues are diverse across all African regions thus developers need to be aware of various security needs within different developing regions. Organizational partners have to work with members of a policymaking community

to develop security plans which address local concerns so everyone can involve in the advanced digital media technology [24]. Lastly, while cybersecurity research and frameworks exist widely in North America and Europe, developing nations have unique problems to ensure there are not enough tools, regulations, or user awareness. In light of these vulnerabilities, the complexity of creating an automated and automated security systems increases. The fast pace of the digital transformation in any region as in Nigeria makes cases for tailor made security solutions that address local threats and still be affordable. Focusing on collaboration between developers, organizations and policymakers to harness local, custom security campaigns and sophistication leveraged regions can then develop resilient cybersecurity and completely integrate advance digital media technologies.

2.7 Gaps in Existing Research

The extensive research on digital media technologies and information security shows persistent knowledge shortages. Data about security concerns in emerging technologies faces inadequate documentation in existing research. Few scholars have studied security challenges related to emerging AR/VR and quantum computing technologies despite extensive academic investigation of blockchain and IoT systems. Most security-focused research studies security practices through the analysis of fixed points measured across different periods of time. Organizational adaptive capabilities to security threats and technical progress must be studied over extended timeframes through longitudinal studies to track security practice changes. The current research literature features insufficient interdisciplinary connections between technical components and sociocultural security perspectives. Understandings of security practices require users' behavior analysis combined with insights from psychology sociology and behavioral economics to create a holistic view of this subject.

3. Research Methodology

Fryer, Larson-Hall, and Stewart’s 2018 guidelines serve as the quantitative basis for this research to pinpoint how digital media exposure impacts data protection protocols. During data collection the study incorporated three groups that consisted of adults aged 25 or older and both student and professional groups including beginner users of advanced technology integrated with information protection strategies. The specialists formed a special demographic segment to ensure that the study participants underwent adequate digital media advancement impacts on security dimensions [25].

A total of 280 individuals completed surveys after being selected for data collection through purposive sampling which incorporated both broad industry experience and diverse expertise levels. The study survey used twenty Likert-scale questions to assess advances in digital media storage while examining matured social media networks and encryption protection features. Each participant rated their responses using a scale ranging from 1 which indicated strong disagreement to 5 which signified full agreement. These specific variables were examined by research to determine their effect on information security practices.

Statistical Package for the Social Sciences (SPSS) was used for data analysis which followed procedures detailed by researchers Hinton, McMurray, and Brownlow [26]. Statistical documentation revealed participant demographics and response patterns while researchers used statistical inference to detect cause-and-effect relationships. The researchers established questionnaire consistency through Cronbach's Alpha by examining item correlations that confirmed their reliability.

Specified exclusive and inclusive parameters served to ensure the participants in the sample matched individuals with serious digital media usage responsibilities. Researchers included participants whose digital media engagement included at least one platform including social media applications and cloud storage services and collaborative tools and lasted for at least six consecutive months. The design element contributed to a fundamental understanding of modern digital solutions and recognized exposure to digital security risks [27]. The participants required fundamental knowledge of information security criteria including passwords and two-factor authentication methods and simple encryption practices before answering survey inquiries. Adults above 25 years’ old who used digital media for everyday purposes in their careers or personal life entered the study together with students whom the academic curriculum demanded to use digital tools for coursework. The inclusion criteria consisted of professionals who routinely managed sensitive data while following their organization's security specifications at work [28].

The study excluded participants who interacted minimally or not at all with digital media platforms or reported language difficulties and cognitive disabilities which hindered their ability to answer the survey questions. The researchers excluded personnel who took part in voluntary questionnaire evaluation because their familiarity with the instrument could generate potential prejudices [29].

The established procedures worked to eliminate survey contaminants thereby providing representative results that showed actual digital media technology usage by different skilled professional groups. Table 1 shows inclusion and exclusion criteria.

