Contents available at the publisher website: G A F T I M . C O M

International Journal of Computations, Information and Manufacturing (IJCIM)

Journal homepage: https://journals.gaftim.com/index.php/ijcim/index

Impact of Information Security on Online Operations: The Mediating Role of Risk Management

Keltoum Bentameur [1], Boudjema Iguenane [2]

[1] *University of Mohamed El Bachir El Ibrahimi, Algeria*

[2] *uTihoo for Artificial Intelligence, France*

A R T I C L E I N F O

Keywords:

Risk Management, Online Transaction, Information Security, Cyber Detect.

Received: May, 14, 2023

Accepted: June, 22, 2023

Published: June, 23, 2023

A B S T R A C T

Online operations are becoming a crucial component of the healthcare ecosystem in the modern world. But, as technology has become more widely used, so too has the risk of cyberattacks grown. Implementing information security measures is therefore crucial if we are to preserve sensitive patient data and maintain online operations. By recognizing, evaluating, and controlling possible dangers, risk management is essential in reducing these risks. In order to understand how information security affects online operations in the healthcare sector, this study will look at the mediating role of risk management. A hypothetical model was assessed using SmartPLS 4.0 containing 132 respondent's data from 56 healthcare providers (hospitals) in Dubai UAE. The empirical results can offer insightful information about the significance of information security and risk management in guaranteeing the security and safety of sensitive patient data in the context of online healthcare.

1. INTRODUCTION

Information security is now of utmost importance to enterprises, especially those in the healthcare industry. Healthcare organizations must take the necessary precautions to maintain the security, integrity, and availability of their information in light of the growing volume of sensitive patient information being stored and exchanged electronically. Healthcare businesses are exposed to a variety of risks, not just information security issues. They must also control risks related to patient security, legal compliance, economic security, and other things. In order to maintain the continuity and sustainability of healthcare services, good risk management is essential. This review of risk management in healthcare with a focus on information security will cover the significance of risk management, fundamental ideas and principles, and best practices for managing risks. (Naeem et al., 2019) introduced a scalable mutation testing approach that utilizes predictive analysis of a deep learning model, offering insights that can contribute to understanding the potential impact of information security measures on online operations through improved risk management

Online operations and information security are essential components of the healthcare sector. The need to keep patient data private has become critical as healthcare professionals depend more and more on technology to store and exchange patient data. Sensitive patient information must be protected by healthcare institutions from cyber threats such data breaches, ransomware attacks, and phishing schemes. With the rise of

telemedicine and remote patient monitoring in recent years, online operations in healthcare have also grown in significance. Although these technologies have helped healthcare practitioners increase patient outcomes and access to care, they also present a special set of security problems. (Saeed, 2023a) and (Saeed, 2023b) explains the role of security and privacy in e-commerce and digital workspaces. Moreover, healthcare firms must have strong information security processes and systems in place to guard against cyber threats given the sensitive nature of patient information. Implementing safe software and hardware, educating workers about cybersecurity best practices, and regularly auditing and evaluating their security posture are all part of this. In this situation, healthcare companies must adopt an all-encompassing strategy for information security and online operations, incorporating security into every facet of their work and placing a constant emphasis on the protection of patient data. By doing this, they can contribute to ensuring that patients receive high-quality, secure care in a reliable setting.

2. LITERATURE REVIEW

2.1. Information Security and Risk Management

Due to the prevalence and sophistication of cyber threats, information security is becoming more and more crucial to risk management. There are several things to take into account to make sure that information security measures are successful in limiting risk, according to several studies. According to (Federico Del Giorgio, 2022), using risk management frameworks is a crucial component of information security. These frameworks offer a methodical method for detecting, evaluating, and reducing risks and can be customized for particular businesses or groups. For addressing cybersecurity risk in critical infrastructure sectors, for instance, the National Institute of Standards and Technology (NIST) Cybersecurity Framework offers a collection of recommendations and best practices. In addition, the function of employees in information security is another important factor. Organizations must give enough training and resources to ensure that employees understand the risks and how to reduce them. Employee conduct and knowledge are crucial in averting cyber assaults. Organizations must also have policies and procedures in place to deal with security issues, guarantee that they are reported right away, and make sure they are dealt with. External factors, like laws and industry norms, can also have an impact on how successful information security procedures are.

