Journal of Theoretical and Applied Information Technology
15th March 2021. Vol.99. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PARTIAL LEAST SQUARES ANALYSIS: THE INTERACTION EFFECT AMONG CYBERSECURITY, CYBERCRIME AND ONLINE SHOPPING INTENTION

[1]JASSIM AHMAD AL-GASAWNEH, [2]GHADA AL-RAWASHDEH, [3]Ali ZAKARIYA Al-QURAN, [4]AHMAD MTAIR AL HAWAMLEH, [5]NAWRAS M. NUSAIRAT, [6]ABDUL HAFAZ NGAH

[1]Digital Marketing Department, Faculty of Management, Applied Science Private University, Amman 11931, Jordan;

[2]Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, Kuala Terengganu 21030, Malaysia;

[3]Faculty of economics and administrative sciences, Al al-Bayt University, Mafraq 25113, Jordan

[3]Distance Training Center, Institute of Public Administration, Riyadh 11141, Saudi Arabia;

[5]Marketing Department, Faculty of Management, Applied Science Private University, Amman 11931, Jordan;

[6]Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu, 21030, Kuala Nerus, Terengganu, Malaysia;

E-mail: J_algasawneh@asu.edu.jo[1], Ghada_rwashdeh@yahoo.com.[2], ali.z.al-quran@aabu.edu.jo, alhawamleha@ipa.edu.sa. [3], n_nserat@asu.edu.jo [4], hafaz.ngah@umt.edu.my[5]

ABSTRACT

This study examined the moderating role of cybersecurity in the relationship between cybercrime and online shopping intention among Jordanian customers. A total of 270 online users were the study sample. Online survey was used to gather data which were then analyzed using partial least squares structural equation modelling run using Smart PLS 3.2.9 software. This study found that the cybersecurity moderated the negative relationship between cybercrime and online shopping intention among Jordanian customers. This study contributes theoretically by filling the gaps in the literature, by proposing the combined use of Perceived Risk Theory and Protection Motivation Theory in using the moderating role of cybersecurity in the relationship between cybercrime and online shopping intention. In practice, this study facilitates E-marketers in improving their company's online markets by altering the perspectives and intention of customers towards online shopping, particularly through the improvement of cybersecurity policies to assure safe transactions.

Keywords: *Cybersecurity, Cybercrime, Online Shopping Intention, Jordan*

1. INTRODUCTION

The end of past millennium witnessed an expanding interest towards electronic Commerce at both individual and institutional levels. It appears that the current development of e-commerce has been significantly catalyzed by the intensifying expansion and development in information and communications technology. There are many areas impacted by such development, including government, banking, learning, healthcare, journalism, and shopping, giving birth to the concepts of electronic-government, electronic-banking, electronic -learning, electronic -healthcare, electronic-Journals and e-shopping. Among these, online shopping or e-shopping, which is the focus of this study, encompasses an element of electronic Commerce with global consumer acceptance. As described in [1], e-shopping is the electronic form of the conventional mail order business or telephone-based ordering system.

In 2020, [2] has reported the increase in global internet users from 2.92 in 2014 to 4.42 billion in 2020, prompting leading marketers to shift to internet in stimulating their activities associated with marketing. Retailing [3] additionally

remarked the dramatic expansion of internet technology function from for information access to online shopping. Further, [4] mentioned the transformation of internet from being a channel of social communication to that of marketing. Among marketers, there is acknowledgement of the potential enormous financial benefits of internet use, and according to [5], they are currently analyzing the needs among their target audience in online retailing industry to effectively improve their business and increase profits. [6] relevantly highlighted the need for marketers to make considerable efforts in order to achieve success in their online endeavors.

Jordan has good infrastructure for payments [7], and such infrastructure is in fact a key component in online shopping. Accordingly, Automated Clearing House for interbank transfers, Real-time gross settlement system, Electronic Cheques Clearing system, JoMo-Pay for mobile payments, Jo-Net for bank-to-ATM transactions, MEPS and EMPS, are among the online payment platforms available in Jordan. Still, the usage rate has been very low. Such low rate has been factored by the reluctance of customers towards online shopping caused by the lack of knowledge in internet shopping, lack of understanding of consumer behaviour in online shopping adoption, and risks associated with online shopping because of the perceived crime [8,9,10,11].

A number of issues and challenges have emerged following the significant expansion of online shopping and electronic commerce. Among the highlighted ones include online payment security, data protection, e-contract validity and enforceability, and inadequate rights enforcement [9,10,11,12]. Equally, the issue of cyber security has been brought up as it impacts online shopping intention. As mentioned in [13,14], secure online process and payment motivates customers or online users to perform online payment or purchasing. Pertinently, cybersecurity affects cybercrime [15,16,17]. This study aims to measure the moderating role of cybersecurity on the relationship between cybercrime and online shopping intention.

2. LITERATURE REVIEW

2.1 Online Shopping Intention

Associated with the Internet usage, online purchase has become the third most popular activity, after email and Web surfing [18], and online purchase has led to the development of electronic -commerce. Online purchase was illustrated in [19], whereby it begins with purchase intention. As indicated in [20,21], purchase intention is the readiness of customers in making purchase by way of the internet. According to [22], purchase intention refers to the willingness of consumers in buying specific product or service through the internet stores. Relevantly, online purchase intention refers to the intention of online shoppers in buying specific goods and services using the Internet or virtual shopping carts [19]. This concept can also be illustrated as the willingness of customers towards the use of the internet services in the execution of real purchase of goods and services or in comparing product prices [23].

