Chapter 21
Information Security Requirement: The Relationship Between Cybersecurity Risk Confidentiality, Integrity and Availability in Digital Social Media

Nik Zulkarnaen Khidzir, Khairul Azhar Mat Daud, Ahmad Rasdan Ismail, Mohd. Shahfik Affendi Abd. Ghani and Mohd. Asrul Hery Ibrahim

Abstract Digital Social Media as a part of the eco-system in today's global cyberspace business environment. It provides an excellent communication and marketing channel for knowledge societies in the world. The popularity of Digital Social Media has also influenced the personal lifestyle and encouraged the digital culture development among cyber community around the globe. Unfortunately, sharing their ideas, activities, statuses, and real-time location could cause them to several critical cybersecurity risks. These categories of risk caused severe impacts to the entire cyber community eco-system associated in digital social media that need to be managed and mitigated seriously. Recent empirical findings underlined the core information security requirement (confidentiality, integrity, and availability) contributes to the severity level of cybersecurity risks in digital social media.

N. Z. Khidzir (✉) · K. A. Mat Daud · A. R. Ismail · Mohd.S. A. Abd. Ghani
Faculty of Creative Technology and Heritage, Universiti Malaysia Kelantan, Kelantan, Malaysia
e-mail: zulkarnaen.k@umk.edu.my

K. A. Mat Daud
e-mail: azhar.md@umk.edu.my

A. R. Ismail
e-mail: rasdan@umk.edu.my

N. Z. Khidzir
Pusat Komputeran dan Informatik,
Universiti Malaysia Kelantan, Kelantan, Malaysia

N. Z. Khidzir
Global Entrepreneurship Research and Innovation Centre,
Universiti Malaysia Kelantan, Kelantan, Malaysia

Mohd.A. H. Ibrahim
Faculty of Entrepreneurship and Business,
Universiti Malaysia Kelantan, Pengkalan Chepa, Kelantan, Malaysia
e-mail: hery.i@umk.edu.my

N. A. Yacob et al. (eds.), *Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016)*,
https://doi.org/10.1007/978-981-13-0074-5_21

Therefore, the aim of this study is to determine the relationship between cybersecurity risks confidentiality, integrity, and availability in Digital Social Media. Questionnaires were distributed to the various active cyber communities and knowledge societies. The results of the mean score indicate that, more cybersecurity awareness program should be implemented in digital knowledge societies. Furthermore, the results of the correlation coefficient (r) values between >0.4 and <0.7 verifies that a moderate positive relationship exists between cybersecurity risks, confidentiality, integrity, and availability of information in Digital Social Media. Findings reveal that the highest moderate cybersecurity risk relationship between integrity and availability. This empirical evidence indicates how the core information security requirement influences each other's on the cybersecurity risk severity. Through the findings, cyber communities and knowledge societies would be able to determine the direction and strength of the relationship among information security requirement and plan the appropriate cybersecurity awareness program to Digital Social Media users as a preventive approach to mitigate critical cybersecurity risks.

Keywords Cybersecurity risk · Digital social media · Human factor
Information security requirement · Social engineering

1 Introduction

Digital Social Media provides an excellent communication platform through uncountable application such as online forums, chatting channels, video streamings, blogs, etc. Unfortunately, digital social media could enable threats and vulnerabilities that lead to cybersecurity risks to the cyber communities and organizations. Thus, it is crucial to manage the confidentiality and integrity of information in Digital Social Media. To this end, the relationship between confidentiality and integrity security requirements were measured and analyzed. The empirical findings point to the significant relationship between information confidentiality, integrity and availability in digital social media. This suggests that organizations should carefully determine and evaluate cybersecurity risks' confidentiality and integrity in their mitigation plan.

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 (Jacka and Scott 2011). 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" (Jacka and Scott 2011).

Cybersecurity is beyond securing a perimeter the individual digital or virtual assets (Carpinella 2015). It entails a comprehensive understanding of every element that might enable penetration, interaction and compromise, and that could lead to catastrophic events or risks. Cybersecurity is becoming increasingly important as

more information and technology are being uploaded into cyberspace. This has led to new terms such as cyberwarfare, cybercrime, and cyberterrorism.