Table 1. *Inclusion and Exclusion Criteria*

Criteria	Details
Inclusion	▪ At least 6 months of active use of a digital media platform ▪ Basic understanding of security practices (e.g., passwords, 2FA) ▪ Adults over 25 engaged in personal/professional digital tasks ▪ Students enrolled in courses using digital tools ▪ Professionals handling sensitive data and adhering to security guidelines
Exclusion	▪ No significant digital media interaction ▪ Language/cognitive barriers preventing valid survey responses ▪ Prior participation in pilot or earlier versions of the survey

Researchers employed strong research methods to determine digital media's effect on information security strategies through technological advances. The study's broad participant diversity when combined with strong statistical methods delivered both reliable and valid results which analyzed permanent digital media platform usage among professional users [30].

Participants in the study obtained complete knowledge about research objectives and full documentation on data collection protocols with protection details for volunteer participants. Research volunteers could fully determine their study engagement and could leave at any point without facing unintended negative consequences anytime throughout the research [31]. Before receiving questionnaires participants provided informed consent in each case while researchers then agreed to keep data confidential and explained its utilization would strictly follow academic purposes. Personal identifiers were not collected from participants because their data resided on encrypted servers which were accessible only to the research team through best security practices for sensitive data [32]. The research protocol earned institutional review board acknowledgment signaling ethical social science research compliance. Ethical protocols established throughout the research ensured complete privacy protection for participants alongside their rights maintenance while maintaining research integrity.

4. Data Analysis

4.1 Frequencies Distributions of Demographics

The demographic analysis covers age groups and familiarity with information security practices. Table 2 summarizes the statistics for the data collected.

Table 2. *Summary of Demographic Statistics*

Statistics			
		What is your age group?	How familiar are you with information security practices?
N	Valid	280	280
	Missing	0	0

4.2 Age

The age distribution of participants is presented in Table 3.

Table 3. *Frequency Distribution of Age Groups*

What is your age group?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	25-35 Year	80	28.6	28.6	28.6
	35-45 Year	103	36.8	36.8	65.4
	Above 45 Years	97	34.6	34.6	100.0
	Total	280	100.0	100.0	

The study data shows that adults within the 35–45 age bracket represent the largest group at 36.8%. Individuals who are above 45 years represent 34.6% of the participants whereas young adults aged 25-35 comprise 28.6% of the group. The participation diversity enables researchers to grasp diverse age-based generational viewpoints regarding digital media knowledge and information protection methods. Figure 1 is the frequency distribution of age groups.

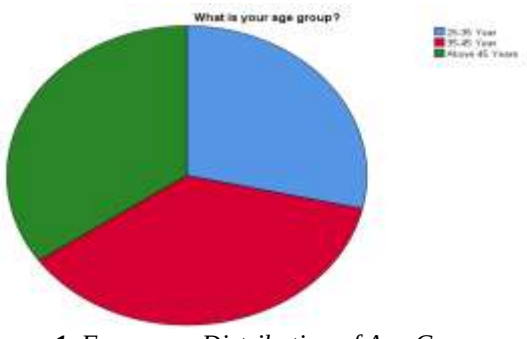

Figure 1. *Frequency Distribution of Age Groups*

4.3 Familiarity with Information Security Practices

Table 4 represents the familiarity levels of respondents with information security practices.

Table 4. *Frequency Distribution of Familiarity with Information Security Practices*

How familiar are you with information security practices?					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Moderately familiar	89	31.8	31.8	31.8
	Very familiar	94	33.6	33.6	65.4
	Extremely familiar	97	34.6	34.6	100.0
	Total	280	100.0	100.0	

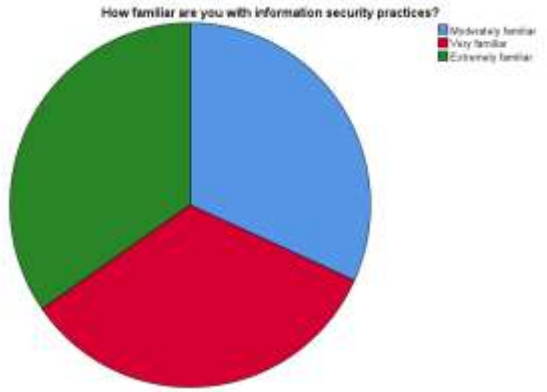

Figure 2. *Frequency Distribution of Familiarity with Information Security Practices*