The purchase intention of consumer can predict consumer behavior. However, considering the many factors impacting purchase intention, it is not easy to quantify consumer behavior. In their study, [24] highlighted that online purchase intention can be increased through the use of privacy and security statements. Equally, companies need to influence purchase intentions of consumers, and gain their trust by showing competency in satisfying their needs and wants. Somehow, among researchers, purchase intention has been used in predicting real purchase activities of consumers.

Online shopping intention has been determined and measured in this study, based on the following constructs as in [11,25], probability of online product purchase, probability of recommending online shopping to others, and probability of making another online purchase if the purchased products are found advantageous.

2.2 Cybercrime

Cybercrimes refer to crimes committed through the Internet [26,27]. In view of that, crimes have changed their nature because of the information capabilities of the Internet. In fact, according to [28], the Internet allows easy, cost-effective and repeatable means of performing fast attacks on a global scale, while the culprits (cybercriminals) could remain anonymous and/or out-of-the-way of law enforcement. Relevantly, consumer-oriented cybercrimes have the most significant impact on online service adoption. These refer to cybercriminal attacks with potential harm to Internet users. As such, certain cybercrimes are not included in this study, for instance, industrial espionage.

In essence, cybercrimes are those linked to the use of the Internet as can be exemplified by identity theft/crimes, electronic fund transfer, deceitful

sales online, advance fee schemes and fake investment [28]. In Ghana, [29] identified three major cyber-crime activities as follows: fabricated identification, counterfeit gold dealings and credit card fraud. These are called sakawa‖.

Cyber-crime activities have made Internet related business risky. Hence, there must be measures for safeguarding the security of both customers and businesses in Internet business transactions. In many less developed countries, there have been considerable efforts towards the adoption of e-commerce technologies and transactions. Nonetheless, [29] reported the consistent attempts among dishonorable computer users in taking advantage of the weaknesses of the Internet medium and computer networks and committing crimes against users. As reported in several studies (e.g.,[30,31]), those that perform cyber-crimes detect vulnerabilities in e-commerce technologies, and using countless of methods, these criminals exploit these vulnerabilities and take advantage of victims.

2.3 Cybersecurity

Security issue has been a significant concern to electronic -commerce customers and this issue has been addressed in various studies on online purchasing [20]. As highlighted in [32], security, which is a technical challenge, involves the aspects of human and organization. In other words, irrespective of the technical approach and solutions used, even the best ones, human aspects such as perception on e-commerce must be taken into account as well. Hence, reliance on just organizational capabilities is not enough. In 2013, [20] accordingly stressed the importance of taking into account human attitude and perceptions towards technology adoption, as they appear to be important factors. In this regard, perception encompasses knowledge of the world that is formed from the information received by one's senses [33], while security perception refers to a level to which an individual is confident towards the security of the online vendor or website [20].

Online security was viewed in [34] as a hazard which generates a situation or event that can potentially lead to economic adversity to data or network resources by destructing, disclosing and altering the data, denying service, and/or by causing fraud, abuse and waste. In [35], the notion of online security was reported as a major concern among consumers, and [35,36] reported security of payment methods and privacy of financial information or technology devices from illegal access or spam as among the factors considered by consumers in regards to online transaction security.

According to [37], security in the application of online shopping is also affected by how trusted parties form dependable and comfortable situations for consumers in handling the system. This refers to the safeguarding of the online or website system termed as cybersecurity, and as highlighted in [35,38], it affects the decision of customers in adopting any services of e-commerce. In this study, cybersecurity was used in comfortability measurement, because of the security, and the customer satisfaction of the website and online services security and the sufficiency of security to make the transactions via online and websites.

2.4 Underpinning Theories

2.4.1 Perceived Risk Theory:

Perceived risk is associated with the search and choice of information relating to products or services prior to the decision of purchase [39]. According to [40], for online customers, the actual purchasing experiences that do not correspond to their purchasing goals will cause them to perceive higher risk. According to [41], perceived risk is affected by the subjective uncertainty of the outcomes. In 2004, [42] indicated that for each purchasing decision of consumers, there will be a number of buying goals or anticipated outcomes. In view of that, past studies have employed various types of perceived risk such as financial risk, performance risk, physical risk, psychological risk, social risk, and convenience risk, as described as follows:

Financial risk refers to the probable monetary loss that consumers may face following a purchase of a given product or service, while performance risk relates to the probability that a product will present the expected performance. Physical risk refers to issues of safety from the use of the product and this usually relates to the consumer's health and security, whereas psychological risk encompasses the likelihood of a given product to be in agreement with the self-image of the consumer. Social risk relates to the viewpoints of significant others towards a given product or service. Meanwhile, convenience risk refers to the inconveniences that consumer will face after purchasing a product or service [43].

2.4.2 Protection Motivation Theory:

Protection motivation theory by [44], illustrates the factors that contribute to the intent to perform desirable information security behaviours.

