Critical Cybersecurity Risk Factors in Digital Social Media: Analysis of Information Security Requirements

Nik Zulkarnaen Khidzir[1,2], Ahmad Rasdan Ismail[1], Khairul Azhar Mat Daud[1], Mohamad Shahfik Afendi Abdul Ghani[1], and Mohd Asrul Hery Ibrahim[3]
[1]Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, Malaysia
[2]Global Entrepreneurship Research Innovation Centre, Universiti Malaysia Kelantan, Malaysia
[3]Faculty of Business and Entrepreneurship, Universiti Malaysia Kelantan, Malaysia
Email: {zulkarnaen.k, rasdan, azhar.md, shahfik.ag, hery.i}@umk.edu.my

***Abstract*—Digital Social Media provides an excellent communication platform through countless application such as online forums, chatting channels, video streaming and blogs. The greatest technological invention ever discovered and gaining fast popularity globally among internet user. Unfortunately, Social Media comes with several risks, especially the cybersecurity risks that could cause serious impacts to the cyber community. Cybersecurity risks are currently becoming serious issues in Social Media. The excitement of sharing their activities, statuses, locations, feelings, they do not realize that the information they shared could contribute to the critical cybersecurity risks. Hence, the objectives of the research are to determine the critical cybersecurity risks in social media digital platforms; and to discuss their criticalness for three information security core principles. Questionnaires were distributed to various cyber community, including professional and non-professional user that commonly used social media digital. The findings show that the most critical cybersecurity risks on the three core principles of information security requirements are Identity Theft; Information Manipulation; Cyber Assault/ Bullying; Information Theft; Espionage; and Privacy Violation. Findings also highlights other critical cybersecurity risk factors in digital social media. Through the findings, cyber community would be able to identify the critical cybersecurity risk factors and address them effectively.**

***Index Terms*—cybersecurity risk, digital social media, internet society, privacy violations, identity theft, social engineering**

I. Introduction

Cybersecurity is beyond securing a perimeter around individual's digital or virtual assets [1]. It entails a comprehensive understanding of every element that might enable penetration, interaction and compromise, and that could lead to catastrophic events or risks. Digital Social Media is among the most popular communication platform for the entire cyberspace community ecosystem that grip into every element of our social, professional and personal lives. Moreover, digital social media is considered as the new telecom; essentially it has become the preferred way to communicate among friends, colleagues, and even adversaries [1]. Unfortunately, digital social media could enable threats and vulnerabilities that lead to cybersecurity risks to cyber community and the organizations. There is a wide range of the cybersecurity risks have been identified from technology-driven to human factor risks in nature.

This paper explores the empirical findings on the cybersecurity risk factor criticalness for digital social media. The study focuses into criticalness level of 18 cybersecurity risk factors for each three core principles of information security requirements.

II. Digital Social Media, Information Security and Cybersecurity Risk

A. Digital Social Media and Information Security

A generic definition for the term "social media" is given as "… the set of Web-based broadcast technologies that enable the democratization of content, giving people the ability to emerge from consumers of content to publishers [2]. With the ability to achieve massive scalability in real time, these technologies empower people to connect with each other to create (or co-create) value through online conversation and collaboration" [2].

Another definition of social media by Merriam-Webster is "form(s) of electronic communication…..through which user creates online communities to share information, ideas, personal messages, and other content" [3]. Besides the excitement of sharing information about their activities, status, location, feeling, etc, they do not realize that the information that they share in digital media social could contribute to the cybersecurity risks that might be difficult to manage and mitigate. The similar principles of information security risk [4] was adopted to redefine the new term of cybersecurity risks nature. Cybersecurity risks are the chances of electronic forms of threats action on core principles of information security [5] such confidentiality, integrity, availability to cause impact contributed to security incidents. Hence the study analyzed the criticalness level of cybersecurity risks

Manuscript received February 23, 2016; revised June 17, 2016.

doi: 10.18178/lnit.4.1.18-24

factor for these three core principles of information security [5].

B. Cybersecurity Risk Factors

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access [6], [7]. In a computing context, the term security implies cybersecurity. According to a recent research and analysis of U.S. spending plans, the federal government has allotted over $13 billion annually to cybersecurity over the next five years [6]. But then, another critical aspect of cybersecurity is the human factor that could also consider among challenging issues to manage and mitigate. Common Cybersecurity Risk Factors such Phishing Ponds, Privacy Violation, Risk of Losing the legal battle, Corporate Espionage, Viruses and Malware, Productivity Loss [7], [8]. Table I highlight 18 generic cybersecurity risk factors involved in the study.

