Online Game Addiction in Cybersecurity Perspective: A Systematic Literature Review

Wan Mohd Yusoff Wan Yaacob
Department of Information Technology & Communication, Polytechnic of Sultan Abdul Halim Mu'adzam Shah, Kedah, MALAYSIA.
yusoff@polimas.edu.my

Nur Haryani Zakaria
School of Computing, College of Art & Sciences, Universiti Utara Malaysia, Sintok, Kedah, MALAYSIA.
haryani@uum.edu.my

Zahurin Mat Aji @ Alon
School of Computing, College of Art & Sciences, Universiti Utara Malaysia, Sintok, Kedah, MALAYSIA.
zahurin@uum.edu.my

***Abstract*— Online Game Addiction (OGA) signifies an issue partnership with technology defined as compulsive, obsessed, impulsive and hasty. Recent research identified cases where digital usage shows symptoms of behavioral addiction especially among the adolescent. Not only that, studies have found that this online game addictive behavior also contributed to network threats such as phishing, social engineering and spamming. Most of the threats mentioned rooted from cybersecurity issues that came from security vulnerability and social interaction risk. This happens when users tend to act in an unethical way if they are not allowed to proceed playing or being stopped from playing due to any constraints or hurdles. In this paper, we conduct a systematic literature review to gather the previous research related to OGA in cybersecurity perspective. The goal of this research is to identify the current research stage and open challenges for future studies in OGA. The research extracted 25 papers from diverse scientific databases. The result demonstrates that the issue of OGA that relates to cybersecurity perspective has been addressed very limitedly and the related research gap were found and well-presented and discussed in this study.**

Keywords—Addictive Behavior, Online Game Addiction, Cybersecurity, Systematic Literature Review

I. INTRODUCTION

Addictive behavior traditionally can be characterized as any activities that features the main components of addiction such as; *Salience, Tolerance, Mood Modification, Conflict, Relapse* and *Withdrawal* [1]. In psychology, undermining common sense is characterised as bravery which motivated by social values and in medicine as impulsivity-led dependence [2]. There are three levels of addiction according to Ng and Wiemer [3] which relate to beginner, intermediate and advance level that reflects the particular degree of self-control and distinct behavioral attitudes. Griffith [4] also mentioned that the subject of addiction will influence the decision making and the individual can be directed by the level of change contributing to the component addiction model within the biopsychosocial framework including Internet Addiction (IA). IA also refers to the Internet usage epidemic which marked by compulsive, impulsive, repetitive and hasty properties. It also has a correlation with unhealthy behaviours such as fatigue, worry, sleep loss, distraction and a decline in social skills [5]. Furthermore, IA also stresses the uncontrollable degree of involvement with other interactions of software products [6]. These content can compensate and provide pleasure for the person who have paucity of social skills but it could socially and psychologically damage a person [7]. Young and de Abreu [8] reported that IA has been categorized into various subtypes including Online Game Addiction (OGA). Meanwhile, in particular with respect to OGA, these issues were specifically established by Hadlington 's main guide in his research on human factors in the field of cybersecurity [9]. In contrast with study conducted by Durak [10] which focus on academic performance among students, Hadlington precisely aim to examine the connection between Internet addiction with impulsivity and risky behaviors among workers and employees. On top of that, both of them are focusing on different perspectives and platform. The existing literatures on OGA mostly are found to be skewed towards its impact in line with medical and psychological needs. Research findings from Hadlington [11] and Durak [10] have noted some relationship according to human factors and cybersecurity perspective and they also found humongous practical-knowledge gap in theoretical framework that relates to cybersecurity behavior that should have given more attention. From the literatures, the findings also mentioned that online game also prone to security threats like phishing and social engineering in order to gain security data and personal information among the attackers and anonymous [12].There were also several researchers that contribute to security behavior improvement like Leach [13] and Whitty et al.[14], but the findings are related to influence and effect of security behavior and risky practice of authentication in different perspective. Li [15] and Nobles [16] also investigated the impact of cybersecurity awareness and human factors among employees and business organizations. Similar result also reported by Samantha et al.[17] and Arunesh et al. [18] which focus on security game and cyber-attacks in the different view. Despite the importance of the literatures, Hadlington [11] and Durak [10] were identified as a prolific reference due to limited publications regarding to online game addiction in cybersecurity perspective. It has now becoming crucial that this addictive behavior has high possibility of affecting the cybersecurity awareness embodiment in an individual. This happens when users tend to act in an unethical way if they are not allowed to proceed playing or being stopped from playing due to any constraints or hurdles [19]. More alarming, Hadlington[20] has highlighted that the intention becomes the most influenced factors that can affect ones behavior along with attitude towards cybersecurity especially in the context of online game addiction. This study argues that people who are addicted to online gaming will hypothetically respond to the point that they might jeopardise their personal information, placing cybersecurity risk at stake which beyond the limits impacted by addiction.