Accordingly, Protection Motivation Theory has been explored in various studies, as in [45,46,47] who tested the effects of factors of Protection Motivation Theory on the intention to abide by the security policy. Further, [47] concluded the good explanatory power of Protection Motivation Theory in their study as it described 44% of the behavioural intention. The authors specifically indicated that five out of six factors of protection motivation theory showed impacts that are significant statistically. Meanwhile, in [45], Protection Motivation Theory factors were combined with General Deterrence Theory and Theory of Planned Behaviour and the effects were tested. The results showed good ability of Protection Motivation Theory factors in explaining the "attitude" construct, specifically, it explained 47% of the behavioural intention's total variance.

PMT has also been used in studies in information security especially in examining the intention in anti-virus software adoption (e.g., [48,49]. For instance, [49] reported the ability of Protection Motivation Theory factors in elucidating 45% of the intention to install anti-virus software. As for [48], their proposed model made up 27% of the intention. Indeed, Protection Motivation Theory has generally demonstrated steady and reasonable explanatory power towards intention to perform the sought-after information security behaviours whereby its initial model had been tested in full, partially, or with other theories combined. However, for tests of non-work context and proactive behaviours, the use of Protection Motivation Theory has been inadequate.

Accordingly, a conceptual is proposed in this study. The model includes Perceived Risk Theory and Protection Motivation Theory in understanding the motivation of online shopping through the implementation of security policies and prevention of online risks (e.g., crime or financial risk).

2.5 Relationship between variable

Perceptions of cyber-crime are significant predictors of intention to purchase using e-commerce technologies, whereby cyber-crime affects intention to purchase negatively [50]. In a study by [51], a parsimonious model was proposed. Based on past works on technology acceptance and insights from criminology, the model was used in identifying the factors that decrease the intention of Internet users to use online services. In Indonesia, [52] found a negative impact of customers' cyber-crime perceptions on their purchase intentions through e-commerce. Contrariwise, [30] reported no impact of cybercrime on intention to use online services. Considering these findings, the hypothesis below is presented:

H1: Cybercrime has a negative impact on online Shopping Intention.

2.6 Cyber Security as moderator

Moderating variables have been used in various studies (e.g., [53]) when dealing with a weak or unpredictable relation between an antecedent (independent variable) and an outcome. In view of that, many past studies related to the present study presented weak and inconsistent outcome between cybercrime and intention to purchase online. For instance, a negative effect between cybercrime and intention to engage in online shopping and services was documented in [50,51,52], while [30] found negative impact between both constructs. As such, some studies (e.g., [53]) proposed including a moderator variable to this relationship.

Cybersecurity affects cybercrime [15] and online purchasing intention [13,14]. Relevantly in [54], it was indicated that the application of contextual factor from other fields with a constructive theoretical explanation (e.g. using generations from sociology in a marketing study) gives a solid foundation for the integration of the aforementioned factor into the study as a moderator. This greatly contributes to the extant knowledge. As such, the present study has chosen to use cybersecurity as a technology field factor in marketing study as a moderator. Considering these findings, the hypothesis below is presented:

H2: Cybersecurity moderates the relationship between cybercrime and online shopping intention.

3. METHOD

3.1 Sample and Procedure

Relevant conditions and phenomena are defined in this descriptive study. Further, a decision-making process is carried out, leading to the construction of hypotheses to be tested. In this study, the data were gathered through the use of questionnaires that were distributed to customers through WhatsApp and email. The data obtained

were related to online shopping. All respondents selected in this study were over 18 years old. Respondents of such age are usually able to make purchasing decisions as they have knowledge in product purchase. Also, in Jordan, individuals of 18 years old and above are allowed to open a bank account.

A convenience sampling technique was used in this study in selecting the samples. The determined sample size corresponds to the analysis power, and the minimum sample size of this study was determined in accordance with the complexity of the model. This study should employ 68 samples as proposed in [55]. Further, the research framework comprised two predictors with medium effect as proposed in [56]. Also, accurateness is important and [57] proposed using a sample size larger than 100. Based on this suggestion, a total of 350 questionnaires were distributed to the respondents.

3.2 Measures

The questionnaire used in this study comprises four sections with the following details: the first section covers the respondents' personal and demographic information (i.e., age, gender, status and education level), the second section comprises five items on cybercrime from [30], the third section presents ten items about cybersecurity based on the work of [33], and the fourth section presents three items related to online shopping intention based on the work of [11,25]. Items in sections two, three and four are furnished with 5-point Likert scale each.

This study used the back-translation method proposed by [58] on the questionnaire. Specifically, the questionnaire which was originally in English, was translated to Arabic, and then, the Arabic version of the questionnaire was translated back to English. This was to assure quality and accurateness of the questionnaire. The instrument was checked for validity and clarity to assure its ability in measuring the objective of the study through sent the survey to academics' professors as well explanatory factor analysis (EFA) to identify how many factors of cybercrime, cybersecurity, online shopping intention were appropriate in representing the data. Accordingly, Table 1 displays the items and construct resulting from EFA test.