Figure 2 shows frequency distribution of familiarity with information security practices. Respondents reported diverse understanding levels regarding information security procedures. Extremely familiar staff make up 34.6% of the sample while people with moderate familiarity make up 31.8% and those who are very familiar comprise 33.6% of those surveyed. Most research participants demonstrate solid information security comprehension which provides trustworthy data for this investigation.

4.4 Reliability Analysis

The reliability of the survey instrument is measured using Cronbach's Alpha. Table 5, 6, 7, 8 summarizes the reliability scores for the four scales.

Table 5. *Advancements in Digital Media Storage Technologies*

Reliability Statistics	
Cronbach's Alpha	N of Items
.799	5

Table 6. *Proliferation of Social Media Platforms*

Reliability Statistics	
Cronbach's Alpha	N of Items
.796	5

Table 7. *Evolution of Encryption Technologies*

Reliability Statistics	
Cronbach's Alpha	N of Items
.785	5

Table 8. *Information Security Practices*

Reliability Statistics	
Cronbach's Alpha	N of Items
.813	5

The scales present reliability ratings between 0.785 to 0.813 which demonstrates good internal consistency according to Cronbach's alpha. The Information Security Practices scale demonstrates the highest reliability score with $\alpha = 0.813$ which indicates strong measurement of the dependent variable. The survey instrument demonstrates reliable results throughout its entire set of scales.

4.5 Normality Analysis

Normality was tested using the Kolmogorov-Smirnov and Shapiro-Wilk tests. Table 9 presents the results.

Kolmogorov-Smirnov and Shapiro-Wilk tests indicate that none of the scales exhibit normal distribution at $p < 0.05$. The observations deviate from normality which makes non-parametric tests necessary for subsequent analysis so researchers can select suitable statistical approaches that fit the distribution pattern of their data.

Table 9. *Normality Tests for Scales*

Tests of Normality						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Advancements in Digital Media Storage Technologies	.091	280	.000	.955	280	.000
Proliferation of Social Media Platforms	.100	280	.000	.952	280	.000
Evolution of Encryption Technologies	.109	280	.000	.948	280	.000
Information Security Practices	.119	280	.000	.938	280	.000
a. Lilliefors Significance Correction						

4.6 Correlation Analysis

Spearman's rho was used to examine the correlations between the independent variables and the dependent variable. Table 10 summarizes the results. The correlation examination demonstrates strong positive connections between Information Security Practices and each independent variable. Performance analysis shows the Proliferation of Social Media Platforms as the main influence on security practices with a significant correlation ($r = 0.810$, $p < 0.01$). Statistical analysis demonstrates each measured relationship holds significant strength making clear that these variables tightly interact with one another.

4.7 Regression Analysis

The regression model evaluates the predictive power of independent variables on Information Security Practices. Tables 11, 12, and 13, and 14 summarize the results. The established regression model demonstrates its ability to predict 71.6% of Information Security Practices variation ($R^2 = 0.716$). The stability indicator of the model remains strong at 0.713 even when researchers correct for potential overfitting phenomena. ANOVA analysis demonstrates the statistical importance of the regression model at $F = 231.742$ ($p < 0.001$). Data shows these independent variables (Advancements in Digital Media Storage Technologies, Proliferation of Social Media Platforms, and Evolution of Encryption Technologies) make a significant total impact on Information Security Practices.

Table 10. *Correlation Analysis*

Correlations					
			Advancements in Digital Media Storage Technologies	Proliferation of Social Media Platforms	Evolution of Encryption Technologies
Spearman's rho	Information Security Practices	Correlation Coefficient	.788**	.810**	.777**
		Sig. (2-tailed)	.000	.000	.000
		N	280	280	280
**. Correlation is significant at the 0.01 level (2-tailed).					