Digital Social Media is gaining fast popularity among Internet users globally. Unfortunately, Digital Social Media could become the main information sources from most of the social engineers to harvest required data and information to plan cyberattacks. The larger possibility of cybersecurity risks happening could cause serious impacts to the organization and cyber community, such Phishing Ponds, Privacy Violation, Risk of Losing the legal battle, Corporate Espionage, Viruses and Malware, Productivity Loss (Social Networking Sites 2011). Cybersecurity risks are currently becoming serious issues in digital social media due to the increasing number of social media population globally. Cybersecurity risks are caused by common risk factors, which are threats and vulnerabilities of information in social media. Social media allows social engineer to use the psychological manipulation of people into performing actions of confidential information for the purpose of information gathering, fraud, or system access (Anderson 2008; Valerică and Oana 2014; Wikipedia 2016a, b). Digital Social Media becomes the source of information for social engineer to capture and harvest useful information for the purpose of the cyberattack.

Information Security Requirements adopted the core principles of information confidentiality, integrity and availability (Vorster and Labuschagne 2005; Parker 2002; Wikipedia 2016a, b) and broadly used in various fields of studies (Khidzir et al. 2010). Confidentiality refers to the limitations on the use and retention of different kinds of information (Vorster and Labuschagne 2005; Parker 2002; Code of Practice for Information Security Management 2005; Canal 2005). Integrity is the guarantee that information has not been manipulated (Vorster and Labuschagne 2005; Parker 2002; Code of Practice for Information Security Management 2005; Canal 2005) while availability is ensuring that authorized users have access to information and associated assets when required (Vorster and Labuschagne 2005; Parker 2002; Code of Practice for Information Security Management 2005; Canal 2005). Information in Digital Social Media might be improperly disclosed due to its confidentiality being exposed, modified in an inappropriate way, if its integrity is jeopardized, and destroyed or lost because its availability is threatened (Blakley et al. 2001).

Therefore, for the purpose of this study, the exploration focused on investigating the relationship of information security requirement between information confidentiality, integrity and availability in Digital Social Media. The results were measured and statistically analyzed to investigate the relationship between them.

2 Methodology

An empirical study was conducted to determine the relationship between confidentiality, integrity and availability of cybersecurity risk in Digital Social Media. Five-Point Likert-Scale was used to measure the severity level of online social media cybersecurity risks. Primary data were collected using questionnaires as the

data collection tool for the study. Analysis of primary data was supported by the application of appropriate statistical techniques such mean score analysis and Bivariate Pearson Correlation test.

3 Research Model

A research model illustrated in Fig. 1 was developed focusing on the confidentiality, integrity and availability core component which has contributed to cybersecurity risk in digital social media.

Based from a research model in Fig. 1, three hypotheses have been developed to test the relationship between each core element of information security requirements, confidentiality, integrity and availability levels. The hypotheses are

H1 There is a positive relationship between confidentiality and integrity for cybersecurity risk in Digital Social Media.
H2 There is a positive relationship between confidentiality and availability for cybersecurity risk in Digital Social Media.
H3 There is a positive relationship between integrity and availability for cybersecurity risk in Digital Social Media.

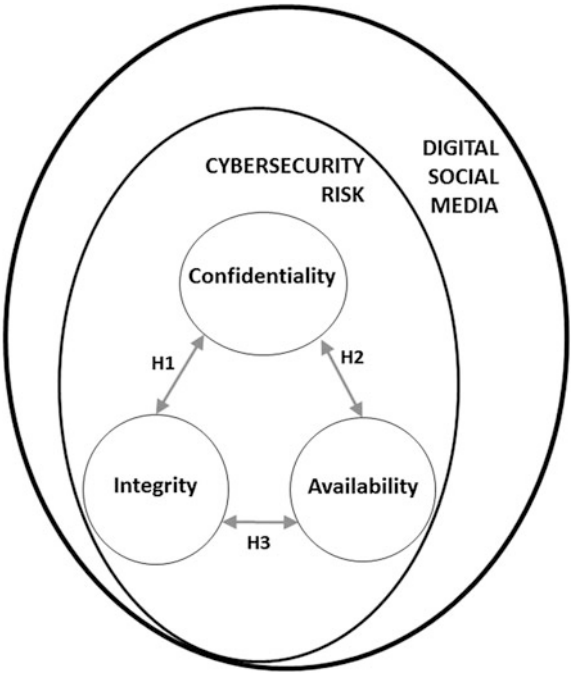

Fig. 1 Research model for relationship between cybersecurity risk on confidentiality, integrity and availability in digital social media

4 Results and Analysis

There are three sections discussing the results and analysis of demographic profiles and information security risk mean score for each core component information security requirement.