Table 1. Explanatory factor analysis

No.	Construct	Dropped items	Achieved
1.	Cybercrime	-	5
2.	Cybersecurity	5	5
3.	Online shopping intention	-	3
Total		5	13

As in table 1 there were three constructs initially pretested using explanatory factor analysis. These constructs were: Cybercrime (five items), Cybersecurity (ten items), and online shopping intention (three items). EFA test was carried out and the results are as follows: all items of cybercrime and online shopping constructs scored higher than the cut-off value of 0.6 and therefore all items for both constructs were retained, while 5 items of cybersecurity construct scored lower than the cut-off value of 0.6 and were thus deleted, resulting in 5 items for cybersecurity. As such, 13 items were used in this study representing three constructs with the following breakdowns: 5 items represented cybercrime, 5 items represented cybersecurity, and 3 items represented online shopping. Further, the internal consistency of each construct which was represented by Cronbach's alpha was greater than 0.70 as follows: Cybercrime = 0.75,

Cybersecurity = 0.87, Online shopping intention = 0.77.

3.3 Data Estimation

The descriptive analysis was carried out in this study through the use of SPSS version 26. In testing the research model, Partial Least Squares Structural Equation Modeling (PLS-SEM) technique was applied. The use of PLS-SEM in this study was factored by the ability to estimate of the endogenous variables [59] and the use of highly complex research model (demonstrated by the hypotheses) [60]. Accordingly, this study used Smart-PLS version 3.2.9 as in [61].

4. RESULT

4.1 Sample Descriptive

This study gained a response rate of 82%, which amounted to 290 returned questionnaires. From the 290 returned questionnaires, 20 had to be excluded due to incompletion. Hence, the final number of usable questionnaires was 270, which was sufficient for analysis. From the returned questionnaires, 210 (77%) were from female respondents, and the remaining 60 (23%) were from male respondents. Therefore, the responses were female dominated. Age wise, all were over the age of 18 with the following details: 15% were 19– 20 years old, 40% were 21–31 years old, 15% were 31– 40 years old, 20% were 41– 50 years old and 10% were 51 years or older. In terms of marital status, the majority (60%) were married while the remaining 40% were single. For their education level, the details are as follows: 33% had a diploma, 27% had a Bachelor's degree, 16% had a PhD, 14% had a Master's degree, and 10% had a high school certificate.

4.2 Data Screening Process

Data screening assures the non-presence of outliers or missing values in the data, while also assuring normal data distribution. This study found no missing data. Further, this study found no variable exceeding -4, +4; specifically, all variables fell in the range between 2.210 and 2.112. As such, for all 270 cases, there was no univariate outlier. In terms of normality, this study found that the skewness and kurtosis values for all variables were between ± 2 and ±7. As proposed in [62], for normal distribution, skewness value should range from -0.421 to 0.320 while kurtosis value should range from -1.012 to - 0.481. This study thus concluded that the obtained data were well modelled and were normally distributed.

4.3 Moderating Analysis Approach

Data analysis was carried out using partial least squares method, specifically through two-stage method for moderator analysis. The available reflective constructs and indicators were applied in this study, and elimination was made to the issues associated with the product indicator approach's weak statistical power. As mentioned, a two-stage method of partial least squares was used in this study, and the details are as follows: the convergent validity and discriminant validity (except for the interaction term, as can be observed in Figure 1) were determined during the first stage, and the requirements of the structural model were addressed during the second stage as can be referred in Figure 3. Also, this study calculated the product indicator linked to the second-stage analysis as demonstrated in [57,63]. Such calculation formed the interaction term as well as the predictor and moderator variables.

4.4 Assessment of measurements model:

In this study, convergent validity was determined through the computation of factor loadings, Cronbach Alpha (CA), rho_A, Composite Reliability (CR), and Average Variance Extracted (AVE) as proposed in Hair et al. (2017). In this study, the loadings of all items surpassed the proposed value of 0.5 (see Table 2 - Figure 1). Also, CA, rho_A, and CR values of all constructs exceeded 0.7, while the obtained values of AVE were greater than 0.5 as recommended in [57]. Convergent validity was therefore affirmed.

