EXAMINING THE NEXUS BETWEEN ENVIRONMENTAL UNCERTAINTY, I T. COMPETENCE, AND INFORMATION SECURITY MANAGEMENT

Mustajab A. Soomro
International Pathway College, University of Tasmania, Australia
(IPC-UTAS)
Correspondence: mustajabahmed.soomro@utas.edu.au

ABSTRACT: *Information security management is gaining much importance in the current era, typically due to growing uncertainties and complexities in the business world. Corporations are striving harder to ensure they have all the right tools and technologies in place to secure their critical information to avoid any unintended consequences. The study attempted to investigate the relationship between factors influencing information security management. Through using quantitative data, the study tested the role of environmental uncertainty and IT competence in boosting information security management. The results suggest that environmental uncertainty can help enhance information security management. This indicates that organizations facing high environmental uncertainty work harder to have stronger information security protocols to avoid any unintended consequences. Accordingly, the findings of the study also indicate that the extent of I.T. competence of a company also helps to boost information security management. The findings of the study offer important implications for practice followed by avenues for future researchers on the topic.*

Keywords: Information, Information security management, environmental uncertainty, I.T competence, Reta*il*

1. INTRODUCTION

Information Security Management refers to the strategic and systematic approach adopted by organizations to protect their valuable information assets from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. It involves the implementation of comprehensive policies, procedures, and controls to ensure the confidentiality, integrity, and availability of sensitive data. Information Security Management encompasses various aspects such as risk assessment and management, incident response planning, security awareness training programs, and the continuous monitoring of security measures.

By effectively managing information security risks and vulnerabilities, organizations can safeguard their critical information from potential threats posed by cybercriminals or malicious insiders while ensuring business continuity and regulatory compliance in an increasingly interconnected digital landscape. Research plays a crucial role in the field of information security management, as it helps organizations stay ahead of emerging threats and protect sensitive data [2]. Through research, professionals can identify vulnerabilities, analyze attack patterns, and develop effective countermeasures to safeguard against cyber-attacks. Furthermore, research facilitates the discovery of new technologies and methodologies that enhance security practices and ensure compliance with evolving regulations. By investing in research, organizations gain a deeper understanding of risks and can make informed decisions to mitigate potential threats. Ultimately, this proactive approach not only strengthens an organization's security posture but also instills confidence among stakeholders in their ability to protect valuable information assets[3]. Keeping the significance thus beforehand, the current study has attempted to outline and investigate how some of the prospects such as environmental uncertainty and IT competence can help strengthen information security management. The paper provides novel empirical results followed by implications for theory and practice.

2. LITERATURE REVIEW

Information Security Management

Information Security Management refers to the strategic and systematic approach adopted by organizations to protect their valuable information assets from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. It involves the implementation of comprehensive policies, procedures, and controls to ensure the confidentiality, integrity, and availability of sensitive data. Information Security Management encompasses various aspects such as risk assessment and management, incident response planning, security awareness training programs, and the continuous monitoring of security measures.

By effectively managing information security risks and vulnerabilities, organizations can safeguard their critical information from potential threats posed by cybercriminals or malicious insiders while ensuring business continuity and regulatory compliance in an increasingly interconnected digital landscape. Research plays a crucial role in the field of information security management, as it helps organizations stay ahead of emerging threats and protect sensitive data. Through research, professionals can identify vulnerabilities, analyze attack patterns, and develop effective countermeasures to safeguard against cyber-attacks. Furthermore, research facilitates the discovery of new technologies and methodologies that enhance security practices and ensure compliance with evolving regulations. By investing in research, organizations gain a deeper understanding of risks and can make informed decisions to mitigate potential threats[4]. Ultimately, this proactive approach not only strengthens an organization's security posture but also instills confidence among stakeholders in their ability to protect valuable information assets.

The key objectives of research on information security management encompass a range of crucial aspects. Firstly, it aims to identify and analyze emerging threats and vulnerabilities in the field of information security, enabling organizations to proactively mitigate risks. Secondly, research strives to develop effective strategies and frameworks for managing information security, ensuring the confidentiality, integrity, and availability of sensitive data. Moreover, it seeks to evaluate the impact of regulatory compliance on information security practices and explore ways to align them effectively.

Additionally, research endeavors to investigate human factors that contribute to security breaches and devise methods for enhancing employee awareness and adherence to best practices. Conducting research on information security management poses several challenges and limitations that researchers must navigate. One significant challenge is the ever-evolving nature of cyber threats and attacks, which requires researchers to constantly update their knowledge and methodologies. Additionally, access to relevant data can be limited due to privacy concerns or corporate policies, making it difficult to obtain comprehensive information for analysis.

