

PAPER • OPEN ACCESS

## Risk and Threat via Online Social Network among Academia at Higher Education

To cite this article: Hanizan Shaker Hussain *et al* 2018 *J. Phys.: Conf. Ser.* **1018** 012008

View the [article online](#) for updates and enhancements.

### Related content

- [The Continuing Quest for Missile Defense: Ballistic missile threats](#)  
P Pella
- [Emerging Models for Global Health in Radiation Oncology: ICT-powered models of global radiation oncology](#)  
W Ngwa and T Ngoma
- [Why not do both?](#)  
Stephen Sweeney



**IOP | ebooks™**

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

# Risk and Threat via Online Social Network among Academia at Higher Education

**Hanizan Shaker Hussain, Roshidi Din, Nik Zulkarnaen Khidzir,  
Khairul Azhar Mat Daud, Suzastri Ahmad**

<sup>1</sup>School of Computing, College Arts and Sciences, Universiti Utara Malaysia,  
06010 UUM Sintok, Kedah

\*Corresponding Author's Email: roshidi@uum.edu.my

**Abstract.** The evolution of information and communication technologies (ICT) nowadays has changed the life style of human living. The current modern societies have adopted ICT as an important thing that they are really needed in their life, especially as a tool to be used for communications activity. However, unfortunately ICT also exposed its user in circumstances of risk, threats and vulnerability. This paper will discuss the risk and threats to the users who are using social media as a medium to communicate. In this paper, the fraction of user will be divided by two types which are gender and working experience. The data that obtained from the distributed of questionnaires among respondent will be analysed by using SPSS. Data will be analysed by using two-way ANOVA statistic in order to examine the significant level in between gender and working experience as an independent variable in this study with the level of threats in cybersecurity risk towards lecturers who are working in higher education institutions in Malaysia. This article also will provide an empirical data and will be referred to another researcher in the future for their further research perhaps.

## 1. Introduction

Cybersecurity risk means the risk which has occurred to the users who are using information and communication technologies in several of aspect. In this paper, discussion will be focused on the lecturers who are working in higher education institution in Malaysia as the user for ICT technologies. In nature, lecturers deal with ICT technologies in teaching activities such as e-learning, research activity, searching for varied types of information through internet, communication in research activities by applying video conferencing to discuss with their colleagues who are located at various places, send and deliver document through email and a variety of activities regarding to their nature of work. By exposing themselves through online networking via varieties of online medium, this will expose lecturers to the threats. However, many lecturers or users are really didn't realize with the risk that they will face. This paper will show the empirical outcome regarding to the level of threats in cybersecurity risk among lecturers at higher education institution in Malaysia.



## **2. The integration of Cybersecurity in Malaysian's Higher Education**

The method of face-to-face learning needs to be reviewed in order to enhance the effectiveness of instructional regarding to the growing up of tremendous information and communication technology in this age [1]. Learning in 21st century is about implementing digital technologies [1]. Social media is a very important medium that must be mastered by the lecturers who are working in higher education institution. By using social media, those who are working as lecturers will tremendously build up their reputation in the academic world. By applying social media, lecturers will build their reputation and bridging in career opportunities such as to market themselves in academicians' activity such as research, publications, co-operation, collaboration and so on [2]. By using social media, scholars will position themselves in popularity of ranking among academicians around the world. In learning and teaching activity for example, the current methods of learning such as problem based learning, inquiry learning and so on which is in group of constructivism learning will be implemented more effectively by the integration of all kind of social medias which is known as e-learning in order to deliver and convey knowledge among students in higher education institutions.

Unfortunately, Social Digital Media could lead to several critical cybersecurity risks that could cause serious impact to the lecturers itself in context of threats among lecturers in higher education institution in Malaysia [2]. Therefore, the extensive awareness programme on cybersecurity risk should be conducted continuously in higher learning institutions in order to minimize the possibility of the risk happened and mitigate their impact more effectively. The entire higher learning institutions eco-sphere will get benefit from this programme as a preventive approach to manage the confidentiality, integrity and availability of the information transported through cyberspace.

## **3. Cybersecurity Challenges and Requirements**

Online social digital media has become very useful equipment in the era of digital nowadays. By the used of online social media in a right way and proper technic and well strategies, the learning activities will be delivered more effectively and it's concurrent with the needs of educations around the globe. However, Nik Zulkarnaen et.al [2] asserted that besides the advantages functions and capability offered by this technology, it's still have several issues and challenge that need to be contemplated by other scholars.

Hanna, et. al. [3] asserted that, users will be able to create online communities to share information, ideas, personal messages, and other content through the social media platform. The rapid evolution of social media was build up and create the ecosphere of communication regardless of border via a variety of social media platforms that currently exist [4]. The emerging of digital technology to promote social media as a communication platform had given many effects to the societies' ways of life. In education aspect, a traditional or conventional way of learning and teaching need to be reviewed and do a little bit of adjustment in order to ensure our education system is relevance and parallel with other countries that adopt e-learning as their main agenda in their country. The challenging to begin the implementation of social media as a main platform in education activities in higher education institution is to break the conventional practices among all education communities. By the way, after through with a long challenging process to shift the perception and prejudice among all members in educations communities and with a proper strategic plan proposed by the ministry of education, more than 15 years ago, now Malaysia is one of the countries in Asia that have some advanced technologies which is able to support ICT and provide internet and social media to the citizens.