TABLE I. GENERIC CYBERSECURITY RISK FACTORS

Factors ID	Cybersecurity Risk Factors	Ref.
R1	Identity Theft	7, 8, 9, 10
R2	Viruses and Malware	7, 8
R3	Cyber Crime	7, 8, 13, 14
R4	Attack of the Software	7, 8, 16
R5	Productivity Loss	8
R6	Risk of Losing the Legal Battle	8, 10
R7	Corporate Espionage	8, 10
R8	Espionage	8, 10
R9	Terrorisms	8, 10, 16
R10	Information manipulation	8, 11, 12
R11	Cyber Assault/ Bullying	8, 12
R12	Advanced Persistence Threats	8, 12
R13	Information Theft	8, 12
R14	Phishing Pond	8, 12
R15	Privacy Violation	8, 12
R16	Cyber Attacks	8, 12, 15
R17	Insider	8, 13
R18	Transactional	8, 13, 16

Cybersecurity is becoming increasingly important as more information and technology are being uploaded in cyberspace. This has led to new terms such as cyberwarfare and cyberterrorism. More and more critical infrastructure is being controlled via computer programs that, while increasing efficiency, exposes new vulnerabilities [9]-[17]. The test will be to see if governments and corporations that control critical systems such as energy, communications and other information will be able to prevent attacks before they occur [17].

C. Cybersecurity Issues and Challenges in Digital Social Media

Digital Social Media is gaining fast popularity among internet user globally. Unfortunately, Digital Social Media does not always provide a positive outcome and the desired benefit. It comes with several risks, especially the cyber security risks that could cause serious impact to the organization and cyber community. Cybersecurity risks are currently becoming serious issues in digital social media due to the increasing number of social media population. Cybersecurity risks caused by common risk factors, which are threats and vulnerability of information in social media. Social media allows social engineer use the psychological manipulation of people into performing actions of confidential information for the purpose of information gathering, fraud or system access [18], [19]. Digital Social Media becomes the source of information for Social Engineer to capture and harvest useful information for the purpose of the cyber-attack.

Therefore, this study will explore and determine the critical cybersecurity risk in digital social media networking as a preliminary study for technology and human factor aspect of cybersecurity risk.

III. RESEARCH METHODOLOGY

A study using questionnaire survey was applied in this research. Five-Point-Likert-Scale was used to measure the criticalness of cybersecurity risk factors. Both primary and secondary data were used in order to accomplish this research objectives. Cybersecurity risk factors as described in the previous section were used to determine whether similar risk factors exist and how critical are they for Malaysian social media digital users and cyber communities.

IV. RESEARCH MODEL

The research model in Fig. 1 is built based on the combination of several past literatures instead of a single research model.

Refer to Table I for a list of generic cybersecurity risk factors. The research model discussed the cybersecurity risk factors in digital social media. Eighteen (18) cybersecurity risk factors were used in the research to determine their ranking based on risk criticalness in Digital Social Media. Fig. 1 illustrates the model of the research.

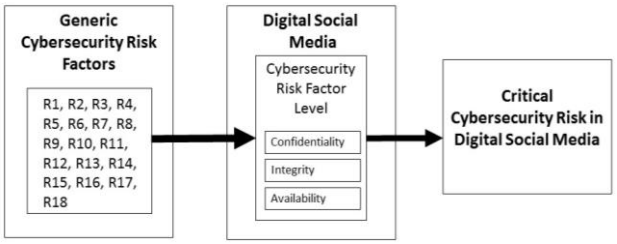

Figure 1. Research model.

V. FINDINGS AND DISCUSSIONS

The survey questionnaire captured background data of respondent profiles for 33 respondents from various cyber community and knowledge society individual in Malaysia. This section discusses respondents' demographic profile, social media digital cybersecurity core principles analysis, cybersecurity risk factors, as well as results of critical cybersecurity risk factors in social media digital.

The Analysis of both of these primary data was supported by the application of appropriate statistical techniques. The analysis led to several significant discoveries and expansion of existing knowledge. This section discusses the findings of the study in detail.

A. Respondents' Demographic Profiles

Respondents' demographic profile examined respondents' personal gender, age, professional experiences, organizational sectors and their industrial involvements. Most of them are the professional and senior executives from various organizations and institutions in Malaysia.