Understanding the Concept of Environmental Uncertainty

Understanding the concept of environmental uncertainty is crucial in the context of information security management. Environmental uncertainty refers to the complexity and unpredictability of external factors that can impact an organization's information security. These factors may include technological advancements, regulatory changes, economic conditions, political instability, and emerging threats. By comprehending environmental uncertainty, organizations can better anticipate potential risks and vulnerabilities to their information systems. This understanding allows them to develop proactive strategies to protect sensitive data and ensure business continuity. Moreover, it enables organizations to stay ahead in an ever-evolving landscape, adapt their security measures accordingly and make informed decisions regarding resource allocation for effective information security management.[5].

Environmental Uncertainty and Its Impact on Information Security Management

According to Singh & Gupta [6], in today's rapidly evolving technological landscape, organizations face an unprecedented level of environmental uncertainty. Factors such as advances in technology, globalization, regulatory changes, and the increasing sophistication of cyber threats contribute to this uncertainty. This uncertain environment poses significant challenges for information security management within organizations. The ability to effectively manage information security risks is critical to ensuring the confidentiality, integrity, and availability of sensitive data.

The relationship between environmental uncertainty and information security management is a critical aspect to consider in today's rapidly evolving digital landscape. Environmental uncertainty refers to the unpredictability and complexity of the external environment that organizations operate within, including technological advancements, regulatory changes, and emerging threats. Information security management involves strategies and practices aimed at protecting an organization's sensitive data and ensuring its confidentiality, integrity, and availability. The dynamic nature of environmental uncertainty poses significant challenges for effective information security management as it requires constant adaptation to mitigate emerging risks. Organizations must proactively assess their environment's uncertainty levels to develop robust information security frameworks that can effectively respond to evolving threats while maintaining business continuity. Thus, navigating through environmental uncertainty is crucial for effective information security management. The ever-evolving landscape of technology and the increasing sophistication of cyber threats pose significant challenges for organizations [7]. To address these challenges, information security managers must adopt a proactive approach that embraces continuous monitoring, risk assessment, and adaptation to changing circumstances. By staying informed about emerging threats and trends in the industry, organizations can better anticipate and respond to potential risks. Additionally, fostering a culture of cyber security awareness and education among employees is vital in mitigating vulnerabilities. Ultimately, by remaining vigilant and adaptive in the face of environmental uncertainty, organizations can ensure robust information security management practices that safeguard critical assets and uphold customer trust [8].

I.T Competence

In today's rapidly evolving digital landscape, having IT. competence has become an essential skill for individuals and organizations alike. IT. competence refers to the ability to effectively and efficiently use information technology tools and resources to solve problems, improve productivity, and achieve desired outcomes. It encompasses a wide range of knowledge and skills, including computer literacy, programming abilities, data analysis, cyber security awareness, and proficiency in various software applications. IT. competence is crucial in both personal and professional domains. From managing personal finances to collaborating with colleagues on complex projects, individuals need a solid foundation in IT competence to navigate the digital world successfully. For businesses, IT. competence is a key driver of innovation, enabling them to streamline operations, enhance customer experiences, analyze data for strategic decision-making, and stay competitive in the market. In the digital age, IT. competence has become increasingly important as technology continues to shape and redefine our personal and professional lives. It is no longer sufficient to simply possess basic computer skills; individuals must develop a deeper understanding of information technology to thrive in this rapidly evolving landscape. IT. competence is crucial for various reasons. Firstly, it enables individuals to effectively navigate and utilize the vast array of digital tools available today. From online collaboration platforms to data analysis software, being IT. competent empowers individuals to harness these tools for increased productivity and efficiency [9]. Furthermore, IT. competence is essential for adapting to new technologies and staying ahead in the job market. As automation and artificial intelligence continue to disrupt traditional industries, those with strong IT skills will be better equipped to embrace these changes and remain relevant in their respective fields. Overall, in an era where technology permeates every aspect of our lives, developing IT. competence has become a fundamental requirement for success in both personal endeavors and professional pursuits [10].