Generally, social media considered as part of the internet society ecosystem that serve an effective communication channel for cyber community. Besides the unbelievable opportunities offered through this technology, cybersecurity risks considered as emerging challenges to look into seriously [5]. Regarding to that issue and the expected risk of cybersecurity, this paper will discuss about the factors of threats that may be faced by the lectures who are working at higher education institution in Malaysia. By looking and examine the level of threats in cybersecurity risk among lecturers at higher education institution in Malaysia, hopefully the finding of this study will give a bit of view to the authorities who are making policies and strategic planning in order to prevent unpleasant matters from occurs to our nation in the future.

Cybersecurity risk is currently becoming serious issues in digital social media due to the increasing number of social media population growth [2]. Valerică Oana [6], asserted that the spectrum of the risks are really wide and unpredictable. Social media allows social engineer use the psychological manipulation of people into performing actions confidential information for the purpose of information gathering, fraud or system access [7]. Digital Social Media becomes the source of information for Social Engineer to capture and harvest the useful information for the purpose of the cyber-attack [8]. Online Social Media might highly contribute to cybersecurity risks on Critical Information Infrastructure and need to be identified and measure in order to understand the level of severity for each of them so that will be managed effectively [2]. The capability of Online Social Media act as communication platform among cyber community and its could also become a phishing pond for cyberwarfare and cybercrimes. For extreme cases, the impact of the cyberwarfare and cybercrime might cause human personal security, safety and psychological impact in nature [9].

#### 4. Research methodology

This research was done by using quantitative methods. Data obtained through the administration of questionnaire to hundred (100) respondents. The respondents were comprised of lecturers from Higher Education Institution in Malaysia. Respondents were randomly selected. The instrument was developed after several constructs involving the formation of threats in cybersecurity risk among lecturers who are using online social media as a communications medium to work. The value of validity and reliability of the instruments were measured through the pilot test. A pilot test was conducted on 30 lecturers from a selected higher education institution in Malaysia separately (Table 1). Through the pilot study, the obtained values of reliability and validity of the instrument was very high. The value of Cronbach Alpha,  $\alpha$  obtained was 0.962. This study was conducted in the state of Selangor. The respondents comprised of 100 lecturers from higher education institution in Malaysia. A brief demographic data distribution of respondents involved in this study is presented in table 2 below.

**Table 1.** Reliability Test Result: Cronbach's Alpha Value

Cybersecurity Risk Factors	Items	Cronbach's Alpha Value	Total Num. of Respondents (N)
Threats	18	0.962	100

**Table 2.** Lecturers' participation by gender

Gender	Frequency	Percent
Male	39	39%
Female	61	61%
Total (N)	100	100%

Table 2 show the gender tabulation among respondents who are involved in this study. Respondents consisted of 52 (17.3%) males and 248 (82.7%) females.

**Table 3.** Working Experience percentage

Working Experience	Frequency	Percent
5 years and below	10	10%
6 years to 10 years	30	30%
11 years to 14 years	23	23%
15 years to 20 years	19	19%
21 years and above	18	18%
Total (N)	100	100%

Table 3 shows the distribution of fractional group of respondents who have different periods of working experience. There are five (5) fraction of working experience among respondents, first is lecturers who had been teaching in the last five (5) years, second is lecturers who had been working in the last six (6) years to ten (10) years, third is lecturers who have working experience in the last eleven (11) years to fourteen (14) years, fourth is the lecturers who have working experience in fifteen (15) years to twenty (20) years and lastly is the lecturers who are working more than twenty-one (21) years.

Data obtained from the questionnaire related on threats in cybersecurity risk to the lecturers who are working at higher education in Malaysia was analyze by using two-way analysis of variance (ANOVA). This analysis was made by using SPSS statistical package for social science (SPSS Version 21). ANOVA analysis was conducted to determine the joint effect of two independent variables on one dependent variable.