II. METHOD

In this article, a Systematic Literature Review (SLR) was conducted to identify the research topics that are important to OGA and the related issues which well discussed by prominent scholars especially from the cybersecurity perspective that need to be addressed in future studies. SLR was chosen as the technique to explore related articles in scientific databases and to schedule a table of existing research scope to achieve this aim. This SLR is carried out in this study that specifically to identify the research topics in relation to OGA. The related issues that prominent scholars have well discussed particularly in the context of cybersecurity will be address thoroughly in the related studies. As defined by Kitchenham and Charters [19][20], we used the simple SLR system. Compared to other approaches, the key distinctions between the methods employed in this analysis are listed below:

- Instead of a restricted manual search process, we used a broad and automatic search process.
- Three researchers obtained data on consistency and classification. For the papers found during the same time as the initial search, the median or mode value was taken as the consensus value (as appropriate). They used the process "consensus' and "minority report" for the collection of papers which were discovered during the initial search time.

A. Research Questions

The three research questions investigated in this study were chosen:

RQ1: How many researches and SLRs that related to OGA were published between 2015 and 2019 in cybersecurity perspective?
RQ2: What research topics are being addressed?
RQ3: What are the current gaps in OGA's studies in cybersecurity perspective?

B. Searching Process and Keywords

The search approach was focused on the move implemented by Yli-Huumo [23] that compresses all the processes as seen in Fig. 1 such as scanning, keywording and data extraction. In this report, a total number of 37 papers were collected. In order to select which of them intensely analyze, we conducted two exclusion stages - one is based on titles and the other is based on abstracts - and we included articles regarding to other aspects that addressing security and legal issues or purely technical aspects of OGA. Finally, a total of 25 articles were finalized whereby knowledge required in order to addressing the study.

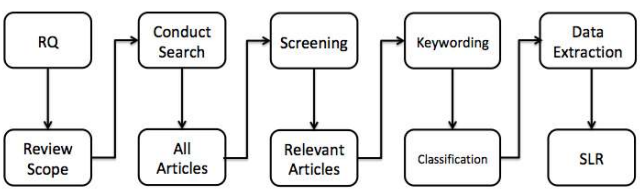

Fig. 1. Systematic Literature Review Search Process by Yli-Huumo [21]

We also followed the guidelines and instruction on SLR by Saltikov [22] and execute for most of the search process. Four digital libraries and one large indexing scheme were explored: IEEE Computer Society Digital Library; ACM; Citeseer; SpringerLink; and Network of Science. In addition, based on Kitchenham, we also tested the indexing method for SCOPUS. The description, keywords and overview were focused based on the subject of all queries. The searches were carried out between 2015 and 2019 and we used a collection of basic search strings for all sources except for SCOPUS and aggregated the results from each of the searches for each source:

1. ''Digital Addiction" AND ''Cybersecurity".
2. ''Internet Game Addiction" AND ''Cybersecurity".
3. ''Online Game Addiction" AND ''Cybersecurity".
4. ''Online Game Addiction" AND ''Phishing".
5. ''Online Game Addiction" AND ''Spamming".
6. ''Online Game Addiction" AND ''Social Engineering".
7. ''Online Game Addiction" AND ''Malicious Code".
8. ''Online Game Addiction" AND ''Authentication".
9. ''Online Game Addiction" AND ''Cybersecurity" AND "Literature Review".
10. ''Online Game Addiction" AND ''Cybersecurity" AND "Literature Analysis".
11. ''Online Game Addiction" AND ''Cybersecurity" AND "In Depth Survey" .
12. ''Online Game Addiction" AND ''Cybersecurity" AND "Literature Survey".
13. ''Online Game Addiction" AND ''Cybersecurity" AND "Meta-Analysis".
14. ''Online Game Addiction" AND ''Cybersecurity" AND "Past Studies".
15. ''Online Game Addiction" AND ''Cybersecurity" AND "Overview of Existing Research".