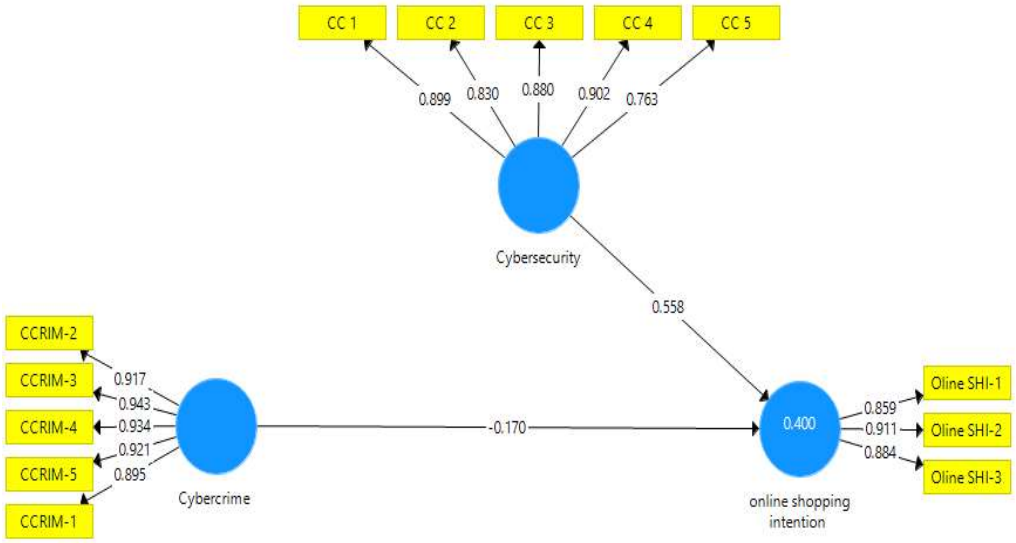

Figure 1. The Measurement Model

Table 2. Measurement Model

First order Construct	Items	Factor loading	CR	AVE
Cybercrime	CCRIM 1	0.917	0.966	0.850
	CCRIM 2	0.943		
	CCRIM 3	0.934		
	CCRIM 4	0.921		
	CCRIM 5	0.895		
Cybersecurity	CC 1	0.899	0.932	0.733
	CC 2	0.830		
	CC 3	0.880		
	CC 4	0.902		
	CC 5	0.763		
Online shopping intention	Oline SHI-1	0.859		
	Oline SHI-2	0. 911	0.916	0.783
	Oline SHI-3	0.884		

The discriminant validity was tested in this study with the use of Heterotrait-Monotrait (HTMT) criterion, and the obtained HTMT values in this study were smaller than 0.85, which, according to [64], demonstrate discriminant validity. The details are provided in Table 3.

Table 3. Discriminant validity (HTMT)

	Cybercrime	Cybersecurity	Online shopping intention
Cybercrime			
Cybersecurity	0.315		
Online shopping intention	0.355	0.675	

As displayed in Table 2 and Table 3; the results of analysis of the constructs, their convergent validity and discriminant validity for the measurement model show that the measurement scale used in this study is both accurate and fitting.

4.5 Assessment of structural model:

Path analysis was carried out in this study after the measurement model validation. The purpose of path analysis is to test the proposed hypotheses. Accordingly, inner VIF values, results of path-coefficient, coefficient of determination (R^2), effect sizes (f^2), and predictive relevance Q^2 were reported, as recommended in [57]. As can be viewed in Table 4, online shopping intention scored R^2 of 0.400 implying 40% degree of variation in online shopping intention, which follows Chin's (1998) proposed cut-off point of 0.19. As such, it can be stated that online shopping intention is clarified by cybercrime. Next, the Q^2 value related to online shopping intention was 0.261, and this value is considerably larger than 0, which affirms the relevance of the predictive model as proposed by [65]. As such, the model is regarded as acceptable. Also, the predictive relevance of model is high. In terms of VIF values, they are lower than 5 at respectively 1.314 and 1.310, following the recommendation of [57].

Following [66], this study applied the bootstrapping method with a resampling of 5000 in the estimation of the significance of the path coefficient. From the details displayed in Table 4 and Figure 2, Cybercrime affects Online shopping intention negatively (β = - 0.240, t = 2.142, p =0.004 < 0.05, f 2 = 0.076), lending support to H1. Further, the result of H2 demonstrates the moderating effect of cybersecurity on the relationship between Cybercrime and Online shopping intention whereby β = 0.475 and p = 0.002 < 0.05. In view of that, Figure 3 shows that the lines are not parallel.

The positive link between Cybercrime and Online shopping intention being solidified by cybersecurity has been proposed, in addition to the change in R^2 before the interaction effect of 0.400 is included (see Figure 1), and the intensity of the link was proposed to increase when interaction occurs at 0.437. This study found moderation of the relationship between Cybercrime and Online shopping intention. Hence, H2 is supported.

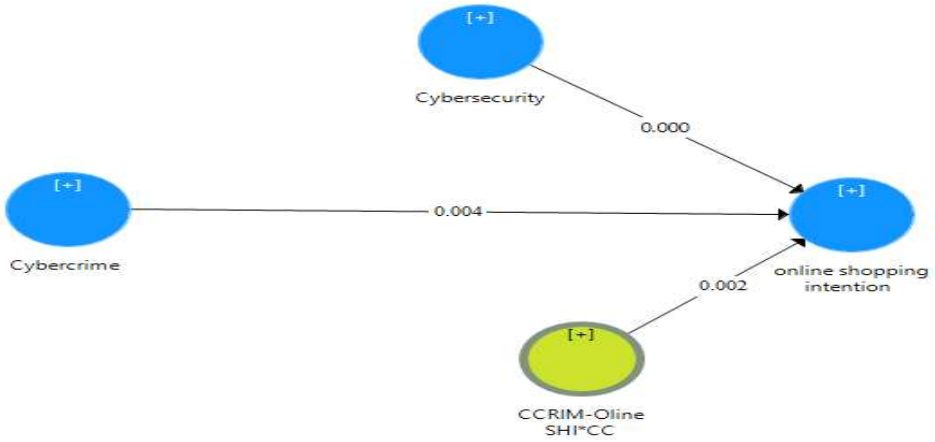

Figure 2. Structural model.