H1: There is significant relationship between Information Security and Risk Management.

2.2. Information Security and Online Operations

A prior study demonstrated many ways in which information security benefited online operations (Von Solms and Van Niekerk, 2013). First of all, it decreased the possibility of data breaches and raised client confidence, which increased sales and revenue. By minimizing the time and effort required to address security events, it improved the efficiency and efficacy of online operations. Lastly, it assisted companies in adhering to legal and regulatory obligations, helping them avoid exorbitant fines and legal actions. The authors discovered that a few other factors affected how information security affected online operations (Bandyopadhyay et al., 2010). For instance, it was discovered that the influence of information security on online operations depends on the size of the organization, the type of business, and the level of security investment. Information security was shown to have a greater impact on bigger companies and those in the financial industry than on smaller companies and those in other industries. Overall, the research indicates that the success of online activities depends heavily on information security. To increase the effectiveness and efficiency of their online operations as well as customer trust and confidence, businesses must invest in information security. The report offers insightful advice for businesses looking to enhance their online operations through information security spending.

H2: There is significant relationship between Information Security and Online Operations.

2.3. Risk Management and Online Operations

As highlighted by (Chu et al., 2020), the use of risk assessment tools and frameworks is a crucial factor in risk management for online operations. These tools can assist businesses in risk identification and

prioritization, risk assessment of likelihood and possible impact, and risk mitigation strategy development. For instance, the ISO 27001 standard, which can be used for online operations, offers a framework for addressing information security threats. The requirement for a thorough security strategy is a crucial component of risk management for online operations. This entails putting in place suitable security measures including firewalls, antivirus software, and encryption as well as conducting regular security tests and assessments. In order to ensure a prompt and efficient reaction in the event of a security breach, companies should also have an incident response strategy in place. The literature also underlines how crucial employee education and awareness are to reducing risk in online business operations. Organizations must give enough training and resources to ensure that employees understand the dangers and how to manage them. Employees play a crucial role in preventing cyber assaults and securing sensitive information.

H3: There is significant relationship between Risk Management and Online Operations.

2.4. Information Security impact on Online Operations with mediating role of Risk Management

For businesses that operate online, information security is a crucial. While concerning the security of online transactions have been raised due to the rise in security lapses and cyberattacks, which can result in monetary loss, reputational harm, and legal consequences. According to (Min, 2019), risk management is essential for organizations to minimize the impact of security breaches and cyber-attacks on their online operations. This framework also considers the impact of information security on online operations and how risk management can mediate this impact. In one study, investigate how risk management acts as a mediator in how information security affects online operations in Chinese e-commerce enterprises. The study discovered that risk management mediates the positive impact of information security on online operations. The study also discovered that risk management benefits online business. Another study by (Sindhuja, 2014) looks at how online buying behavior is impacted by information security, including the roles of risk perception and risk management. The study discovered that risk management efficiently supports the information security, which has a considerable positive impact on online purchasing behavior. The study also discovered that risk perception had a detrimental effect on consumers' online shopping behavior.

(Bottle and Aylin, 2008) study explores how risk management functions as a mediating factor in the UAE when examining the influence of information security on the adoption of online banking. The study discovered that risk management mediates the influence of information security, which has a considerable beneficial impact on the adoption of online banking. The study also discovered that the adoption of internet banking is positively impacted by risk management (Fan et al., 2015). In a study (Rachid et al., 2017), the mediating effects of risk perception and risk management are examined in relation to the influence of information security on online buying behavior in China. The study discovered that risk management mediates the influence of information security, which has a considerable impact on online shopping behavior. However, there are few components have been discussed in order to assess the risk and manage within the information security concerns, for instance, “risk identification”, “risk analysis’, and “risk mitigation”. The use of risk assessment frameworks, such as the ISO/IEC 27005 standard, which offers a systematic approach to identifying and analyzing risks in information security, is one well-known method of risk identification. Identifying assets and their values, identifying threats and vulnerabilities, evaluating the likelihood and effect of risks, and choosing appropriate controls to manage risks are all stages that are often included in these frameworks (Brandon-Jones et al., 2014).