C. Screening

Due to the fact that not all found papers are relevant in their actual contents, screening process is compulsory to narrow down the search into relevant papers only [23]. At the first phase, papers were screened according to their titles and then studies that were not relevant to the research topic were excluded. For instance, the search engine shows papers related to OGA and data security in other scientific fields, which is not related to the cybersecurity issues. These articles were clearly beyond the reach of this comprehensive analysis of literature. Nevertheless, in some instances, the validity of the research depending on the title has been difficult to determine. In this case, papers were transferred for further reading process through the following stage. In the second step, we read each paper's abstracts which passed the preceding process. In addition, each paper was screened using a clear inclusion and exclusion criterion. Then, It was decided to exclude the following types of papers: (1) papers without full text availability, (2) papers where the main language was not English (i.e. Turkish), (3) papers that had addresses OGA from other aspects and (4) papers that were duplicates. When a paper passed all four exclusion requirements and after reading the abstract, it was deemed to concentrate on cybersecurity OGA and we agreed to progress to the next level.

III. Data Extraction Result

25 papers that have been written in the past five years (2015-2019) have been listed in this section. This grouping would include categorizing the findings depending on the research approach (qualitative and quantitative) except triangulation regarding to specific requirement. Based on this result, it is a strong evident that research regarding to OGA has continued to increase over the years of study. The results extracted from the analyzed papers were reported and organized to answer research question (RQ1, RQ2 and RQ3). Discussion on the results will follow in the next section. The results answering the research question were presented below in a form of discussion and summary tables of articles. For each study we discussed, we classified them according to the author and year, scope of article, the area of research and methodology used.

A. Qualitative Research

The first category in this classification is qualitative analysis. The authors used the questionnaire and the focus group in this category as a means to carry out their study. We have finalizing 12 articles that most related to OGA in cybersecurity perspective. Starting with a research conducted by Aivazpour [24] investigated the sufficient basis and the effect of impulsiveness on risky security behaviors in OGA by conducting an inductive and investigative interviews among the respondents in three separate categories to determine the Impulsivity and risky cybersecurity behaviors. Furthermore, Kerem Kilicer in his research [25] regarding to cyber human values scale and the study of development, validity and reliability have develop a scale to measure level of cyber human values based on behavior of online game in social media and cyberspace. The finding was derived on the basis of chosen demographics from the cyber values system for size, question item in the interview session and focus group observation. On the other hand, Hadlington [26] also highlighted in his article regarding to human factor in cybersecurity based on OGA environment whereby 5 factors model of personality from John and Srivastava 1999 were reveiled according to mindspace framework which was used to examine the impact of human factors to influence cybersecurity practices and behaviors in online game environment. Another research that focusing cybersecurity behaviors in OGA by Monica [14] also revealed internal and external control scale involving focus group interview.

Similar result also reported by Calvin Nobles [16] regarding to the article about botching human factors in cybersecurity in business organizations. The researcher has successfully disclosed the significance of human factors in online games based on interview sessions between addicted users. In terms of cybersecurity in particular, Samantha [17] has also been one of the famous author reporting on cyber-attacks and offering insight into contributing factors and tackling strategies especially among teenagers in the online gaming environment. The current status and future work also reposted very well and need special focus if other scholars want to continue the study. It also gives some alternative to review existing literature that related to cybersecurity especially involving the current issues using empirical research and qualitative data such as focus group.

Other scholars such as Arunesh [18] also contributing to the knowledge through the development of Stackelberg security games (SSG) which looking beyond a decade of success of selected games to mitigate phishing attack in online game environment and proposed the technical advance in SSG and sharing a future work in the study. The author also revealed the technical advance related to this topic using empirical research and combination of qualitative data. In another study performed by Hayani [27] that focus on cybersecurity element in OGA have enhance the cybersecurity awareness program on personal data protection among youngster in Malaysia. This effort was sustained from awareness campaign in enhancing safety and procedure according to the trend and current internet usage among youngsters. This study also has beneficial in preliminary data in order to emphasis on findings.

A recent study was conducted by Neupane [28] regarding to neural markers of cybersecurity involving fMRI also contributing in the study of phishing and malware warnings. The objective of this study is to introduce the neuroscience based on study methodology in order to inform the design of security systems in human brain. The marker on human brain regarding to cybersecurity and impulsivity were recorded and have a strong relationship with addictive behavior especially OGA. This claim can be supported by Hadlington [29] through his hand book regarding to cybercognition and relationship between brain, behavior and digital world. This book has emphasized on the definition of cybercognition and the related topic to these cognitive activities. This prominent author also has successfully exploring the concept of cyberspace and the connection with OGA in cybersecurity perspective.