Significance of Developing I.T Competence

Developing IT competence offers numerous benefits that can enhance both personal and professional growth. Firstly, possessing I.T. skills enable individuals to navigate the digital world with ease. This includes proficiently using various software applications, effectively browsing the internet, and efficiently managing electronic files. By acquiring IT. competence, individuals can save valuable time and effort in their daily tasks. Moreover, having IT skills is highly valued in today's job market. Employers seek candidates who possess technical proficiency to drive innovation and streamline processes within organizations. By developing IT. competence, individuals increase their employability and open doors to a wide range of career opportunities. Furthermore, cultivating IT. competence fosters critical thinking and problem-solving abilities. It enables individuals to analyze complex data sets, identify trends, and make informed decisions based on insights gained through technological tools. This competency also promotes effective communication by facilitating information sharing through various digital platforms.

Challenges Building and Maintaining I.T Competence

According to Van Kleef & Roome [11], building and maintaining I.T. competence is a challenging task that organizations face in today's rapidly evolving technological landscape. One of the major challenges is the constant need for up-skilling and reskilling of IT. professionals to keep pace with emerging technologies. As new trends like artificial intelligence, cloud computing, and cyber security emerge, organizations must invest in training programs to ensure their workforce remains competent. Additionally, attracting and retaining top IT talent poses a significant challenge. The demand for skilled IT professionals often exceeds the supply, leading to intense competition among organizations. Organizations must offer competitive compensation packages, provide opportunities for career growth, and foster a positive work environment to attract and retain talented individuals. Furthermore, another challenge lies in staying updated with ever-changing regulations and compliance requirements. Organizations must ensure their IT professionals understand these regulations to maintain data security and privacy standards. Lastly, the rapid obsolescence of technology necessitates continuous learning and adaptation.

I.T Competence and Information Security Management

In today's digital age, organizations heavily rely on information technology IT to streamline operations, enhance productivity, and gain a competitive edge. However, this increased reliance on IT also brings forth significant challenges in terms of information security. The importance of safeguarding sensitive data and ensuring the confidentiality, integrity, and availability of systems and information cannot be overstated. IT. competence refers to the knowledge, skills, and abilities required to effectively manage I.T. resources within an organization. It encompasses various areas such as network administration, software development, database management, and cyber security [12]. By possessing a strong IT. competence framework, organizations can ensure that their employees have the necessary expertise to handle the complexities associated with managing IT. systems securely. Information security management is a crucial component of any organization's overall risk management strategy. It involves implementing measures to protect information assets from unauthorized access or disclosure while also addressing potential threats and vulnerabilities [13].

Enhancing I.T Competence for Information Security

Continuous Training and Skill Development: Foster a culture of continuous learning within the organization by providing regular training programs and opportunities for employees to enhance their IT competence and stay up-to-date with the latest technologies and security practices. Accordingly, implementing a comprehensive recruitment process that includes thorough screening of candidates' IT skills and knowledge, ensures that only competent individuals with a strong understanding of information security are hired. Similarly, encourage collaboration between different teams within the organization, such as IT., human resources, legal, and management, to ensure that information security measures are integrated into all aspects of business operations. 4. Regular Risk Assessments: Conduct regular risk assessments to identify potential vulnerabilities in the organization's IT infrastructure [14]. This will help in developing effective strategies for mitigating risks and enhancing information security [15].

Challenges and Risks in I.T Competence and Information Security Management

The increasing reliance on technology and the constant evolution of cyber threats pose significant challenges and risks in IT competence and information security management. One key challenge is the shortage of skilled professionals with expertise in information security. The demand for qualified individuals who can effectively implement robust security measures often exceeds the available supply, leaving organizations vulnerable to potential breaches [16]. Another challenge lies in ensuring continuous training and development programs for existing IT personnel. As technology rapidly evolves, it becomes essential to keep employees updated with the latest skills and knowledge required to address emerging threats effectively. Failure to do so may result in outdated practices that can easily be exploited by malicious actors. Furthermore, managing the complexity of IT systems presents inherent risks [10]. As organizations adopt new technologies, their infrastructure becomes increasingly intricate, making it harder to identify vulnerabilities or potential points of failure. Lastly, maintaining a proactive approach towards cyber security is critical but challenging[6]

Future Trends in I.T Competence and Information Security

As technology continues to advance at an exponential rate, the future of IT competence and information security management will undoubtedly undergo significant transformations. One of the key trends that will shape this field is the increasing demand for professionals with expertise in emerging technologies such as artificial intelligence, blockchain, and cloud computing. Organizations will seek individuals who can navigate these complex systems while ensuring robust information security measures are in place [10]. Furthermore, the rise of remote work and the Internet of Things (IoT) will present new challenges and opportunities for IT professionals. With an ever-expanding network of interconnected devices, ensuring information security across various platforms and endpoints will become paramount.