The use of threat modelling techniques, which entail identifying potential threats and attack vectors to a system or application, is another method of risk identification. These methods usually entail building a thorough model of the system or application, spotting potential threats and vulnerabilities, and figuring out how likely and damaging these threats are to be. However, information security relies heavily on the process of risk analysis, which examines potential threats and weaknesses to information assets and evaluates their likelihood and potential effects.

Using quantitative risk analysis approaches, such as the annualized loss expectancy (ALE) method, is one method of doing risk analysis. Based on the likelihood that the breach will occur and the potential consequence of the breach, this method estimates the cost of a prospective security breach over a one-year period. Moreover, risk mitigation is a critical process in information security that involves implementing controls and strategies to reduce the likelihood and potential impact of risks to information assets. Using technical controls like firewalls, intrusion detection and prevention systems, and encryption is one method of risk reduction. These safeguards are intended to stop illegal access to information assets, identify and address potential security holes, and guard against unauthorized disclosure or alteration of sensitive data. The prior studies evidences proven there is no mediation of risk management in the relationship between information security and online operations in healthcare sector. Based on the above literature following hypothesis was developed:

H4: There is significant relationship between risk identification and online operations using information security.

H5: There is significant relationship between risk analysis and online operations using information security.

H6: There is significant relationship between risk mitigation and online operations using information security.

H7: There is significant relationship between information security and online operations with mediating role of risk management.

2.5. Research Model

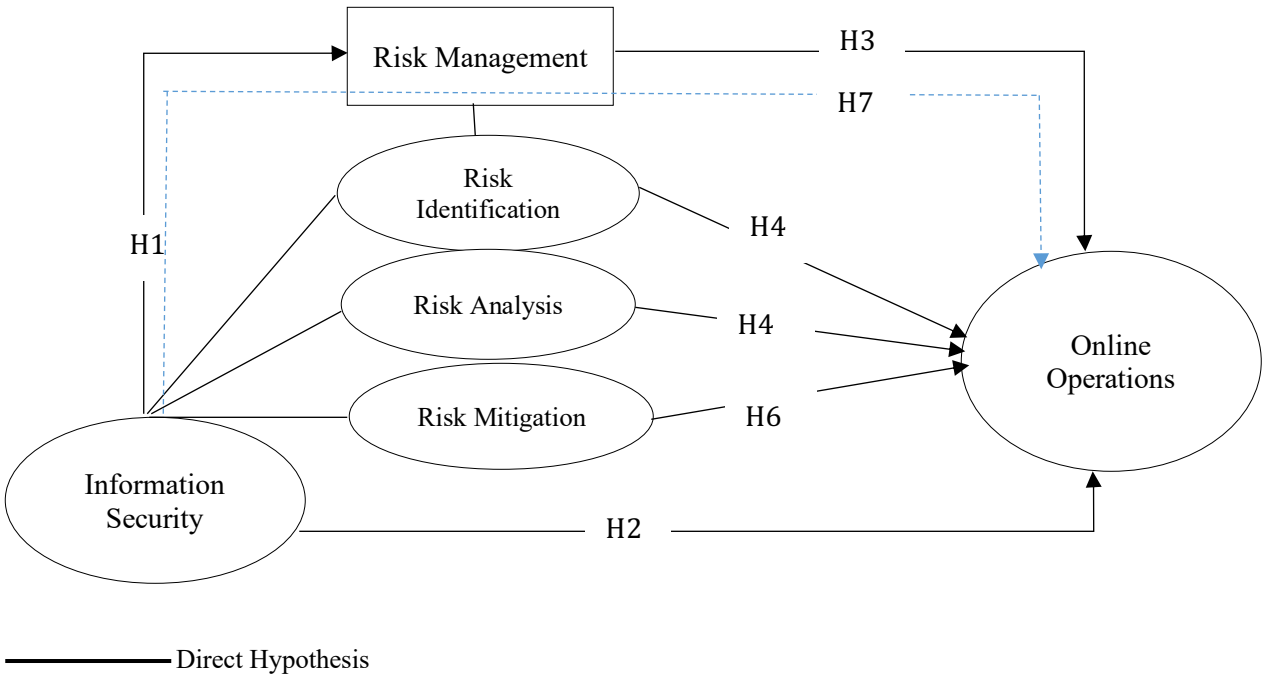

Figure 1: Research Model

3. METHODOLOGY

The research was conducted to examine the impact of information security on online operations with mediating role of risk management. These variables were assessed using a quantitative technique to collect empirical evidences from healthcare sector located in UAE. however, the healthcare sector has increased to adopt the information security because of using technological techniques in the business models. So the managerial employees were targeted to respond our survey questionnaire in order to collect primary data of the research. 56 public and private hospitals were approached to get the responses. 132 respondent's data were utilized to assess the research model.