Meanwhile, the researcher such as Hans de Bruijn [30] also not been left behind in building security awareness whereby he successfully develop the need for evidence-based framing strategies in his study regarding the challenge in framing policies in cybersecurity. The result from this study can offer better communication and very useful in mitigating policy makers paradoxes according to OGA. This study has benefit on policy maker evidence-based framing strategies using prediction equation based on qualitative data from respondents. Interviews were carried out to investigate the participants perceived toward these issues.

Finally, as for future potential direction in network attack such as phishing and social engineering, Arachchilage [31] has create a simple solution through phishing threat avoidance behavior research. He also recommends exploring the materiality of the model and develop a game design framework in order to thwart phishing attack and successfully implement the phishing education among the respondents based on interview and focus group. However, the research can also allow a broader spectrum of participants of diverse age, technical history and financial literacy. All the related qualitative articles were compressed in Table I.

TABLE I. QUALITATIVE ARTICLES

No	*Author and Year*	*Scope of Articles*	*Area of Research*	*Methodology Used*
1.	Monica Whitty, (2015) [14]	Individual differences in cybersecurity behaviors in sharing password perspective.	Focus on risky practice of sharing passwords.	Focus group interview
2.	Ajaya Neupane, (2016) [28]	Cybersecurity Neural Markers: Phishing and Malware Alerts fMRI research.	Introducing a research approach focused on neuroscience to guide the design of protection systems.	Empirical study, experimental based
3.	Arachchilage, (2016) [31]	Phishing threat avoidance behavior Game Design Framework to avoid phishing.	Phishing Education.	Model Interview
4.	Samantha Bordoff, (2017) [17]	Cyber-attack, reasons leading and tactics tackling: present status.	To study current cybersecurity relevant literature.	Empirical research Interview
5.	Hans de Bruijn, (2017) [30]	Building security awareness: The need for evidence-based framing strategies.	To discuss the challenge in framing policies on cybersecurity to offer better communication.	Document Summary and focus group
6.	Kerem Kilicer, (2017) [25]	Cyber human values scale: the study of development, validity and reliability.	Establish a scale to assess the extent of cyber-human principles focused on social networking and cyberspace actions.	Focus group interview
7.	Zahra Aivazpour (2018) [24]	Impulsivity and risky cybersecurity behaviors: a replication.	To investigate sufficient basis the effect of impulsiveness on risky security behaviors.	Replication examination and interview
8.	Lee Hadlington, (2018) [9]	The Human Factor in cybersecurity.	To examine the impact of human factors to influence cybersecurity practices and behaviors.	Analysis papers and focus group
9.	Calvin Nobles, (2018) [16]	Botching of human cybersecurity variables of corporation enterprises.	To analyze the important of human factors in cybersecurity.	Interviews and expert review
10.	Arunesh Sinha, (2018) [18]	Looking beyond a decade of success in Stackelberg Security Games (SSG).	To survey the technical advance in SSG and future work.	Empirical research
11.	Lee Hadlington, (2018) [29]	Cybercognition: Brain, Behavior and Digital World.	Definition of cybercognition and related topic to these cognitive activities.	Empirical study (book) and interview
12	Hayani Rahim, (2019) [27]	Improving the cybersecurity awareness program for the safety of personal data among young people in Malaysia.	To enhance cybersecurity awareness with current internet usage among youngster.	Preliminary research and focus group

B. Quantitative Research

The second category in this section is quantitative analysis. In this category, the authors used the survey as a tool for their data collection mechanism. We have finalizing 13 articles that most related to OGA in cybersecurity perspective between 2015 and 2019. Starting with Alrobai [32] in his Ph.D thesis addressed the engineering social networks to combat digital addiction especially OGA via survey of 657 participants. The findings indicate that student performance expectancy and effort expectancy are considered as significant factors influencing the OGA using online peer groups. As for future work, the author recommended extending the population of the study to design a persuasive system in mitigating OGA among the youngsters.