Table 11. *Model Summary*

Variables Entered/Removed[a]			
Model	Variables Entered	Variables Removed	Method
1	Evolution of Encryption Technologies, Advancements in Digital Media Storage Technologies, Proliferation of Social Media Platforms[b]	.	Enter
a. Dependent Variable. Information Security Practices			
b. All requested variables entered.			

Table 12. *Model Summary*

Model Summary[b]					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.846[a]	.716	.713	.572204326896579	2.172
a. Predictors: (Constant), Evolution of Encryption Technologies, Advancements in Digital Media Storage Technologies, Proliferation of Social Media Platforms					
b. Dependent Variable: Information Security Practices					

Table 13. *ANOVA*

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	227.629	3	75.876	231.742	.000[b]
	Residual	90.367	276	.327		
	Total	317.996	279			
a. Dependent Variable: Information Security Practices						
b. Predictors: (Constant), Evolution of Encryption Technologies, Advancements in Digital Media Storage Technologies, Proliferation of Social Media Platforms						

Table 14. *Coefficients*

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.207	.107		1.935	.039
	Advancements in Digital Media Storage Technologies	.297	.061	.291	4.884	.000
	Proliferation of Social Media Platforms	.391	.064	.380	6.138	.000
	Evolution of Encryption Technologies	.243	.062	.234	3.928	.000
a. Dependent Variable: Information Security Practices						

Analysis shows all three independent variables demonstrate relevance toward Information Security Practices with a high significance value ($p < 0.001$). Social Media Platform proliferation emerges as the main predictor ($\beta = 0.380$) based on standardized beta coefficients while Digital Media Storage Technologies follow closely ($\beta = 0.291$) and Encryption Technologies Evolution stands at ($\beta = 0.234$). The research shows different strengths with which these variables affect information security practices.

4.8 Discussion

E findings of this research provide significant insights about digital media technology development along with their effects on information security practices. The examination of security framework determinants and organizational adaptation to modern technology changes included information from 280 participants. This paper presents the results against their security strategy background while establishing their research content connection to previous literature.

4.8.1 Advancements in Digital Media Technologies and Security Practices

Digital media technology developments involving storage systems combined with encryption methods help fundamentally shape how organizations implement information security practices. People underlined the necessity of implementing powerful storage systems which serve to minimize access-related security threats and data exposure incidents. The results support research done by Chua et al. showing that cloud-based systems remain exposed to risks while storage technology research must remain active [33].

The development of encryption technology strengthened its impact on the security practices landscape. Research findings demonstrate that effective data protection through encryption depends on both system maintenance and user education about encryption practices. New research backs by Mohammad et al. demonstrating the necessity of using advanced cryptographic protocols to defeat current cyber threats [34]. The research uncovers obstacles organizations experience notably in developing nations because of limited resources along with technical integration complexities.

4.8.2 The Role of Social Media in Security Vulnerabilities

Social media platforms increased at an exponential rate and research showed this development created substantial security risks. Organization participants admitted they faced recurrent breaches and phishing incidents through social media usage across their professional domain. The research by Jain et al. promoted social media platforms as key risk points for cyberattacks. Strict governance measures alongside social media monitoring ought to be strengthened because they represent the main defense against professional vulnerabilities [35].

Organizations which use social media for business functions consistently show weaknesses in their security protocols designed to secure important data. According to Bandari et al. organizations require specific training programs and protective policies that strike a balance between social media use and security requirements to reduce exposure [36].

4.8.3 Influence of User Awareness and Training Programs

Research reveals that user understanding plays a major role in developing enhanced information security practices. Security breaches result frequently from human mistakes like weak password management and susceptibility to phishing attacks according to participant feedback. The research by Ogbanufe shows that training programs hold essential power to give staff members adequate skills in recognizing potential threats for defense [37]. Organizations focused on

educating their users achieved lower security incident rates which demonstrates that establishing security-minded employee awareness produces optimal risk management capabilities. The Cybersecurity Alliance reports that scheduling regular workshops together with simulated phishing simulations and straightforward security policy education reduces operational vulnerabilities while improving organizational defense capacity.