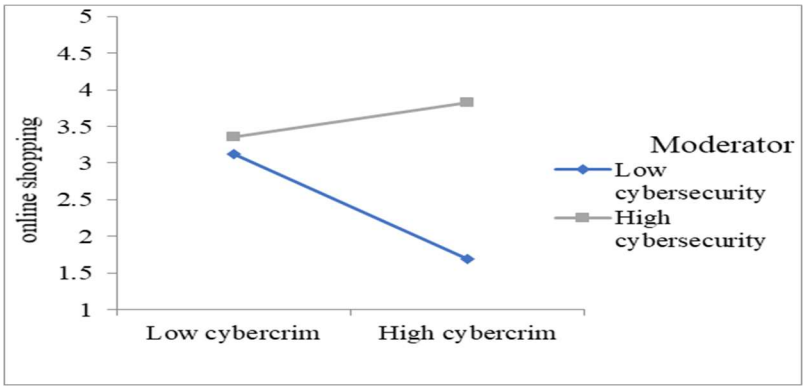

Figure 3. Moderation Effect of cybersecurity on the Relationship between cybercrime and online shopping intention

Table 3. Structural model

	S. B	S. D	R^2	Q^2	VIF	F^2	T-value	P Values
Cybercrime > Online shopping intention	- 0.240	0.112	0.437	0.261	1.314	0.076	2.142	0.004
Cybercrime - Online shopping intention *cybersecurity	0.475	0.161			1.310	0.041	2.950	0.002

5. DISCUSSION:

Cybercrimes can potentially impede the future growth potential of online sales. Hence, for online business companies, it is important to understand such threat and increase e-security budgets to assure protection to consumers. Meanwhile, among consumers, there has been a dramatic increase in their knowledge on the Internet and its usage risks, and consumers have also demonstrated dramatically higher

expectations of service. It is thus crucial for these companies to establish trust among consumers through lawful declaration of e-security measures, privacy and policies on information-use. Notably, breach in e-security can cause significant financial disaster which could harm the company's reputation.

Accordingly, the model proposed in this study presents cybercrime as a predictor variable, online shopping intention as endogenous variable, and cybersecurity as a moderator variable. From the hypotheses testing, for H1, cybercrime was found to negatively affect online shopping intention. Similar finding was reported in [50] whereby the authors reported that cybercrime is a serious problem in society, is damaging to e-commerce transaction, a danger those involved in E-commerce, and causes losses of valuables (money etc.), impacting online purchasing intention. For H2, this study concluded a moderating impact of cybersecurity on the relationship between cybercrime and online shopping intention. Specifically, transaction security via secure password and username, websites security policies and secure process of online transactions, all moderate the negative intention of customer toward the online shopping.

6. CONCLUSION

6.1 Theoretical contributions

The present study provides evidence that support the theoretical foundation concerning the impact imparted by cybercrime on the intention of online shopping. Further, the knowledge of Jordanian e-commerce particularly on the impact of cybercrime on online shopping intention is enriched in this study. Additionally, this descriptive study is the first that explored the moderating role of cybersecurity between cybercrime and online shopping intention. Further, this study integrated Perceived Risk Theory and Protection Motivation Theory in motivating online shopping, specifically by the use of security policies and the prevention of online risks (e.g., crime or financial risk). Lastly, this study applied PLS-SEM methods that involve a two-stage approach to analyse and construe the (reflective) moderating role of cybersecurity in the relationship between cybercrime and online shopping intention.

6.2 Practical Implications

This study deliberates Jordanian online markets from the aspects of cybercrime and cybersecurity. For e-marketers, the outcomes of this study can be perused in the improvement of their online markets, especially by changing the outlooks and intent of customers towards online shopping through the improvement of policies associated with cybersecurity, in order to assure safe transactions.

7. Limitations and future works

The unit of analysis posed a limitation to this study as this study was focusing on just the customers. Hence, similar study should be carried out, but from the viewpoint of company. This will enrich the understanding of the moderating role of cybersecurity in the relationship between cybercrime and intention of online shopping. The use of quantitative approach in this study in meeting its objectives became a limitation as well. As such, similar study should be carried out, but with the use of longitudinal approach through other methods such as qualitative technique. This will allow the understanding of the possible changes in online shopping intention following the occurrence of cybercrime, with the presence of cybersecurity as moderator. Additionally, the direct relationship between cybercrime and online shopping intention was explored in this study. For this reason, it is suggested that the relationship between cybercrime and actual online shopping is addressed in future studies. Furthermore, as this study was focusing on the moderating role of cybersecurity in the relationship between cybercrime and online shopping intention, other factors that can potentially affect the link between cybercrime and online shopping intention (e.g., reference group) should be examined in future studies.

REFERENCES:

[1] ALrawimi AA. Influence of Online Security, Protection, Website Credibility and Previous After Sales Experience on the Intention to Purchase Online. European Journal of Business and Innovation Research. 2015;3(2):1-0.

[2] Internet world Stats. (2020). Internet user's distribution in the world. 2020. Retrieved from https://www.internetworldstats.com/stats.html.

[3] Today R. Study: 81% research online before making big purchases. accessed June. 2013;20:2015.

[4] Nagar K. Assessing the Impact of Online Retailer Models on Consumer's Attitude and Purchase Intentions. IIM Kozhikode Society & Management Review. 2018 Jan;7(1):1-2.

[5] Kwon KJ, Mai LW, Peng N. Determinants of consumers' intentions to share knowledge and intentions to purchase on s-commerce sites: incorporating attitudes toward persuasion attempts into a social exchange model. Eurasian Business Review. 2020 Mar;10(1):157-83.