Moreover, as cyber threats become more sophisticated, there will be a growing emphasis on proactive approaches to information security management [7]. This includes implementing advanced threat detection systems, conducting regular vulnerability assessments, and fostering a culture of cyber security awareness within organizations.

3. CONCEPTUAL FRAMEWORK AND HYPOTHESES TESTING

Based on the review of the literature, the current study tested the following framework and hypotheses:

H1: There will be a positive relationship between environmental uncertainty and information security management

H2: There will be a positive relationship between I.T competence and information security management

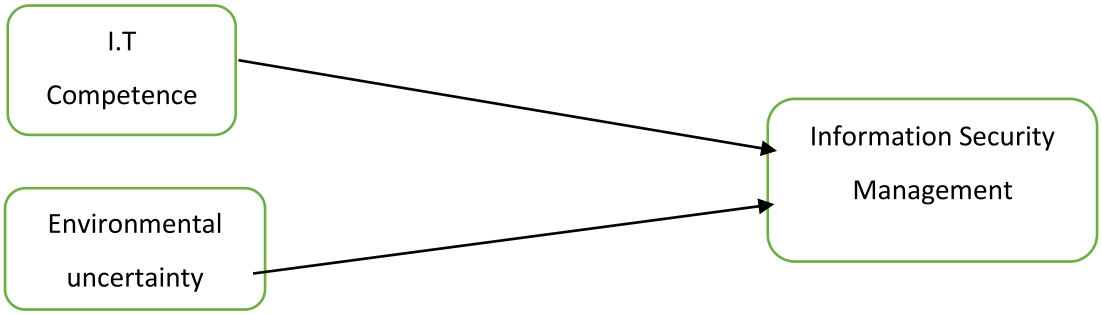

Figure 1: Conceptual Model

4. METHODOLOGY

Sampling

Retail sector was targeted in the current study. A total of 500 individuals in the managerial positions in the general merchandise retail sector were targeted using the convenience sampling approach. The study managed to receive 411 responses out of which 38 were found to be not appropriately done. Therefore, 373 were taken for final analysis and interpretation.

Measurement Model Assessment

For measurement model current research assessed the measurement model through the PLS algorithm to check reliability and validity by using Smart PLS. table 01 and figure (measurement model) show the findings about the measurement model.

Table 01: Reliability and validity

Item code	Loading	CR	AVE
Environmental uncertainty		**0.878**	**0.548**
EU1	0.647		
EU2	0.720		
EU3	0.779		
EU4	0.849		
EU5	0.763		
EU6	0.666		
Information Security Management		**0.937**	**0.714**
ISM1	0.904		
ISM2	0.776		
ISM3	0.847		
ISM4	0.685		
ISM5	0.913		
ISM6	0.921		
I.T competence		**0.933**	**0.584**
ITC1	0.707		
ITC10	0.757		
ITC2	0.813		
ITC3	0.767		
ITC4	0.679		
ITC5	0.698		
ITC6	0.794		
ITC7	0.817		
ITC8	0.798		
ITC9	0.796		

Individual item reliability (Factor loading)

Assessment of factor loading is used to assess the individual item reliability [17, 18]. The threshold factor of loading for retaining item is 0.50 and above [17]. In current research factor loading was examined for each item and results showed loading of each item well above the stated threshold. Hence based on the results of factor loading this can be narrated that each item has sufficient reliability in current research. Loadings found in the research are presented in Table 01.

1.Internal consistency reliability (CR)

CR can be used to assess reliability [18, 19]. CR values above 0.70 shown as good [20, 23]. Findings on CR values is presented in table 01. By following the results this can be narrated that sufficient internal consistency reliability was achieved.

1.1Convergent validity (AVE)

Threshold for AVE of 0.50 [21] was recommended. Results for current study about AVE are presented in table 01. All values of AVE were found greater than the stated threshold which shows that current research has achieved sufficient convergent validity.

1.2Discriminant validity

For the assessment of discriminant validity, two approaches are recommended. One is the square root of AVE [24] second is HTMT values [25]. In Table 02, all square roots of AVE were found greater than other corresponding values. In HTMT criteria all HTMT values need to be less than HTMT 0.90, [26, 27]. Table 03 represents HTMT values. Results on HTMT values show all understated thresholds. Hence based on results in the stated criteria represent that current research has achieved sufficient level of discriminant validity.