Therefore, the analysis showed that most of the respondents were considered as appropriate professional that possess sufficient experience to response to the entire question trustfully and accurately. Table II summarized the demographic profiles of respondents involved in the study.

TABLE II. RESPONDENT'S DEMOGRAPHIC PROFILES DATA

Respondent's Demographic Items		
Respondent's Gender	**Frequency**	**Percentage**
Male	*18*	*54.5 %*
Female	*14*	*42.4 %*
Respondent's Age	**Frequency**	**Percentage**
26 – 30 years	7	21.2 %
31 – 35 years	8	24.2 %
36 – 40 years	6	18.2 %
41 – 45 years	6	18.2 %
46 – 50 years	2	6.1 %
> 50 years	3	9.1 %
Working Experiences	**Frequency**	**Percentage**
< 5 years	9	27.2 %
6 – 10 years	5	15.2 %
11 – 15 years	2	6.1 %
15 – 20 years	11	33.3 %
> 20 years	6	18.2 %
ICT Security Experiences	**Frequency**	**Percentage**
0 Year	7	21.2 %
1 – 3 years	14	42.4 %
4 – 6 years	5	15.2 %
> 6 years	7	21.2 %
Organizational Sector	**Frequency**	**Percentage**
Government - Link – Companies Sector	3	9.1 %
Government Sector	28	84.9 %
Private Company Sector	2	6.1 %
Industry Involvement	**Frequency**	**Percentage**
Creative Technology	2	6.0 %
Healthcare Private	2	6.0 %
Healthcare Government	1	3.0 %
Higher Education	23	69.7 %
Information Communication Technology	2	6.0 %
Services	3	9.1 %
Total	**33**	**100%**

B. Reliability Test

Cronbach's Alpha Coefficient was used to test the survey item's reliability. A coefficient value which is closer to "1" is required. The Cronbach Alpha value of Cybersecurity risks in term of Confidentiality, 0.970; Integrity, 0.964 and Availability, 0.980 are high. Since all items in the Table III had a reliability of more than 0.7. The value 0.7 used as a benchmark value for reliability test by others the researchers [20], [21], the scale for these construct were considered to exhibit an acceptable reliability.

TABLE III. RELIABILITY TEST RESULTS

Digital Social Media Cybersecurity Risk Requirement	**Items**	**Cronbach's Alpha Value**	**N**
Confidentiality	18	0.970	33
Integrity	18	0.964	33
Availability	18	0.980	33

Note: Items - Number of variables, N - Total Number of Respondents

C. Results of Cybersecurity Risk Critical Level on Social Media Digital

Three core principles of information security requirements (Confidentiality, Integrity and Availability) were considered in order to measure the critical level of cybersecurity risks for digital social media. This section discusses the critical level of 18 cybersecurity risks for each information security requirement core principle.

1) Confidentiality principle: Critical cybersecurity risk factors in digital social media

The highest mean in Table IV represents the most critical cybersecurity risk affected the data confidentiality in digital social media while the lowest mean represents the least critical. Identity Theft is considered as the most critical cybersecurity risk factors (mean value = 3.97) from the study. Confidentiality of the identity should become a serious concern in digital social media because, any unauthorized access to social media account could cause to other vulnerabilities.

TABLE IV. RESULT: MEAN SCORE RANKING FOR CRITICAL CYBERSECURITY RISKS LEVEL IN DIGITAL SOCIAL MEDIA (CONFIDENTIALITY PRINCIPLE)

Cybersecurity Risk Factors (Number of Cases = 33)	**Confidentiality Criticalness**		
	Mean	***Std. Deviation***	***No. Rank***
Identity Theft*	3.97	1.121	1
Information manipulation*	3.94	1.014	2
Cyber Assault/ Bullying*	3.81	0.859	3
Information Theft	3.75	1.218	4
Privacy Violation	3.66	0.937	5
Cyber Crime	3.63	1.040	6
Phishing Pond	3.63	0.976	6
Cyber Attacks	3.59	0.946	7
Advanced Persistence Threats	3.56	1.045	8
Productivity Loss	3.56	0.840	8
Terrorisms	3.56	0.801	8
Espionage	3.53	1.016	9
Insider	3.50	1.047	10
Transactional	3.50	0.880	10
Risk of Losing the Legal Battle	3.50	0.762	10
Corporate Espionage	3.50	0.803	10
Viruses and Malware	3.44	1.014	11
Attack of the Software	3.34	1.004	12

The second critical cybersecurity risk factors was Information manipulation (mean value = 3.94). This risk factor is caused by unauthorized access to user account digital social media. When the unauthorized users access the system, they are able to manipulate the information associated with the account.