4.8.4 Regression Analysis and Implications

This study uses regression analysis to explore the complex interaction patterns between advancements in storage technologies and social media proliferation and encryption techniques and their impact on information security practices. The model's results show these factors account for **71.6%** of the security practice variance because of their R^2 value. Research findings demonstrate a high level connection between social media growth patterns and security concerns leading to an immediate need to resolve this problem area. The research of Alshaikh shows organizations need to follow three main steps including monitoring tools and policy enforcement coupled with user education to defend against social media risks. Security practice improvements stem from encryption technology advancements according to the research although smaller organizations face challenges with both accessibility and affordability [38].

4.8.5 Broader Implications for Organizations

Security frameworks developed by organizations can benefit from the outcomes discovered in this study. Security practices require continuous investment in research and development because technological advancements have an increasingly strong influence. In order to confront newly developing threats organizations require both revolutionary technological solutions and continuous security protocol updates. The study highlights that organizations must combine human elements and technology as essential parts of their security systems. Storage and encryption technology advancements remain vital but user education about security stands equally essential for modern security standards. The prevention of threats demands organizations to establish training and awareness initiatives ensuring their personnel fully understand how to effectively respond to threats [39]. Finally, research evidence shows security requires complete integration of technical systems alongside human influences for developing protective defenses. Businesses must defend potential weaknesses across every section including their access to social media and their data storage procedures along with their encryption system configurations.

4.9 Limitations and Future Research

This study provides crucial research insights along with identifiable limitations that researchers must address. This research encounters obstacles because participants may misreport by exaggerating their security practices or minimizing the number of security incidents that occur. The study examined IT professionals to establish findings yet maintained a control for regional specificities. Multiple research restrictions derived from these underlying conditions limited the applicability of broad themes. To produce a holistic understanding of security information practice elements researchers, need to carry out comprehensive surveys with users of different backgrounds alongside policy-makers across multiple demographic regions. The study of security practices evolution in response to technological change needs longitudinal research throughout extended time periods.

5. Conclusion

The findings of this research shows modern digital technology developments directly influence information protection requirements. Sophisticated storage infrastructure implementation by organizations together with social media applications and encryption solutions has created advanced information security threats that become increasingly complicated through their amalgamation. Organizations should take immediate action to protect their digital resources according to this research. The fields of digital security have achieved powerful data storage protections coupled with encryption capability improvements. The deployment of security measures encounters several obstacles because organizations do not have enough resources and struggle to meet requirements and their users practice insufficient security methods. The functions of social media platforms enable cybercriminal organizations to create novel security threats which both allow unauthorized data access and execution of phishing schemes against users. The results show an urgent need for stronger governance systems alongside effective monitoring systems and policy regulatory methods to manage exposure points.

According to the analysis findings organization cyber protection abilities develop through user

awareness programs and educational initiatives. Institutional security suffers from human mistakes yet must implement comprehensive staff education programs that increase security awareness throughout the entire organization. Organizations achieve successful threat prevention through scheduled training alongside policy learning programs that feature active threat simulation practices. The research regression analysis identifies that combining updated file storage systems with encrypted standards plus strict social media control mechanisms establishes superior security environments. Sustainable cybersecurity achievement requires a united system that unites technological advancements with official government rules coupled with proper user conduct control processes. The research describes cost-efficient solutions that organizations must implement for dealing with their contemporary digital obstacles. Organizations can create stronger defensive angles through sophisticated technology integration with secure systems and public security consciousness development programs. Future information security research should study these concepts by applying them to diverse population samples and conduct qualitative testing alongside time-based investigations of how new technologies influence security conditions.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Nuriddinov. (2023). Use of Digital Sports Technologies in Sports Television. *American Journal of Social Sciences and Humanity Research*. 3(11);208-219. https://theusajournals.com/index.php/ajsshr/article/view/1980/1915