Figure 2: Measurement Model

Assessment of Structural Model

Sarstedt, et al. [17] has recommended to apply bootstrapping procedure to check path coefficients through Smart PLS. current research used 5000 resamples bootstrapping approach to assess the path coefficients. Path coefficients show the level of strength of relationship between exogenous and endogenous variables [28]. Current research tested two relationships environmental uncertainty with information security management and second was I.T competence and information security management. Both hypotheses were found significant

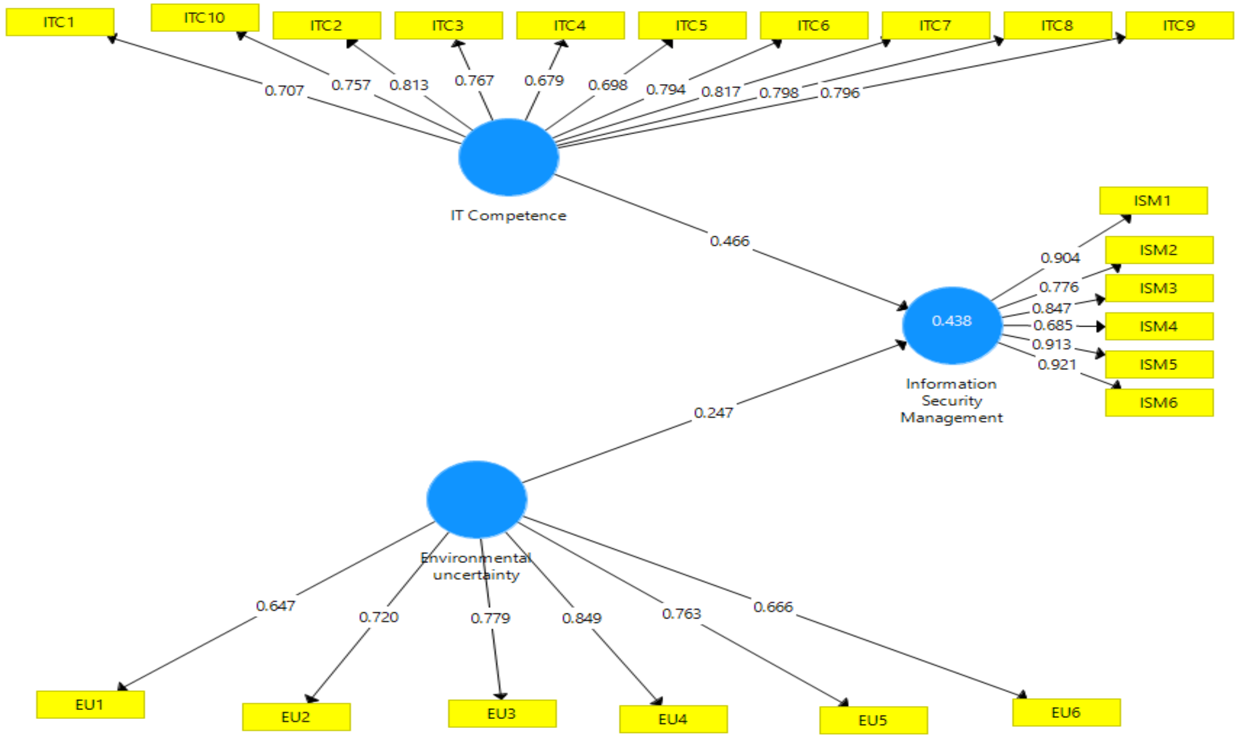

Figure 2: Strictural model

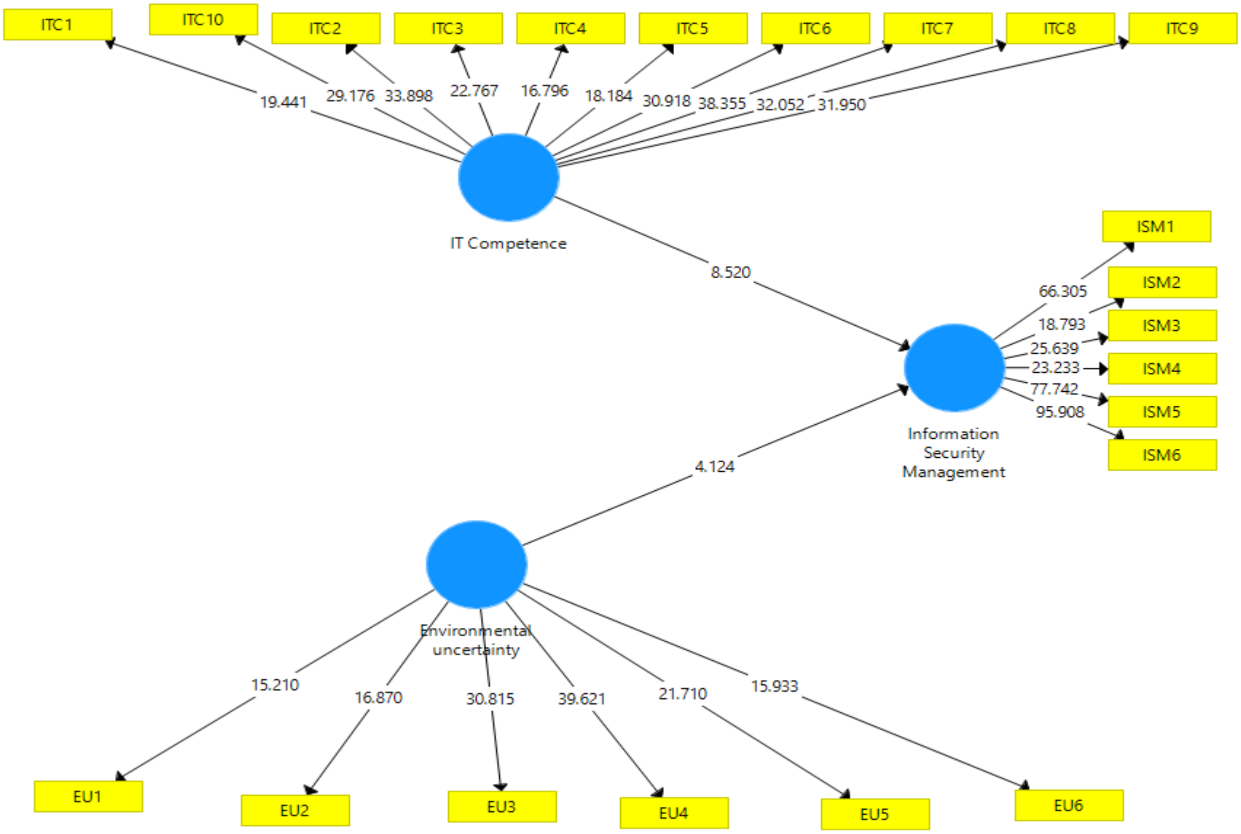

Figure 3: Structural Model

Table 02: Square root of AVE [24]criteria

Construct	EU	ITC	ISM
Environmental uncertainty	0.741		
IT Competence	0.693	**0.764**	
Information Security Management	0.570	0.637	**0.845**

Table 03: HTMT Criteria

Construct	EU	ITC	ISM
Environmental uncertainty	==		
I.T Competence	0.781	==	
Information Security Management	0.616	0.642	==

Table 04: Path Assessment

Hypothesis	Beta	STDEV	T value	P value
EU>ISM	0.247	0.060	4.124	0.000
ITC>ISM	0.466	0.055	8.520	0.000

R square is another way of assessment structural model. It is also known as coefficient of determination [23]. Prominent scholars have recommended different acceptable ranges of R^2 value based on nature of the research [20]. Current research has found R square values as moderate level. Results are presented in table 05.

Table 05: Variance explained in endogenous variable (R^2)

Variable	R^2	Adjusted R^2
Information Security Management	0.438	.434

Effect size can be defined as relative effect of single independent variable on dependent variable with relative to change in R^2 [28]. Recommended range of effect size of 0.02 is treated as small, 0.15 up to 0.34 treated as medium and 0.35 and above treated as large effect size. Results are presented in table 06 which indicate the small and medium effect level.

Table 06: Effect size (f^2)

Variable	Information Security Management	effect
Environmental uncertainty	0.056	Small
IT Competence	0.201	Medium

Blindfolding

Current study also assessed the model through predictive relevance. For this current study used Stone-Geisser test through blindfolding [10]. Predictive relevance is used to assess good of Fit model as additional tool to assess model [10]. Current study utilized the blindfolding option which is applied only to endogenous variables [31, 32]. In blindfolding for assessing predictive relevance cross validated redundancy (Q^2) test was executed [29, 33, 34]. Predictive relevance achieved when Q^2 value is found more than zero [28, 35]. Table 07 show the results. Current research has found Q-square values above zero. Current research has found good fit of model.