**Table 4.** Descriptive Statistics  
Dependent Variable: Risk Threats of Cyber Security at Higher Education in Malaysia

Teachers' Gender	Teaching Experiences	Mean	Std. Deviation	N
Male	5 years and below	2.7889	.39752	5
	6 years to 10 years	3.0556	.72344	15
	11 years to 14 years	3.3765	.49906	9
	15 years to 20 years	2.5278	.66782	2
	20 years and above	3.3194	1.13146	8
	Total	3.1225	.75361	39
Female	5 years and below	3.1111	.31427	5
	6 years to 10 years	3.2815	.87878	15
	11 years to 14 years	3.1270	.58892	14
	15 years to 20 years	3.3529	.69443	17
	20 years and above	3.3056	.69401	10
	Total	3.2559	.68676	61
Total	5 years and below	2.9500	.37811	10
	6 years to 10 years	3.1685	.79917	30
	11 years to 14 years	3.2246	.55769	23
	15 years to 20 years	3.2661	.72188	19
	20 years and above	3.3117	.88441	18
	Total	3.2039	.71282	100

**Table 5.** Two-way ANOVA test results

Source	Sum of Squares	df	Mean Square	F	Sig. (p)	Partial Eta Squared
Gender	.821	1	.821	1.569	.214	.017
Working Experiences	1.367	4	.342	.653	.627	.028
Gender * Working Experiences	1.904	4	.476	.909	.462	.039
Error	47.125	90	.524			
Total	1076.793	100				

\* Value is significant when  $p < 0.01$

a. R Squared = .063 (Adjusted R Squared = -.002)

According to Table 5, it was found that there was no significant difference in level of threats to cybersecurity risk in higher education of Malaysia among lecturers based on gender ( $F(1, 90) = 1.57$ ,  $p = 0.21$ ), in which the effect size is very small ( $\eta^2 = 0.02$ ). This means that the level of threats in cybersecurity risk is the same between of genders. Comparison of the threats on cybersecurity risk in higher education in Malaysia toward working experience, found that no significant differences in the level of threats on cybersecurity risk in higher education of Malaysia based on working experience ( $F(1, 90) = 0.653$ ,  $p = 0.63$ ), in which the effect size is very small ( $\eta^2 = 0.03$ ). In the perspective of higher learning institution, personal working experience does not influence much the cybersecurity risk threats level.

According to Table 5, there was no significant interaction effect between gender and working experience on the threats of cybersecurity risk in higher education of Malaysia ( $F(1, 90) = 0.909$ ,  $p = 0.039$ ). This means that the level of threats of cybersecurity risk in higher education of Malaysia is not dependent on the join effect gender and working experience. Therefore, further analysis is not needed in order to describe the lecturers' threats of cybersecurity risk based on gender and working experiences.

## 5. Conclusion

The current trend of social communications is supported by digital technologies. Every kind of communication activities among members of society was applying the social media as an effective and practical platform. In the scope of educations, e-learning is an indicator to show the priorities of social media in learning and teaching activity. Regarding to that, almost all lecturers at higher education institutions in Malaysia have been using social media as an important and main tool of their teaching activity. In other words, lecturers were exposed with the global ecosphere according to their academicians' activities such as research, collaboration, publications, and conferences, e-learning and so on.

The studies finding discovered the level of threats among lecturers in view of gender and working experiences factors among the lecturers who are working at higher education institution in Malaysia. The finding shows that the level of threat toward lecturers is not really significant with the gender and working experience. Regarding to the finding of this research, the authorities who are intended to do strategic planning or proposed some kind of policies regarding to the cybersecurity risk doesn't need to worry to thinking about the factors of gender and working experience. The two independent variables that are highlighted in these studies were being concluded that they do not give any effect to contribute threats in cybersecurity risk.

## References

- [1] Khairul Azhar Mat Daud 2016 A New Interaction Design Model For Digital Chronological Infographic Development *Elixir Edu. Tech.* 90 (2016) 37522-37527 ISSN: 2229-712X
- [2] Nik Zulkarnaen Khidzir, Ahmad Rasdan Ismail, Khairul Azhar Mat Daud, Mohamad Shahfik Affendi Abdul Ghani, Suriatini Ismail and Asrul Hery Ibrahim. Human 2016 Factor of Online Social Media Cybersecurity Risk Impact on Critical National Information Infrastructure *7th International Conference on Applied Human Factors and Ergonomics (AHFE 2016)*
- [3] Hanna, R, Rohm, A, and Crittenden, V L 2011 We're all connected: The power of the social media ecosystem *Business Horizons* **54**(3) 265–273.
- [4] Colliander, J, and Dahlén, M 2011 following the fashionable friend: The power of social media. *Journal of Advertising Research* **51**(1) 313–320.
- [5] National Cyber Security Policy 2013 *An Assessment. Institute for Defence Studies and Analyses* [http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013\\_stomar\\_2608](http://www.idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_2608) 13
- [6] Valerică GREAVU-ŞERBAN, Oana ŞERBAN 2014 Social Engineering a General Approach *Informatica Economica Journal* **18** no. 2 2014.
- [7] Anderson and Ross J 2008 *Security engineering: a guide to building dependable distributed systems (2nd ed.)* Indianapolis IN: Wiley 1040. ISBN 978-0-470-06852-6. Chapter 2, 17.
- [8] Kaplan, A. M, and Haenlein, M. 2010 Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons* **53**(1) 59–68.
- [9] Tang, Q, Gu, B and Whinston, A B 2012 Content contribution for revenue sharing and reputation in social media: A dynamic structural model *Journal of Management Information Systems* **29**(2) 41–76.