[2] Aondover, E. M., Tosin, Y. A. N., Akin-Odukoya, O. O., Onyejelem, T. E., & Ridwan, M. (2025). Exploring the Application of Social Media in Governance in Nigeria. *SIASAT*. 10(1);30-43. https://doi.org/10.33258/siasat.v10i1.193

[3] Qalati, S. A., Ostic, D., Sulaiman, M. A. B. A., Gopang, A. A., & Khan, A. (2022). Social media and SMEs' performance in developing countries; Effects of technological-organizational-environmental factors on the adoption of social media. *Sage Open*. 12(2);21582440221094594. https://doi.org/10.1177/21582440221094594

[4] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors*. 23(15);6666. https://doi.org/10.3390/s23156666

[5] Sharma, P., Sharma, R., & Bhardwaj, K. (2024). Cloud Computing in Everyday Life: Revolutionizing How We Live, Work, and Connect. In *Driving Transformative Technology Trends With Cloud Computing*. IGI Global. 43-53. https://doi.org/10.4018/979-8-3693-2869-9.ch003

[6] Susanto, H., Fang Yie, L., Mohiddin, F., Rahman Setiawan, A. A., Haghi, P. K., & Setiana, D. (2021). Revealing social media phenomenon in time of COVID-19 pandemic for boosting start-up businesses through digital ecosystem. *Applied System Innovation*. 4(1);6. https://doi.org/10.3390/asi4010006

[7] Thakur, M. (2024). Cyber security threats and countermeasures in the digital age. *Journal of Applied Science and Education (JASE)*. 4(1);1-20. https://doi.org/10.54060/a2zjournals.jase.42

[8] Mukherjee, S., Baral, M. M., Nagariya, R., Chittipaka, V., & Pal, S. K. (2024). Artificial intelligence-based supply chain resilience for improving firm performance in emerging markets. *Journal of Global Operations and Strategic Sourcing*. 17(3);516-540. https://doi.org/10.1108/JGOSS-10-2022-0075

[9] Kaur, G., Bonde, U., Pise, K. L., Yewale, S., Agrawal, P., Shobhane, P., Maheshwari, S., Pinjarkar, L., & Gangarde, R. (2024). Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime. *Engineering Proceedings*. 62(1);6. https://doi.org/10.3390/engproc2023062006

[10] Bellovin, S. M., Blaze, M., Clark, S., & Landau, S. (2014). Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Northwestern Journal of Technology and Intellectual Property*. 12;1. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip

[11] Holloway, S. (2024). The Impact of Cloud-Based Information Systems on Collaboration and Productivity in Remote Teams. https://doi.org/10.20944/preprints202412.0958.v1

[12] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things; Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*. 22(1);616-644. https://doi.org/10.1109/COMST.2019.2953364

[13] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*. 22(1);616-644. https://doi.org/10.1109/COMST.2019.2953364

[14] Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*. 28(2);359-374. https://doi.org/10.1108/JFC-08-2020-0173

[15] Yu, S. (2021). Application of Blockchain-Based Sports Health Data Collection System in the Development of Sports Industry. *Mobile Information Systems*. 2021;4663147. https://doi.org/10.1155/2021/4663147

[16] Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*. 24;1-22. https://doi.org/10.1007/s10796-020-10044-1

[17] Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2024). A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software*. 208;111899. https://doi.org/10.1016/j.jss.2023.111899

[18] Abdulhadi, O. (2023). The human connection to information security: A qualitative study on policy development, communication and compliance in government agencies. https://his.diva-portal.org/smash/record.jsf?pid=diva2%3A1772736

[19] Zhang, Z., Wen, F., Sun, Z., Guo, X., He, T., & Lee, C. (2022). Artificial intelligence-enabled sensing technologies in the 5G/internet of things era: from virtual reality/augmented reality to the digital twin. *Advanced Intelligent Systems*. 4(7);2100228. https://doi.org/10.1002/aisy.202100228