The survey instrument was a five point likert scale questionnaire developed by authors. The questionnaire contained 23 items specified to each variable (dimension) respectively. The respondent's data were assessed using SmartPLS 4.0 software to validate the model. The model assessment inclusive of discriminant and convergent validity, PLS-SEM approach was applied to check path coefficients and significance level of the hypothesis. Empirical analysis section contains overall statistical analysis demonstrated below.

4. DATA ANALYSIS

4.1. Assessment of the Measurement Model

Reliability (item and internal consistency) and validity tests are included in the measuring model to validate the variables utilized in this investigation (convergent and discriminant). The validity and reliability of the construct are demonstrated in Table 1. The results (see Table 1) show that the structures' internal reliability was further validated using CA and CR values, and the outcome had to be greater than 0.60 to be considered acceptable. The results show that all factors' CA and CR values exceeded the recommended value of 0.60, indicating that the study met the requirements for internal consistency and reliability.

Table 1: Composite Reliability, Cronbach's Alpha, AVE, HTMT

Variables	IS	RM	OO	RI	RA	RMT	CA	CR	AVE
Information Security	-						0.871	0.899	0.636
Risk Management	0.564	-					0.844	0.829	0.613
Online Operations	0.619	0.459	-				0.917	0.844	0.722
Risk Identification	0.655	0.681	0.554	-			0.814	0.907	0.654
Risk Analysis	0.722	0.634	0.611	0.639	-		0.732	0.898	0.578
Risk Mitigation	0.598	0.797	0.723	0.765	0.583	-	0.865	0.836	0.620

IS=Information Security, RM=Risk Management, OO=Online Operations, RI=Risk Identification, RA=Risk Analysis, RMT=Risk Mitigation, AVE=Average Variance Extracted, CA=Cronbach's Alpha

The convergent validity of the research variables was also examined using the AVE value, and the results revealed that the AVE values ranged from 0.501 to 0.640, which is higher than the recommended value of 0.50. It is plausible to conclude that the research variables satisfy convergent validity as a result. The validity (discriminant) of the research variables was also evaluated using the heterotrait-monotrait correlation ratio (HTMT). The results showed that, no problems with discriminant validity are shown by the HTMT values for all components being less than 0.85. The results display that the variables under study have strong discriminant validity.

Table 1 demonstrate overall results.

4.2. Structured Equation Modeling and Hypothesis Testing

The structural model is evaluated after the establishment of the measurement model, and the hypothesis is then tested. The study employed PLS-SEM and employed a boot-strapping resampling procedure with 5000 subsamples. In Figure 2 and Table 2, the outcomes of the hypothesis testing are displayed.