The third critical cybersecurity risk factors was cyber assault/ bullying (mean value = 3.81). Cyber assault/ bullying normally happen when an attacker able to access, analyze most of the confidential personal data and reformulate the meaning of the data and execute the attack.

Conversely, the least critical cybersecurity risk factors of the study is determined by the lowest min score value. Data analysis results discover mean value, 3.34 for Attack of the Software is considered as least critical cybersecurity risks on confidentiality issues in digital social media.

2) Integrity principle: Critical cybersecurity risk factors in digital social media

The highest mean in Table V represents the most critical cybersecurity risk affected the data integrity in digital social media while the lowest mean represents the least critical. Cyber Assault/ Bullying is considered as the most critical cybersecurity risk factors (mean value = 3.81) from the study. Cyber Assault/ Bullying perpetrated by an intentional threat source that attempt to alter its data or its operations in personal digital social media account. This active attack could affect the integrity of the victim profile information and post information for their account. For more extreme cases, this cybersecurity risk gives serious psychological impact that affected the emotion, behavior, safety and security of the victim.

TABLE V. RESULT: MEAN SCORE RANKING FOR CRITICAL CYBERSECURITY RISKS LEVEL IN DIGITAL SOCIAL MEDIA (INTEGRITY PRINCIPLE)

Cybersecurity Risk Factors (Number of Cases = 33)	Integrity Criticalness		
	Mean	*Std. Deviation*	*No. Rank*
Cyber Assault/ Bullying*	3.81	0.693	1
Identity Theft*	3.78	0.870	2
Information manipulation*	3.78	0.806	2
Information Theft*	3.78	1.008	2
Espionage*	3.72	0.772	3
Privacy Violation	3.69	0.693	4
Advanced Persistence Threats	3.66	0.701	5
Cyber Crime	3.63	0.833	6
Insider	3.63	0.751	6
Corporate Espionage	3.56	0.670	7
Cyber Attacks	3.56	0.759	7
Productivity Loss	3.56	1.047	7
Transactional	3.53	0.803	8
Risk of Losing the Legal Battle	3.53	0.842	8
Phishing Pond	3.53	0.915	8
Terrorisms	3.44	0.759	9
Viruses and Malware	3.38	0.870	10
Attack of the Software	3.31	0.859	11

The second critical cybersecurity risk factors were Identity Theft, Information Manipulation and Information Theft (mean value = 3.78). The risk of Identity Theft and Information Theft might jeopardize the integrity of data owned by digital social media users. For any computerized system, including digital social media, users can be recognized through identity. If the identity was stolen, the thief will pretend as he/his is the owner of the particular online social media account. This will give an opportunity to unauthorized data modification through undetected manner. Meanwhile, an Information Manipulation risk contributes to the lack of data/information integrity in digital social media.

The third critical cybersecurity risk factors was espionage (mean value = 3.72). Espionage is the act of an individual who obtaining information considered as secret or confidential without the permission of the holder of the information. Espionage was considered as the most effective ways to gather data and information about enemy through the pool of information available in digital social media platform for the entire network of digital social media.

On the contrary, the results of the study also showed that the most least critical cybersecurity risk factors on integrity issues were also Attack of the Software.

3) Availability principle: Critical cybersecurity risk factors in digital social media

The highest mean in Table VI represents the most critical cybersecurity risk affected the data availability in digital social media while the lowest mean represents the least critical. Looking into available principle in digital social media, Privacy Violation is considered as the most critical cybersecurity risk factors (mean value = 3.81) from the study. When users' personal data and information are widely available for public views and disseminate through digital social media without careful control, it could lead to critical risk of privacy violation due to personal-profile data leakage. Personal-profile data such as chat logs and photos were the source of information for personal privacy violation.