[20] Habbal, M. K. Ali, & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*. 240;122442. https://doi.org/10.1016/j.eswa.2023.122442

[21] Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*. 124;102974. https://doi.org/10.1016/j.cose.2022.102974

[22] UNCTAD. (2021). Digital economy report 2021: Cross-border data flows and development. *United Nations Conference on Trade and Development*. Available at: https://unctad.org/webflyer/digital-economy-report-2021/

[23] Oke, E., Aliu, J., Fadamiro, P. O., Akanni, P. O., & Stephen, S. S. (2023). Attaining digital transformation in construction: an appraisal of the awareness and usage of automation techniques. *Journal of Building Engineering*. 67;105968. https://doi.org/10.1016/j.jobe.2023.105968

[24] Wale-Oshinowo, Omobowale, A. O., Adeyeye, M. M., & Lebura, S. (2023). Least developed countries in Africa. In *The Palgrave Encyclopedia of Global Security Studies*. Springer International Publishing. 882-897. https://doi.org/10.1007/978-3-319-74336-3_346-1

[25] ITU. (2021). Global cybersecurity index 2020. *International Telecommunication Union*. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

[26] Couch, V. (2024). Investigating the Impact of Cybersecurity Awareness in K12 Context: A Quantitative Research Method. *Ph.D. dissertation, Colorado Technical University.*

[27] Hinton, P. R., McMurray, I., & Brownlow, C. (2014). *SPSS Explained*. 2nd ed. Routledge.

[28] Alcock, P. M. (2021). Cybersecurity perception and behavior, insights from a global workforce: A quantitative comparative study. *Doctoral dissertation, Capella University.*

[29] Trunfio, M., & Rossi, S. (2021). Conceptualising and measuring social media engagement: A systematic literature review. *Italian Journal of Marketing*. 2021(3);267-292. https://doi.org/10.1007/s43039-021-00035-8

[30] Aschbrenner, K. A., Kruse, G., Gallo, J. J., & Plano Clark, V. L. (2022). Applying mixed methods to pilot feasibility studies to inform intervention trials. *Pilot and Feasibility Studies*. 8(1);217. https://doi.org/10.1186/s40814-022-01173-2

[31] Hasan, N., Rana, R. U., Chowdhury, S., Dola, A. J., & Rony, M. K. K. (2021). Ethical considerations in research. *Journal of Nursing Research, Patient Safety and Practise (JNRPSP)*. 1(01);1-4. https://doi.org/10.55529/jnrpsp11.1.4

[32] Lee, T., & Kim, M. (2021). Data Encryption Protocols for Protecting Confidential Survey Responses. *Computers & Security*. 101;102881. https://doi.org/10.1016/j.cose.2020.102881

[33] Chua, E. M. X., & Chan, T. J. (2022). The influence of corporate social responsibility communication and corporate image of beverage companies: A customers' perspective. *Journal of Arts and Social Sciences.* 5(2);1-14. https://ruijass.com/wp-content/uploads/2022/03/CTK0011.pdf

[34] Mohammad, N. (2021) Enhancing Security and Privacy in Multi-Cloud Environments: A Comprehensive Study on Encryption Techniques and Access Control Mechanisms. *International Journal of Computer Engineering and Technology (IJCET).* 12;51-63. http://iaeme.com/Home/issue/IJCET?Volume=12&Issue=2

[35] Jain, K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*. 7(5);2157-2177. https://doi.org/10.1007/s40747-021-00359-0

[36] Bandari, V. (2023). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization

types. *International Journal of Business Intelligence and Big Data Analytics*. 6(1);1-11. https://research.tensorgate.org/index.php/IJBIBDA/article/download/3/3

[37] Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Computers & Security*. 108;102340. https://doi.org/10.1016/j.cose.2021.102340

[38] Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*. 100;102090. https://doi.org/10.1016/j.cose.2020.102090

[39] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*. 109;102387. https://doi.org/10.1016/j.cose.2021.102387