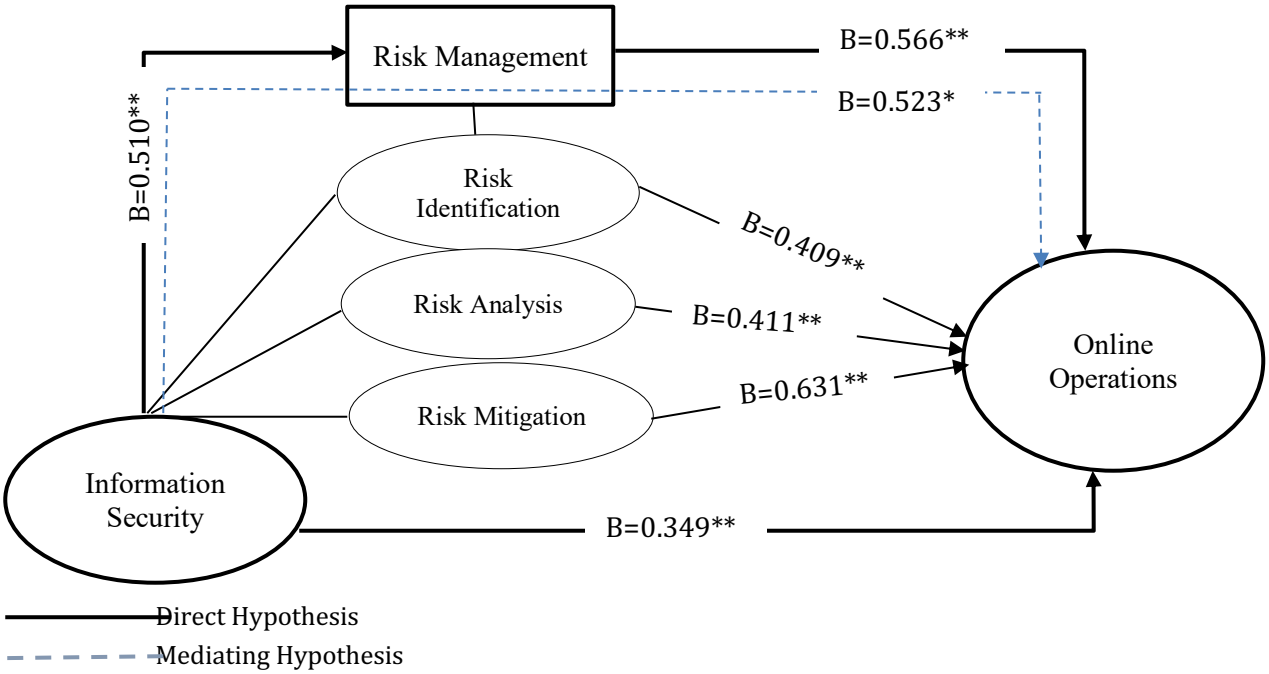

Figure 2: Structured Model Measurement

Additionally, the hypothesis testing findings exhibited, big data positively influence the demand forecasting (IS → RM β= 0.51, t = 4.31, p 0.000) supporting the H1. The results indicating a significant impact of information security on online operations as (IS → OO β= 0.34, t = 3.66, p 0.000), supporting H2 of the model. The H3 demonstrate the relationship between risk management and online operations a significant relationship by (β=0.56, t=2.99, p=0.000) supporting H3 of the model. In addition, the components of risk management were assessed with online operations that depicted significant relationship as (IS → RI → OO, β= 0.40, t=7.10, p=0.000), supporting H4. The impact of risk analysis showed as (IS → RA → OO, β= 0.41, t=5.51, p=0.000), and (IS → RMT → OO β= 0.63, t=9.11, p=0.003) shows the H6 is also accepted. Finally, the H7 representing the main mediating hypothesis revealed as partially mediated between the relationship of information security and online operations with path coefficients of (IS → RM → OO, β=0.52, t=6.34, p=0.000) indicating a support to H7 of the research model. Table2 and figure 2 demonstrate the hypothesis results.

Table 2: Hypothesis Testing using PLS-SEM

Paths	Beta	t-value	p-value	Decision
H1: Information Security → Risk Management	0.510	4.31	0.000	Supported
H2: Information Security → Online Operations	0.349	3.66	0.000	Supported
H3: Risk Management → Online Operations	0.566	2.99	0.000	Supported

H4: Information Security → Risk Identification → Online Operations	0.409	7.10	0.000	Supported
H5: Information Security → Risk Analysis → Online Operations	0.411	5.51	0.000	Supported
H6: Information Security → Risk Mitigation → Online Operations	0.631	9.11	0.002	Supported
H7: Information Security → Risk Management → Online Operations	0.523	6.34	0.000	Partial Mediation

*Note: Level of significance at p<0.05**, Critical Value,,t <1.69.*

5. DISCUSSION

Our research analysis proven to be said the significant impact of information security on online operations through risk analysis, identification and mitigation. However, due to the potentially serious and wide-ranging consequences of security breaches, information security is of the utmost importance for online activities. Without sufficient security measures, businesses run the danger of disclosing critical information, losing client confidence, and tarnishing their name. In order to reduce possible risks and the effects of security breaches on online operations, good risk management is crucial. One essential factor to take into account is how risk management influences how information security affects online operations. The process of discovering, evaluating, and reducing possible threats to information assets is known as risk management. Organizations can better safeguard their digital assets and lessen the impact of security breaches on their online operations by using the right risk management practices.