TABLE VI. RESULT: MEAN SCORE RANKING FOR CRITICAL CYBERSECURITY RISKS LEVEL IN DIGITAL SOCIAL MEDIA (AVAILABILITY PRINCIPLE)

Cybersecurity Risk Factors (Number of Cases = 33)	Availability Criticalness		
	Mean	*Std. Deviation*	*No. Rank*
Privacy Violation*	3.81	0.931	1
Information Theft*	3.78	1.039	2
Identity Theft*	3.75	1.047	3
Cyber Assault/ Bullying*	3.75	0.9158	3
Information manipulation	3.72	1.023	4
Cyber Attacks	3.71	0.924	5
Espionage	3.69	0.820	6
Transactional	3.66	0.901	7
Corporate Espionage	3.65	0.937	8
Attack of the Software	3.63	0.975	9
Productivity Loss	3.62	0.870	10
Cyber Crime	3.62	0.942	10
Advanced Persistence Threats	3.59	0.837	11
Insider	3.59	0.910	11
Terrorisms	3.56	0.981	12
Phishing Pond	3.56	1.045	12
Risk of Losing the Legal Battle	3.50	0.983	13
Viruses and Malware	3.50	1.016	13

The second critical cybersecurity risk factors was Information theft (mean value = 3.78). When the Personal-profile data were easily available through digital social media, the possibility of information theft is higher. Social Engineering skills are needed in most of the information theft activities in digital social media. Therefore, cyber community should be aware for any suspicions individual questions, wall statement, and

message posted in digital social media. It could be an attempt for Information theft activities.

The third critical cybersecurity risk factors was Identity Theft and cyber assault/ bullying (mean value = 3.75). There are several reasons why identity theft and cyber assault/bullying become a serious concern in digital social media. Reconstruction of the piece or a fraction of the information available in digital social media allows the attacker to commit launch identity theft and cyber assault/bullying either intentionally or unintentionally purpose. Cyber assault/ bullying normally happen when an attacker able to access, analyze most of the available personal-profile data and reformulate the meaning of the data and execute the attack.

In terms of critical cybersecurity risks on available principle, the least critical cybersecurity risk factors is the Risk of Losing the Legal Battle. The information shared in digital social media was inconsistent and intentionally was manipulated which lead to inaccurate perception and judgment.

4) Analysis summary results: The most critical cybersecurity risk on information security requirement for digital social media

Analysis results in Table VII summarize the top 6 most critical cybersecurity risks on confidentiality, integrity and availability of the information in digital social media. The results of the findings able to quantify the criticalness of cybersecurity risk, therefore an appropriate planning for the risk control could be implemented more effectively.

TABLE VII. RESULT: MEAN SCORE RANKING FOR THE MOST CRITICAL SOCIAL MEDIA CYBERSECURITY RISKS ON INFORMATION SECURITY REQUIREMENT

Cybersecurity Risk Factors (Number of Cases = 33)	**Criticalness Level**					
	Confidentiality		**Integrity**		**Availability**	
	Mean	***Rank***	**Mean**	**Rank**	**Mean**	**Rank**
Identity Theft*	3.97	1	3.78	2	3.75	3
Information manipulation*	3.94	2	3.78	2	3.72	4
Cyber Assault/ Bullying*	3.81	3	3.81	1	3.75	3
Information Theft*	3.75	4	3.78	2	3.78	2
Espionage*	3.53	9	3.72	3	3.69	6
Privacy Violation*	3.66	5	3.69	4	3.81	1

As shown in the Table VII, high critical digital social media cybersecurity risk factors against three core principles of information security requirement discovered through this study. Top 6 cybersecurity risks, such as Identity Theft; Information Manipulation; Cyber Assault/ Bullying; Information Theft; Espionage; and Privacy Violation were identified and quantified through a systematic approach. But then, the criticalness of the cybersecurity risks is determined by mean score for each information security requirement core principle were differently interpreted. The study highlight, the most critical cybersecurity risks on confidentiality is Identity Theft. Then, the most critical cybersecurity risks on integrity principle is Cyber Assault/ Bullying. Meanwhile, the most critical cybersecurity risk on availability core principles is Privacy Violation. Thus, cyber community, especially digital social media users should be alert on these critical cybersecurity risk that could influence their digital culture lifestyle.

VI. CONCLUSION

Besides the benefits gained from digital social media as an effective platform for communication and online marketing tool among cyber community, there are still potential risks need to consider. Serious consideration of the cybersecurity risk factors is needed in order to ensure safety and security of digital social media users. Eventually, the findings possibly will provide significant empirical evidence of critical cybersecurity risk factors arise in the digital social media platform.