Table 07: Predictive relevance

Factor	SSO	SSE	Q2=(1-SSE/SSO)
Information Security Management	1788.000	1294.909	0.276

5. DISCUSSION AND IMPLICATIONS

The current study attempted to investigate the role of environmental uncertainty and I.T competence towards boosting information security management. The results have revealed that organizations facing high environmental uncertainty strive harder to improve their information security. This hence outlines that organizations facing a challenging environment tend to focus more and strategically work to improve their information security protocols. This hence suggests policy makers consider environmental scanning to understand the level of environmental uncertainty and ensure the robustness of their information security accordingly to avoid any unintended consequences. Notably, in the current era of growing complexities and insecurities in the business environment, it has become even more important for companies to ensure they have tight controls when it comes to information security management.

Accordingly, the current study also found a significant relationship between IT competence and information security management. This suggests that companies with stronger technological functionality were able to boost their information security. This outlines how crucial it is for businesses to improve their IT competence to handle any criticalities a business is facing. This implies for policymakers and management entities to invest in IT technologies and skills. The businesses in retail need also look out of recruiting the right talent that it technologically advanced and can help them boost their information security management. This also indicates the need and demand for training and development interventions that can help companies equip their staff accordingly.

6. LIMITATIONS AND SCOPE FOR FUTURE STUDIES

The current study presents the following avenues for future studies. First, the current study deployed a cross-sectional research design for data collection thus limiting the generalizability of the study findings. Future studies are thus advised to consider testing the framework with a longitudinal design. Secondly, the study focused on retail businesses thus it is advised for scholars engaged in this area to consider other occupational sectors. Third, the current study tested the direct relationship between environmental uncertainty, I.T competence, and information security management It may be interesting to test and outline any mediating or moderating variables in the study that would help booth understanding of information security management.

7. REFERENCES

1. Soomro ZA, Shah MH, Ahmed J. Information security management needs more holistic approach: A literature review. Int J Inf Manag. 2016;36(2):215-25. doi: 10.1016/j.ijinfomgt.2015.11.009.
2. Baker WH, Wallace L. Is information security under control?: investigating quality in information security management. IEEE Secur Privacy Mag. 2007;5(1):36-44. doi: 10.1109/MSP.2007.11.
3. Moustafa AA, Bello A, Maurushat A. The role of user behaviour in improving cyber security management. Front Psychol. 2021;12:561011. doi: 10.3389/fpsyg.2021.561011, PMID 34220596.
4. Zammani M, Razali R, Singh D. Factors contributing to the success of information security management implementation. IJACSA. 2019;10(11). doi: 10.14569/IJACSA.2019.0101153.
5. Kobis P. Human factor aspects in information security management in the traditional IT and cloud computing models. Oper Res Decis. 2021;31(1). doi: 10.37190/ord210104.
6. Singh AN, Gupta MP. Information security management practices: case studies from India. Glob Bus Rev. 2019;20(1):253-71. doi: 10.1177/0972150917721836.
7. Chen J, Wang X, Shen W, Tan Y, Matac LM, Samad S. Environmental uncertainty, environmental regulation and enterprises' green technological innovation. Int J Environ Res Public Health. 2022;19(16):9781. doi: 10.3390/ijerph19169781, PMID 36011417.
8. Bokhari S, Hamrioui S, Aider M. Cybersecurity strategy under uncertainties for an IoE environment. J Netw Comput Appl. 2022;205:103426. doi: 10.1016/j.jnca.2022.103426.
9. Tsohou A, Holtkamp P. Are users competent to comply with information security policies? An analysis of professional competence models. Inf Technol People. 2018;31(5):1047-68. doi: 10.1108/ITP-02-2017-0052.
10. Haqaf H, Koyuncu M. Understanding key skills for information security managers. Int J Inf Manag. 2018;43:165-72. doi: 10.1016/j.ijinfomgt.2018.07.013.
11. Van Kleef JAG, Roome NJ. Developing capabilities and competence for sustainable business management as innovation: a research agenda. J Cleaner Prod. 2007;15(1):38-51. doi: 10.1016/j.jclepro.2005.06.002.
12. Bassellier G, Benbasat I. Business competence of information technology professionals: conceptual development and influence on IT-business partnerships. MIS Q. 2004;28(4):673-94. doi: 10.2307/25148659.
13. Welty Peachey JW, Cohen A, Shin N, Fusaro B. Challenges and strategies of building and sustaining inter-organizational partnerships in sport for development and peace. Sport Manag Rev. 2018;21(2):160-75. doi: 10.1016/j.smr.2017.06.002.
14. Ahmed U, Zin MLM, Majid AHA. Impact of intention and technology awareness on transport industry's E-service: evidence from an emerging economy. *산경연구논집 (JIDB)*. IJIDB. 2016;7(3):13-8. doi: 10.13106/ijidb.2016.vol7.no3.13.
15. Thomson KL, von Solms R. Towards an information security competence maturity model. Comput Fraud Sec. 2006;2006(5):11-5. doi: 10.1016/S1361-3723(06)70356-6.