As we know, Lee Hadlington is one of the most prominent authors that contribute many articles regarding to OGA in cybersecurity perspective. One of the most influence articles that were produced by the author is related to human factors in cybersecurity emphasizing on examining the link between Internet addiction, impulsivity and attitudes towards cybersecurity and risky cybersecurity behaviors. This survey was implemented among the workers [11] in selected region in United Kingdom that contributing to human factors analysis and related scale such as ABIS, OCS, RScB and ATC-IB. Another study [20] which was demonstrate by Hadlington [33] also involving employees side, like an empirical assessment in United Kingdom according to employees attitude towards cybersecurity and risky online behaviors. This study was implemented between full time and part-time workers and tends to explore whether if the size of company and age towards cybersecurity affected the frequency to engage risky online behaviors. This study was pioneer basis and cited by Lemmens [34]. The third study which was recorded under Hadlington's supervision is related to media multitasking whether is good for cybersecurity or vice-versa [35]. The focus of the study is to explore the relationship between media multitasking and everyday cognitive failure on risky cybersecurity behaviors in order to engage in media multitasking. The findings indicate four main factors affecting media multitasking and Linear regression. This study revealed peer group as a motivational mechanism and tested with Kaiser-Meyer-Olkin (KMO) algorithm. In the same vein, Hadlington [33] also propose a study that exploring the role of work identity and work locus of control in information security awareness in order to find the difference between human factors and adherence to organization. Cyberloafing also have been investigated by Hadlington [36] and the relationship with Internet addiction which affected the organizational security in general. This article has exploring the survey among the workers in the side of security practices. The result regarding to IA Standardized estimated model were obtained including statistical assessment. Additionally, Hadlington [37] also execute an experiment regarding to segmentation analysis of susceptibility to cybercrime which is affected by Internet addiction. This study tends to explore if susceptibility to cybercrime can be linked to information security awareness and personal factors in cybersecurity domain. This process was gone through 40 college students together with six domains of addiction (salience, withdrawal, conflict, relapse, tolerance and mood modification). Instead of the study among of workers and adults, Hadlington [38] also have a contribution to research among adolescent. The article tittle "I cannot live without my tablet" was launched in order to examine children's experience of using tablet technology at home. This article has revealed the characteristic of participant regarding to OGA in mobile environment. The result obtained in this article was in line with Funk (1993), Fisher (1994) including Griffith and Hunt (1995).

Another prominent research by the author like Durak [10] also addressed the human factors and cybersecurity in OGA. This study related to an analysis of the relationship between high school students which suspected as addicted user and the state of providing personal cybersecurity and human values which effecting by addictive behavior. The result was obtained from high school students in Turkey related to human factors, human values and cybersecurity manners in online games. This research was based on Internet Addiction Scale by Young (1996) and the result also indicates the strong correlation within genre and tremendous curve on multiple regressions. Osman Erol from Turkey [39] also performed the personal cybersecurity provision scale development study that related to IA in order to develop a scale to determine user behavior that related to cybersecurity perspective. The result consists of item in the scale using selected model including Segmentation and classification of the item, demographic and graph which relate to Rational Additional Model (RAT) according to the respondent's demographic in the study.

Abdulmajeed Alqhatani [40] also produced a quantitative article that related to OGA in cybersecurity perspective when performing an exploration of parent's security and privacy concerns and practices regarding to addictive behavior among teenagers. This article provides a clear understanding of security and privacy on parents and teenagers. This research clearly revealed the research model together with sample question and the prediction of multiple regressions. On the same vein, Ling Li [15] also invested the impact of cybersecurity policy awareness on employees cybersecurity awareness in order To extend the published literature on cybersecurity behavior among 579 business manager. This study involves 21 items in game addiction scale, sosiodemographic and awareness characteristic. Margaret Gratian [41] have study the correlation between human traits and cybersecurity behaviors intentions in order to relate the human characteristic with cybersecurity human behavior intentions among 369 students. This study was conducted among homogenous sample according to the related theoretical framework. And last but not least, David Blackwell [42] has successfully explored the extraversion, neuroticism, attachment style and fear of missing out (FOMO) as predictors of social media use and Internet addiction. This article investigating whether these factors can affect the level of OGA among adolescent. The result was obtained from 271 respondents according to playing time per week statistic which relate to motives of gaming. All the related quantitative articles that discussed in this section were compressed in Table II.