[6] Alharthey B. The Role of Online Trust in Forming Online Shopping Intentions. International Journal of Online Marketing (IJOM). 2020 Jan 1;10(1):32-57.

[7] U.S. Agency for international development. Digital finance country report Jordan. 2019. http://tanmeyahjo.com/Portals/0/Digital%20Finance%20COUNTRY%20REPORT%20(USAID%20LENS).pdf?ver=2019-04-02-133749-100.

[8] Al-dweeri RM, Obeidat ZM, Al-dwiry MA, Alshurideh MT, Alhorani AM. The impact of e-service quality and e-loyalty on online shopping: moderating effect of e-satisfaction and e-trust. International Journal of Marketing Studies. 2017;9(2):92-103.

[9] Alhawamleh AM, Ngah A. Knowledge sharing among jordanian academicians: A case study of tafila technical university (TTU) and mutah university (MU). In2017 8th International Conference on Information Technology (ICIT) 2017 May 17 (pp. 262-270). IEEE.

[10] Hawamleh AM, Ngah A. An Adoption Model of Mobile Knowledge Sharing Based on the Theory of Planned Behavior. Journal of Telecommunication, Electronic and Computer Engineering (JTEC). 2017 Oct 20;9(3-5):37-43.

[11] Al-Gasawneh JA, Omar K. (2020). Moderating role of content marketing on the relationship between perceived risk and the intention to online shopping. Journal of Theoretical and Applied Information Technology. 2020:98(04):587-595.

[12] Paynter J, Lim J. Drivers and impediments to e-commerce in Malaysia. Malaysian Journal of Library & Information Science. 2001 Dec 1;6(2):1-9.

[13] Pookulangara S. Does Gender Matter: An Exploratory Study of Influence of Cybersecurity, Privacy, and Trust on Purchase Intention. InInternational Textile and Apparel Association Annual Conference Proceedings 2015 Nov 11 (Vol. 72, No. 1). Iowa State University Digital Press.

[14] Meskaran F, Shanmugamm B, Ismail Z. Factors affecting on security perception in online purchase intention. Advanced Science Letters. 2014 Oct 1;20(10-11):2004-8.

[15] Schjolberg S, Ghernaouti-Helie S. A global treaty on cybersecurity and cybercrime. Cybercrime Law. 2011;97.

[16] Alhawamleh AM. Web Based English Placement Test System (ELPTS) (Doctoral dissertation, Universiti Utara Malaysia).2012.

[17] Kshetri N. Cybercrime and cybersecurity in the global south. Springer; 2013: 80(3): 541-555.

[18] Jamali HR, Russell B, Nicholas D, Watkinson A. Do online communities support research collaboration?. Aslib Journal of Information Management. 2014 Nov 11.

[19] Close AG, Kukar-Kinney M. Beyond buying: Motivations behind consumers' online shopping cart use. Journal of Business Research. 2010 Sep 1;63(9-10):986-92.

[20] Meskaran F, Ismail Z, Shanmugam B. Online purchase intention: Effects of trust and security perception. Australian journal of basic and applied sciences. 2013;7(6):307-15.

[21] Wei N, Baharudin A, Hussein LA, Hilmi M. Factors Affecting User's Intention to Adopt Smart Home in Malaysia. (2019): 39-54.

[22] Chu KK, Li CH. A study of the effect of risk-reduction strategies on purchase intentions in online shopping. IJEBM. 2008;6(4):213-26.

[23] Iqbal S, Hunjra AI, Rehman KU. Consumer intention to shop online: B2C E-commerce in developing countries. Middle East Journal of Scientific Research. 2012;12(4):424-32.

[24] Schlosser AE, White TB, Lloyd SM. Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. Journal of marketing. 2006 Apr;70(2):133-48.

[25] Ariffin SK, Mohan T, Goh YN. Influence of consumers' perceived risk on consumers' online purchase intention. Journal of Research in Interactive Marketing. 2018 Aug 13.

[26] European Commission. Special Eurobarometer 390 Cyber security. 2012. URL http://ec.europa.eu/public_opinion/archives .

[27] Kraemer-Mbula E, Tang P, Rush H. The cybercrime ecosystem: Online innovation in the shadows?. Technological Forecasting and Social Change. 2013 Mar 1;80(3):541-55.

[28] Clough J. Cybercrime Principles. 2010.

[29] Warner J. Understanding cyber-crime in Ghana: A view from below. International journal of cyber criminology. 2011;5(1):736.

[30] Apau R, Nti F, Adu S. Cyber-Crime and its Effects on E-Commerce Technologies. Journal of Information. 2019 Mar;5(1):39-59.

[31] Patel P, Patel R, Patel V, Pathrabe T. Survey of Privacy and security issues in spice world e-commerce website. International Journal for Innovative Research in Science & Technology. 2017:19-23.

[32] Damghanian H, Zarei A, Siahsarani Kojuri MA. Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran. Journal of Internet Commerce. 2016 Jul 2;15(3):214-38.

[33] Netshirando V. The Effect of Cyber Security on Citizens Adoption of e-Commerce Services: The Case of Vhembe District in Limpopo Province of South Africa (Doctoral dissertation).

[34] Roca JC, García JJ, De La Vega JJ. The importance of perceived trust, security and privacy in online trading systems. Information Management & Computer Security. 2009 Jun 5.