The findings show that similar cybersecurity risk factors extracted from previous literature also exist in digital social media. However the criticalness of these factors were differently interpreted and discussed. For the confidentiality issue, Identity Theft is considered as the most critical. From the integrity perspective, Cyber Assault/ Bullying considered the most critical cybersecurity risk. Meanwhile, from the availability aspect, Privacy Violation considered as the most critical.

Furthermore, these findings give some significant contributions towards implementing the best practices in digital social media interaction and user account activities. An Empirical evidence from the analysis gives an indicator for more cybersecurity awareness programs to cyber community, practitioners and cybersecurity professional or expert on the critical cybersecurity risks that commonly arise in digital social media. These significant findings could be useful for them to plan an appropriate effort to manage, control and mitigate the cybersecurity risks effectively through several strategic approaches. Finally, they could get optimum benefit from the usage of digital social media in their digital social lifestyle.

ACKNOWLEDGMENT

The authors wish to thank Cybersecuirty Malaysia and their team of researcher who inspire me to extend the study. Thanks to Ministry of Higher Education (MOHE) for their financial support through the Research Articulation Grant Scheme (RAGS) and to all respondents who had participated in the study.

REFERENCES

[1] R. Carpinella, "Cybersecurity and social media," in *Cybersecurity in Our Digital Lives*, J. LeClair and G. Keeley, Eds., Hudson Whitman/Excelsior College Press, 2015, ch. 3.

[2] P. R. Scott and J. M. Jacka, *Auditing Social Media: A Governance and Risk Guide*, Wiley, 2011.

[3] "Merriam-Webster dictionary," Social Media, 6 February 2016.

[4] G. Hinson, "Top information security risk for 2008: Information security risk," in *Proc. CISSP Forum*, 2008, pp. 2-5.

[5] Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary, ISO/IEC 27000:2009 (E).

[6] Cybersecurity definition. [Online]. Available: http://whatis.techtarget.com/definition/cybersecurity
[7] M. Gasser, *Building a Secure Computer System (PDF)*, Van Nostrand Reinhold, 1988, p. 3.
[8] *Best Practices in Social Networking Sites*, Cyber Security Malaysia, 2011
[9] Oxford English Dictionary Online, Oxford University Press, September 2007.
[10] Cyber warfare and the crime of aggression: The need for individual accountability on tomorrow's battlefield. [Online]. Available: https://Law.duke.edu
[11] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., Indianapolis, IN: Wiley, 2008, ch. 3, p. 1040.
[12] V. Greavu-Şerban and O. Şerban, "Social engineering a general approach," *Informatica Economica Journal*, vol. 18, no. 2, 2014.
[13] R. Willison, "Understanding the perpetration of employee computer crime in the organisational context," *Information and Organisation*, vol. 16, no. 4, pp. 304-324, 2006.
[14] R. Moore, *Cyber Crime: Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing, 2005.
[15] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.
[16] J. Blitz, "Security: A huge challenge from China, Russia and organized crime," *Financial Times*, 1 November 2011.
[17] M. Clayton, "The new cyber arms race," *Christian Science Monitor*, 2011.
[18] Wikipedia, The free encyclopedia. (2016). Social Engineering. [Online]. Available: http://en.wikipedia.org
[19] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu, "Reverse social engineering attacks in online social networks," in *Proc. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2011.
[20] N. N. Rahim, N. Z. Khidzir, A. M. Yusof, and K. A. M. Daud, "Towards a conceptual framework of animated infographics in an islamic context," in *Proc. 1st International Islamic Heritage Conf.*, 2015, pp. 38-48.
[21] N. Z. Khidzir, N. H. Arshad, and A. Mohamed, "Information security risk factors: Critical threats and vulnerabilities in ICT outsourcing," in *Proc. International Conf. on Information Retrieval and Knowledge Management*, 2010, pp. 194-199.

Dr. Nik Zulkarnaen Khidzir, Senior Lecturer Faculty of Creative Technology and Heritage; research fellow at Global Entrepreneurship Research and Innovation Centre, UMK, Universiti Malaysia Kelantan has been involved in ICT industry for the past 15 years. He graduated in Computer Science Degree and Diploma Specialize in Software Engineering. Master's degree specialized in Information Privacy and ICT Strategic Planning. His PhD in Information Security Risk Management provide him a skill for research and consultation works.