TABLE II. QUANTITATIVE ARTICLES

No	*Author and Year*	*Scope of Articles*	*Area of Research*	*Methodology Used*
1.	Osman Erol, (2015) [39]	Personal cybersecurity provision scale development study.	To develop a scale to determine user behavior related to cybersecurity.	Survey
2.	Lee Hadlington, (2017)[36]	Can cyberloafing and internet addiction affected organizational security?	To investigate the link between cyber-loafing, internet addiction and knowledge of information security.	Questionnaire based study
3.	David Blackwell, (2017) [42]	Extraversion, neuroticism, type of commitment and risk of losing out as predictors of usage and addiction to social media.	To investigate if there were predictors of extraversion, neuroticism, attachment type and fear of losing out.	Social media
4.	Lee Hadlington, (2017) [37]	Cybercrime susceptibility segmentation study.	To investigate if cybercrime vulnerability may be linked to knowledge of computer protection and personal variables.	Survey Questionnaire
5.	Lee Hadlington, (2017) [11]	Human cybersecurity factors; the connection between internet addiction, impulsivity, cybersecurity attitudes, and dangerous cybersecurity behaviors.	Human factors and cybersecurity.	Survey using scale (ABIS, OCS, RScB and ATC-IB)
6.	Margaret Gratian, (2018) [41]	Correlating human traits and cybersecurity behaviors intentions.	To correlate human characteristic with cybersecurity human behavior intentions.	Survey
7.	Abdulmajeed Alqhatani, (2018) [40]	Exploring parent's security and privacy concerns and practices.	To provide clear understanding of security and privacy on parents and children.	Interview and observation
8.	Lee Hadlington, (2018) [20]	Employee's attitude towards cybersecurity and risky online behaviors: an empirical assessment in UK.	To explore if the size of company and age towards cybersecurity affected freq. to engaged risky online behaviors.	Survey (full and part-time employee)
9.	Lee Hadlington, (2018) [35]	The effect of media multitasking in cybersecurity.	To investigate the connection between media multitasking and daily cognitive failure with risky cybersecurity behaviors.	Survey Questionnaire
10.	Lee Hadlington, (2018) [33]	Exploring the role of job identification and control locus of job in understanding of information protection.	To explore the distinction between human influences and information security conformity.	Survey Questionnaire
11	Hatice Yildiz Durak, (2019) [10]	Human Factors and Online Gaming Addiction Cybersecurity: An Overview of the interaction between OGA high school students and the status of OGA 's private cybersecurity and human values.	Human factors, human values and cybersecurity in online games.	Survey and group discussion
12	Lee Hadlington, (2019) [38]	OGA in mobile environment among the children.	To examine children's experience of using tablet tech at home.	Survey Questionnaire
13.	Ling Li, (2019) [15]	Investigating the effect of understanding of cybersecurity policies on the understanding of cybersecurity among employees.	To extend the published literature on cybersecurity behaviour.	Survey and documentary analysis

IV. Discussion and Research Gap

We found the research gaps in the cybersecurity sense of the OGA studies in this systematic literature review that have the possibility to be checked for further analysis. The methodologies employed to categorize those gaps are as follows. First, we detecting the problems or limitations from the research papers which included in this study and secondly, we considering challenges that the authors have highlighted as a potential future work.

The first gap is lack of study on significant factors influencing the OGA among adolescent. Based on the summary of article in Table 1 and Table 2, the literatures do revealed some interesting highlights on human factors in online game addiction, but mostly in a limited views and perspectives. This indicates that there is lack of research particularly in looking further into the context of understanding the human factors in exhibiting the intention of secure behavior particularly among adolescent who are addicted to online games in cybersecurity perspective. Hence, this research tends to explore this path further as it is highly relevant with the current situation and requirement in order to contribute to the new knowledge in this domain area

The second gap is the lack of technology adoption models used in addressing the issue of OGA in the side of cybersecurity. It has now becoming crucial that this addictive behavior (i.e.: online games) has high possibility of affecting the cybersecurity awareness embodiment in an individual. This happens when users tend to act in an unethical way if they are not allowed to proceed playing or being stopped from playing due to any constraints or hurdles. More alarming, Hadlington [26] also has highlighted that the intention becomes the most influenced factors that can affect ones behavior along with attitude towards cybersecurity especially in the context of online game addiction. Unfortunately, the issue of online game addiction that relates to cybersecurity perspective has been addressed very limitedly. Moreover, the issue gets complicated as not many behavioral studies have actually focused on addictive behavior relating to cybersecurity context. Therefore, this study found the gaps that the future work should be preform and intending to propose a secure intention behavior model of online game addiction from cybersecurity perspective among adolescent. As mentioned earlier, this research indicates that people who are addicted to online gaming may hypothetically react outside the boundaries of addiction to the point that they may jeopardize their personal information by placing computer protection at risk.

The final gap is the absence of a high-quality study report on the relevant paradigm in order to mitigate the OGA and cyber protection solutions. Most of the papers identified were not detailed in terms of study in addressing the problem of OGA among adolescents. The need for extensive, high-quality publications on OGA matters together with a significant commitment to cyber protection should be performed in order to fulfill the gaps.