The empirical findings demonstrated the significance level of risk management on online operations. Similarly, implementing efficient security controls is one method risk management can mitigate the impact of information security on online operations. To prevent unauthorized access to their systems and safeguard sensitive data, for instance, businesses can put in place access controls, encryption, and intrusion detection systems. They may lessen the potential harm to their online operations and lower the likelihood and effect of security breaches by doing this. Furthermore, a culture of security can be established throughout the firm due to proper risk management. This include raising awareness of potential hazards, putting policies and procedures in place to lessen risks, and giving staff members security training. The findings suggest it's crucial to remember that risk management cannot totally avoid the possibility of security breaches having an adverse effect on online operations. Because cyber risks are dynamic in nature, enterprises must maintain vigilance and flexibility in their risk management procedures. To detect new threats and make sure that risk management solutions continue to work over time, regular risk assessments, vulnerability scans, and penetration testing are critical.

6. CONCLUSION

In conclusion, there has been noted a significant impact of information security on online operations with mediation of risk management. However, data security is an essential component of internet business in the healthcare industry. Effective risk management is a key mediator in reducing these risks because security breaches can have serious effects on patient data and online operations. Sensitive patient data must be protected from illegal access, modification, or disclosure, so healthcare companies must put in place effective risk management plans that involve technical and administrative controls. Additionally, they must make sure that all employees are compliant with all applicable legal and regulatory obligations, as well as aware of any risks and how to minimize them. Moreover, the ability to manage risk effectively is essential for preserving the confidence of patients and other stakeholders. Healthcare businesses with strong risk management practices are more likely to be regarded as responsible stewards of patient information, increasing their standing and encouraging client loyalty.

REFERENCES

Bandyopadhyay, T., Jacob, V., Raghunathan, S., 2010. Information security in networked supply chains: Impact of network vulnerability and supply chain integration on incentives to invest. Inf. Technol. Manag. 11, 7–23.

Bottle, A., Aylin, P., 2008. Intelligent information: A national system for monitoring clinical performance. Health Serv. Res. 43, 10–31.

Brandon-Jones, E., Squire, B., Autry, C.W., Petersen, K.J., 2014. A Contingent Resource-Based Perspective of Supply Chain Resilience and Robustness. J. Supply Chain Manag. 50, 55–73.

Chu, C.Y., Park, K., Kremer, G.E., 2020. A global supply chain risk management framework: An application of text-mining to identify region-specific supply chain risks. Adv. Eng. Informatics 45, 101053.

Fan, Y., Heilig, L., Voß, S., 2015. Supply chain risk management in the era of big data. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 9186, 283–294.

Federico Del Giorgio, S., 2022. IMPACTS OF CYBER SECURITY AND SUPPLY CHAIN RISK ON DIGITAL OPERATIONS: EVIDENCE FROM THE UAE PHARMACEUTICAL INDUSTRY Federico Del Giorgio Solfa. Int. J. Technol. Innov. Manag. (IJTIM), 2(2). 2, 18–32.

Min, H., 2019. Blockchain technology for enhancing supply chain resilience. Bus. Horiz. 62, 35–45.

Naeem, M.R., Lin, T., Naeem, H., Ullah, F., Saeed, S., 2019. Scalable mutation testing using predictive analysis of deep learning model. IEEE Access 7, 158264–158283.

Rachid, B., Roland, D., Sebastien, D., Ivana, R., 2017. Risk Management Approach for Lean, Agile, Resilient and Green Supply Chain. Int. J. Econ. Manag. Eng. 11, 802–810.

Saeed, S., 2023a. A customer-centric view of E-commerce security and privacy. Appl. Sci. 13, 1020.

Saeed, S., 2023b. Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. Sustainability 15, 6019.

Sindhuja, P.N., 2014. Impact of information security initiatives on supply chain performance an empirical investigation. Inf. Manag. Comput. Secur. 22, 450–473.

Von Solms, R., Van Niekerk, J., 2013. From information security to cyber security. Comput. Secur. 38, 97–102.