His research interests are Software Engineering, Cybersecurity Risks, Information Security Risk Management, Business and Education Computing/e-commerce and Creative Computing. Throughout his years of experiences in industry, he also involved in telecommunications, digital Multimedia content development, and System Integrator and ICT solution provider as System Analyst, Database Administrator, Certified Software Tester, Software Designer, Assistant Project Manager (ICT-related project). Also involved in research and consultation as well as training program development for academia and industry. He actively involved in organizing local and international conferences. Also become as proceeding conference and journal reviewer local and international. Pertaining his research interest and contribution to the body of knowledge, he has published several articles in indexed proceedings and journals. He is a member of the IACSIT, IEEE and PECAMP.

Dr. Khairul Azhar Bin Mat Daud, Senior Lecturer, was awarded a Bachelor of Mechanical Engineering (Manufacturing) with Honor in 1998. Prior to his education, he worked at several manufacturing companies such as Artwright (M) Technology Sdn. Bhd, Automation Engineer Sdn. Bhd, Johnson & Johnson Sdn. Bhd and Sony (M) Sdn. Bhd.

Former lecturer in Automotive Engineering and Manufacturing Engineering. He continued his education at Masters level (UTM) and PhD (USM) in Education and Educational Technology. He has developed a self -directed learning system called E-Student Oriented Learning Management System (E-SOLMS) for Politeknik Malaysia.

He has studied the multimedia application systems and their impact on society and humanity. He joined University of Malaysia Kelantan as a senior lecturer and former in the Faculty of Creative Technology and heritage (FTKW). Currently, he's working with research in the field of product design and multimedia. He thought a several courses in product design and multimedia such as digital design, technical drawings, research methodology, final project, research and Student in Enterprise Program (SIEP).

Dr. Mohd Asrul Hery is currently a Senior Lecturer at Universiti Malaysia Kelantan (UMK) Campus Kota, Malaysia since 2014. He was first appointed as a lecturer at Infrastructure University Kuala Lumpur (IUKL) since 2010. He graduated in Financial Mathematics Degree and Master's degree (MSc. IT) Specialized in Applied Mathematics (Optimization). Now, he is further his pH. D's studies at Universiti Sultan Signal Abidin in 2012 specialize in optimization, specifically the quasi-Newton methods. To date, he involves with many research project in Optimization and social education which is funding by IUKL. Pertaining his research interest and contribution to the body of knowledge, he has published several articles in indexed proceedings and journals. Also become as journal reviewer for British journal of Mathematics and Computer Science. He is member of Malaysian Mathematical Sciences (PERSAMA).

Assoc. Prof. Ir. Dr. Ahmad Rasdan Ismail is currently an academician at Universiti Malaysia Kelantan (UMK) Bachok Campus. He graduated his PhD in Mechanical Engineering (Industrial Ergonomics), Master of Science in Manufacturing Systems Engineering and a Bachelor Degree in Mechanical Engineering from Universiti Kebangsaan Malaysia. Currently, he is a Head of Occupational Safety Health Environment Management Unit Registrar Office of Universiti Malaysia Kelantan. His research interest in the area of ergonomics, human factor and safety. He has been a principal consultant and project leader for many private and government projects from multinational oil and gas companies for many years.

He had translated his research finding in 105 international and local journals and 188 proceedings conferences and managed to publish 1 book as main author, 4 books (as the Editor) as well as 5 chapters in distinguish ergonomics books which were published by Taylor and Francis, CRC. So far he has published more than 200 scientific papers in his field of interest including international scholarly journals and conferences. According to the google scholar, Dr Ahmad Rasdan Ismail's articles have been cited exceeding 374, H index at 10 and i10-index 7.

Mohamad Shahfik Afendi Bin Abdul Ghani, Lecturer at Universiti Malaysia Kelantan (UMK) under Department of Multimedia. He is a graduate of Brunel University London with an MSc. In Advanced Multimedia Design and 3D Technologies. He was previously at Universiti Putra Malaysia where he studied Indusial Design. He has been involved in Academic profession since 2014 and engage with the research grants. He has experience in 3D Technologies, 3D Visualisation, Computer Generated Imagery (CGI), and Stereoscopic and Anaglyph Film. He also participated in few external research grants as a member since him joining the UMK. His ongoing research grant is Augmented Reality- Traditional Houses, focusing on augmented technology application and heritage building as the materials.

His passion is to explore the technology in multimedia and film industries and to develop new strategies and pipelines to enhance the Malaysia multimedia and film potentials to the world level. Shahfik's current goal is to become an academics in Multimedia that can contribute to the industries need and involve with the consultation to improve Malaysia Creative industries.