V. Conclusion and Future Work

In conclusion, as online gaming and other interactive media have become an important part of everyday life, recognizing and distinguishing the ways in which excessive usage is linked to growth especially on mobile platforms is become crucial and more important at this time. We concern about OGA in cybersecurity perspective which also become crucial issues among adolescent whereby they have potentially exposed to network attack such as Phishing, Social Engineering, Spamming and others when they involved in OGA. The issue of online game addiction that relates to cybersecurity perspective also has been addressed very limitedly. Moreover, the issue gets complicated as not many behavioral studies have actually focused on addictive behavior relating to cybersecurity context. Thus, it is a vital need for future research to disentangle this issue in order to describe briefly the relationship between OGA and cybersecurity perspective especially among adolescent.

Acknowledgement

This research was supported by Ministry of Higher Education (MoHE) through Fundamental Research Grant Scheme (Ref: FRGS/1/2020/ICT03/UUM/02/1). The content of this article is solely the responsibility of the authors and does not necessarily represent the official views of the MoHE, Malaysia.

References

[1] M. Griffiths, "A 'components' model of addiction within a biopsychosocial framework," *J. Subst. Use*, vol. 10, no. 4, pp. 191–197, 2005.

[2] A. Błachnio, A. Przepiórka, and N. S. Hawi, "Exploring the Online Cognition Scale in a Polish sample," *Comput. Human Behav.*, vol. 51, no. PA, pp. 470–475, 2015.

[3] B. D. Ng and P. Wiemer-Hastings, "Addiction to the Internet and online gaming," *Cyberpsychology Behav.*, vol. 8, no. 2, pp. 110–113, 2005.

[4] M. Griffiths, "Internet gambling in the workplace," *J. Work. Learn.*, vol. 21, no. 8, pp. 658–670, 2009.

[5] L. T. Lam, "Internet gaming addiction, problematic use of the Internet, and sleep problems: A systematic review," *Curr. Psychiatry Rep.*, vol. 16, no. 4, 2014.

[6] A. Shams and M. Mahmudul, "DIGITAL DEVICE ADDICTION EFFECT ON LIFESTYLE OF," vol. 1, no. 2, pp. 21–44, 2018.

[7] J. Bishop, *Psychological and social implications surrounding internet and gaming addiction*. 2015.

[8] K. S. Young, "Internet addiction: A handbook and guide to evaluation and treatment," pp. 173–189, 2011.

[9] L. Hadlington, "The 'Human Factor' in Cybersecurity," *IGI Glob.*, vol. 3, pp. 46–63, 2018.

[10] H. Yildiz Durak, "Human Factors and Cybersecurity in Online Game Addiction: An Analysis of the Relationship Between High School Students' Online Game Addiction and the State of Providing Personal Cybersecurity and Representing Cyber Human Values in Online Games," *Soc. Sci. Q.*, vol. 100, no. 6, pp. 1984–1998, 2019.

[11] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, p. e00346, 2017.

[12] N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," *Comput. Human Behav.*, vol. 29, no. 3, pp. 706–714, 2013.

[13] J. Leach, "Improving user security behaviour," *Comput. Secur.*,

vol. 22, no. 8, pp. 685–692, 2003.

[14] M. Whitty, J. Doodson, S. Creese, and D. Hodges, "Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords," *Cyberpsychology, Behav. Soc. Netw.*, vol. 18, no. 1, pp. 3–7, 2015.

[15] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. Inf. Manage.*, vol. 45, no. February 2018, pp. 13–24, 2019.

[16] C. Nobles, "Botching Human Factors in Cybersecurity in Business Organizations," *HOLISTICA – J. Bus. Public Adm.*, vol. 9, no. 3, pp. 71–88, 2018.

[17] S. Bordoff, Q. Chen, and Z. Yan, "Cyber Attacks, Contributing Factors, and Tackling Strategies: The Current Status of the Science of Cybersecurity," *Int. J. Cyber Behav. Psychol. Learn.*, vol. 7, no. 4, pp. 68–82, 2017.

[18] A. Sinha, F. Fang, B. An, C. Kiekintveld, and M. Tambe, "Stackelberg security games: Looking beyond a decade of success," *IJCAI Int. Jt. Conf. Artif. Intell.*, vol. 2018-July, pp. 5494–5501, 2018.