16. Alghazo SHA, Humaidi N, Noranee S. Assessing information security competencies of firm leaders towards improving procedural information security countermeasure: awareness and cybersecurity protective behavior. Inf Manag Bus Rev. 2023;15(1(I)SI)(1 (I) SI):1-13. doi: 10.22610/imbr.v15i1(I)SI.3408.
17. Sarstedt M, Ringle CM, Smith D, Reams R, Hair JF. Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers. J Fam Bus Strategy. 2014;5(1):105-15. doi: 10.1016/j.jfbs.2014.01.002.
18. Mccrae RR, Kurtz JE, Terracciano A. Internal consistency, retest reliability, and their implications for personality scale validity. Pers Soc Psychol Bull. 2011;15(1):28-50. doi: 10.1177/1088868310366253.Internal.
19. Peterson RA, Kim Y. On the relationship between coefficient alpha and composite reliability. J Appl Psychol. 2013;98(1):194-8. doi: 10.1037/a0030767, PMID 23127213.
20. Hair JF, Black WC, Babin BJ, Anderson RE. Multivariate data analysis. 7th ed. Upper Saddle River, NJ: Prentice Hall; 2010.
21. Hair JF, Hult GTM, Ringle CM, Sarstedt M. A primer on partial least squares structural equation modeling. 2nd ed. Thousand Oaks, CA: SAGE; 2017.
22. Bagozzi RP, Yi Y. On the evaluation of structural equation models. J Acad Mark Sci. 1988;16(1):74-94. doi: 10.1007/BF02723327.
23. Hair JF, Ringle CM, Sarstedt M. PLS-SEM: indeed, a silver bullet. J Mark Theor Pract. 2011;19(2):139-52. doi: 10.2753/MTP1069-6679190202.
24. Fornell C, Larcker DF. Evaluating Structural Equation Models with unobservable variables and measurement error. J Mark Res. 1981;18(1):39-50. doi: 10.1177/002224378101800104.
25. Henseler J, Ringle CM, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. J Acad Mark Sci. 2015;43(1):115-35. doi: 10.1007/s11747-014-0403-8.
26. Gold AH, Malhotra A, Segars AH. Knowledge management: an organizational capabilities perspective. J Manag Inf Syst. 2001;18(1):185-214. doi: 10.1080/07421222.2001.11045669.
27. Teo TSH, Srivastava SC, Jiang L. Trust and electronic government success: an empirical study. J Manag Inf Syst. 2008;25(3):99-132. doi: 10.2753/MIS0742-1222250303.
28. Chin WW. The partial least squares approach to structural equation modeling. In: Marcoulides GA, editor. Modern methods for business research. Mahwah, NJ: Lawrence Erlbaum Associates; 1998.
29. Geisser S. The predictive sample reuse method with applications. J Am Stat Assoc. 1975;70(350):320-8. doi: 10.1080/01621459.1975.10479865.
30. Duarte P, Raposo M. A PLS model to study brand preference: an application to the mobile phone market. In: Esposito Vinzi V, Chin WW, Henseler J, Wang H, editors. Handbook of partial least squares. Berlin: Springer Heidelberg; 2010. p. 449-85.
31. Sattler H, Völckner F, Riediger C, Ringle CM. The impact of brand extension success drivers on brand extension price premiums. Int J Res Mark. 2010;27(4):319-28. doi: 10.1016/j.ijresmar.2010.08.005.
32. McMillan B, Conner M. Using the theory of planned behaviour to understand alcohol and tobacco use in students. Psychol Health Med. 2003;8(3):317-28. doi: 10.1080/1354850031000135759.
33. Hair JF, Ringle CM, Sarstedt M. Partial least squares structural equation modeling: rigorous applications, better results and higher acceptance. Long Range Plann. 2013;46(1-2):1-12. doi: 10.1016/j.lrp.2013.01.001.
34. Ringle CM, Sarstedt M, Straub DW. Editor’s comments: a critical look at the use of PLS-SEM in “MIS Quarterly”. MIS Q. 2012;36(1):iii-xiv. doi: 10.2307/41410402.
35. Hair JF, Hult GTM, Ringle CM, Sarstedt M. A primer on partial least squares structural equation modeling (PLS-SEM). UK: SAGE; 2014a

.