[35] Román S, Cuestas PJ. The perceptions of consumers regarding online retailers' ethics and their relationship with consumers' general internet expertise and word of mouth: a preliminary analysis. Journal of Business Ethics. 2008 Dec 1;83(4):641-56.

[36] Rawashdeh G, Bin Mamat R, Bakar ZB, Rahim NH. Comparative between optimization feature selection by using classifiers algorithms on spam email. International Journal of Electrical & Computer Engineering (2088-8708). 2019 Dec 15;9.

[37] Salo J, Karjaluoto H. A conceptual model of trust in the online environment. Online information review. 2007 Oct 2.

[38] Morris D, Madzudzo G, Garcia-Perez A. Cybersecurity threats in the auto industry: Tensions in the knowledge environment. Technological Forecasting and Social Change. 2020 Aug 1;157:120102.

[39] Dowling GR. Perceived risk: the concept and its measurement. Psychology & Marketing. 1986 Sep;3(3):193-210.

[40] Pires G, Stanton J, Eckford A. Influences on the perceived risk of purchasing online. Journal of Consumer Behaviour: An International Research Review. 2004 Dec;4(2):118-31.

[41] Cox DF, Rich SU. Perceived risk and consumer decision-making—the case of telephone shopping. Journal of marketing research. 1964 Nov;1(4):32-9.

[42] Huang WY, Schrank H, Dubinsky AJ. Effect of brand name on consumers' risk perceptions of online shopping. Journal of Consumer Behaviour: An International Research Review. 2004 Sep;4(1):40-50.

[43] Li YH, Huang JW. Applying theory of perceived risk and technology acceptance model in the online shopping channel. World Academy of Science, Engineering and Technology. 2009 May 22;53(1):919-925.

[44] Rogers RW. A protection motivation theory of fear appeals and attitude change1. The journal of psychology. 1975 Sep 1;91(1):93-114.

[45] Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 2009 Apr 1;18(2):106-25.

[46] Dang-Pham D, Pittayachawan S. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. Computers & Security. 2015 Feb 1;48:281-97.

[47] Vance A, Siponen M, Pahnila S. Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management. 2012 May 1;49(3-4):190-8.

[48] Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS quarterly. 2010 Sep 1:549-66.

[49] Lee D, Larose R, Rifon N. Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology. 2008 Sep 1;27(5):445-54.

[50] Apau R, Koranteng FN. Impact of Cybercrime and Trust on the Use of E-Commerce Technologies: An Application of the Theory of Planned Behavior. International Journal of Cyber Criminology. 2019 Jul 1;13(2):228-54.

[51] Riek M, Bohme R, Moore T. Measuring the influence of perceived cybercrime risk on online service avoidance. IEEE Transactions on Dependable and Secure Computing. 2015 Mar 9;13(2):261-73.

[52] Rofiq A. Impact of cyber fraud and trust of e-commerce system on purchasing intentions: Analysing planned behaviour in Indonesian business (Doctoral dissertation, University of Southern Queensland).

[53] Baron RM, Kenny DA. The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. Journal of personality and social psychology. 1986 Dec;51(6):1173.

[54] Memon MA, Ting H, Cheah JH, Thurasamy R, Chuah F, Cham TH. Journal of Applied Structural Equation Modeling. 2019: 3(1).

[55] Green SB. How many subjects does it take to do a regression analysis. Multivariate behavioral research. 1991 Jul 1;26(3):499-510.

[56] Gefen A. How do microclimate factors affect the risk for superficial pressure ulcers: a mathematical modeling study. Journal of tissue viability. 2011 Aug 1;20(3):81-8.

[57] Hair Jr JF, Sarstedt M, Ringle CM, Gudergan SP. Advanced issues in partial least squares structural equation modeling. saGe publications; 2017 Apr 5.

[58] Brislin RW. Back-translation for cross-cultural research. Journal of cross-cultural psychology. 1970 Sep;1(3):185-216.

[59] Jöreskog KG, Wold HO. Systems under indirect observation: Causality, structure, prediction. North Holland; 1982.

[60] Hair JF, Risher JJ, Sarstedt M, Ringle CM. When to use and how to report the results of PLS-SEM. European Business Review. 2019 Jan 14.

[61] Sarstedt M, Cheah JH. Partial least squares structural equation modeling using SmartPLS: a software review. Journal of Marketing Analytics. 2019 Sep 1;7(3):196-202.

[62] Ghasemi A, Zahediasl S. Normality tests for statistical analysis: a guide for non-statisticians. International journal of endocrinology and metabolism. 2012;10(2):486.

[63] Al-Gasawneh JA, Al-Adamat AM. The Relationship between Perceived Destination Image, Social Media Interaction and Travel Intentions Relating to Neom City. Academy of Strategic Management Journal. 2020;19(2).

[64] Henseler J, Ringle CM, Sarstedt M. A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the academy of marketing science. 2015 Jan 1;43(1):115-35.

[65] Chin WW. Commentary: Issues and opinion on structural equation modeling.1998.

[66] Streukens S, Leroi-Werelds S. Bootstrapping and PLS-SEM: A step-by-step guide to get more out of your bootstrap results. European Management Journal. 2016 Dec 1;34(6):618-32.