[19] D. J. Kuss, "Internet gaming addiction: Current perspectives," *Psychol. Res. Behav. Manag.*, vol. 6, pp. 125–137, 2013.

[20] L. Hadlington, "Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom," *Int. J. Cyber Criminol.*, vol. 12, no. 1, pp. 269–281, 2018.

[21] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on Blockchain technology? - A systematic review," *PLoS One*, vol. 11, no. 10, pp. 1–27, 2016.

[22] B. Kitchenham *et al.*, "Systematic literature reviews in software engineering-A tertiary study," *Inf. Softw. Technol.*, vol. 52, no. 8, pp. 792–805, 2010.

[23] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering - A systematic literature review," *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009.

[24] Z. Aivazpour and V. Srinivasan Rao, "Impulsivity and risky cybersecurity behaviors: A replication," *Am. Conf. Inf. Syst. 2018 Digit. Disruption, AMCIS 2018*, no. 2017, pp. 1–9, 2018.

[25] K. Kilicer, A. N. Coklar, and V. Ozeke, "Cyber human values scale (i-value): the study of development, validity and reliability," *Internet Res.*, vol. 27, no. 5, pp. 1255–1274, 2017.

[26] A. R. Gillam and W. T. Foster, "Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study," *Comput. Human Behav.*, vol. 108, no. February, p. 106319, 2020.

[27] N. H. A. Rahim, S. Hamid, and M. L. M. Kiah, "Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment," *Malaysian J. Comput. Sci.*, vol. 32, no. 3, pp. 221–245, 2019.

[28] A. Neupane, N. Saxena, J. O. Maximo, and R. Kana, "Neural Markers of Cybersecurity: An fMRI Study of Phishing and Malware Warnings," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 9, pp. 1970–1983, 2016.

[29] N. Kashyap, " Lee Hadlington, Cybercognition: Brain, Behaviour, and the Digital World ," *Psychol. Learn. Teach.*, vol. 17, no. 3, pp. 323–325, 2018.

[30] H. de Bruijn and M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," *Gov. Inf. Q.*, vol. 34, no. 1, pp. 1–7, 2017.

[31] N. A. G. Arachchilage, S. Love, and K. Beznosov, "Phishing threat avoidance behaviour: An empirical investigation," *Comput. Human Behav.*, vol. 60, pp. 185–197, 2016.

[32] A. A. Alrobai, "Engineering Social Networks to Combat Digital Addiction : The Case of Online Peer Groups Amen Ali Alrobai," no. April, p. 416, 2018.

[33] L. Hadlington, M. Popovac, H. Janicke, I. Yevseyeva, and K. Jones, "Exploring the role of work identity and work locus of control in information security awareness," *Comput. Secur.*, vol. 81, pp. 41–48, 2019.

[34] J. S. Lemmens, P. M. Valkenburg, and J. Peter, "Development and validation of a game addiction scale for adolescents," *Media Psychol.*, vol. 12, no. 1, pp. 77–95, 2009.

[35] L. Hadlington and K. Murphy, "Is Media Multitasking Good for Cybersecurity? Exploring the Relationship between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors," *Cyberpsychology, Behav. Soc. Netw.*, vol. 21, no. 3, pp. 168–172, 2018.

[36] L. Hadlington and K. Parsons, "Can Cyberloafing and Internet Addiction Affect Organizational Information Security?," *Cyberpsychology, Behav. Soc. Netw.*, vol. 20, no. 9, pp. 567–571, 2017.

[37] L. Hadlington and S. Chivers, "Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors," *Polic. A J. Policy Pract.*, no. April, pp. 1–14, 2018.

[38] L. Hadlington, H. White, and S. Curtis, "'I cannot live without my [tablet]': Children's experiences of using tablet technology within the home," *Comput. Human Behav.*, vol. 94, pp. 19–24, 2019.

[39] O. Erol, Y. L. Şahin, E. Yılmaz, and H. İ. Haseski, "Personal Cyber Security Provision Scale development study<p>Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması," *Int. J. Hum. Sci.*, vol. 12, no. 2, p. 75, 2015.

[40] A. Alqhatani and H. Lipford, "Exploring Parents ' Security and Privacy Concerns and Practices," no. February, pp. 1–6, 2018.

[41] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, 2018.

[42] D. Blackwell, C. Leaman, R. Tramposch, C. Osborne, and M. Liss, "Extraversion, neuroticism, attachment style and fear of missing out as predictors of social media use and addiction," *Pers. Individ. Dif.*, vol. 116, pp. 69–72, 2017.