4.1 Demographic Profiles and Analysis

Respondents' demographic profiles examined were respondents' 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 shows that most of the respondents were considered as appropriate professionals that possess sufficient experience to respond to the entire question trustfully and accurately. Table 1 summarized the demographic profiles of respondents involved in the study.

In terms of respondents' years of ICT Security Experiences, majority of 42.4% had experience between 1–3 years. Only 15.2% respondents had ICT Security Experience between 4–6 years. About 21.2% of those had less than 1 year as well as more than 6 years' experience.

4.2 Information Security Requirement Mean Score Analysis (Confidentiality, Integrity, Availability)

Information security requirement (Confidentiality, Integrity and Availability) mean score for cybersecurity risk in Digital Social Media were measured to determine each severity level.

As summarized in Table 2, the highest mean score on availability (3.6510) of information in Digital Social Media indicates most of the cyber community alert on the availability aspect towards the cybersecurity risk severity level. The highest mean score of availability signifies the respondents really care about the availability aspects. The second highest mean score on confidentiality (3.6094) of information indicates the level of cyber community awareness on the confidentiality issues in Digital Social Media. Therefore, the confidentiality issues awareness among cyber community could also significant to severity level of cybersecurity risk. The results prove that integrity (3.6042) of information stored, processed, and transferred through Digital Social Media platform is also given an attention among cyber communities. They also realize that the integrity of information should give priority in managing the cybersecurity risk impact.

Table 1 Demographic analysis

Respondent's gender	Percentage (%)
Male	54.5
Female	42.4
Respondent's age	Percentage (%)
>50 years	9.1
46–50 years	6.1
41–45 years	18.2
36–40 years	18.2
31–35 years	24.2
26–30 years	21.2
Years of working experience	Percentage (%)
>20 years	18.2
15–20 years	33.3
11–14 years	6.1
6–10 years	15.2
<= 5 years	27.2
Years of ICT security experience	Percentage (%)
>6 years	21.2
4–6 years	15.2
1–3 years	42.4
<1 year	21.2
Organizational sectors	Percentage (%)
Private company	6.1
Government agencies	84.9
Government-link-company (GLC)	9.1
Industrial cluster	Percentage (%)
Healthcare private	6.0
Healthcare government	3.0
Creative technology	6.0
Higher education	69.7
Information communication technology	6.0
Services	9.1

4.3 Analysis of Relationship between Confidentiality, Integrity and Availability in Digital Social Media

The Bivariate Pearson Correlation test was then conducted on the formulated research hypotheses to determine the significant relationship, strength, and direction between three core component of information security requirement (confidentiality, integrity and availability). The correlation coefficient values, (r) were derived to explain the relationship strength between them. A result of p-value <0.01 is

Table 2 Mean score cybersecurity risk confidentiality, integrity and availability

Information security requirement	Digital social media cybersecurity risk severity		
	Mean	Std. Dev.	N
Confidentiality	3.6094	0.78713	32
Integrity	3.6042	0.63700	32
Availability	3.6510	0.79239	32

considered significant. A weak relationship is indicated by a (r) value of less than 0.4, values between 0.4 and 0.7 indicate moderate relationship and a strong relationship has a value higher than 0.7.

5 Discussion

The analysis of mean score results discovers the empirical evidence on how the cyber communities concerned on the core element of information security requirement in Digital Social Media that could cause the cybersecurity risks. Generally, the mean score results demonstrate the moderate level of cyber communities concerned on the confidentiality, integrity and availability of information when using Digital Social Media. Therefore, cybersecurity awareness program should be in place to educate cyber communities how to use, communicate and interact through Digital Social Media in order to minimize the frequency of cybersecurity incident and mitigate the associated risks more effectively.

A specific target group and generation gap for cybersecurity awareness program also being identified based on the demographic analysis results for more effective outcome of the program. Specific awareness content focuses on information security requirement and cybersecurity risks issues also being identified through the findings.

As revealed in Table 3, the results of the hypothesis tests indicate positive correlations for the three hypotheses. H1, H2, and H3 were accepted and the null was rejected based on significant *p-value* < 0.001. The correlation coefficient (r) values were 0.627 for H1, 0.591 for H2, and 0.631 for H3. All the significant

Table 3 Hypotheses test results for the significant relationship between cybersecurity risk confidentiality, integrity and availability

Hyp.	Correlation coefficient (r)	Sig. (p-value)	Decision	Results
H1	0.627	0.000*	Significant	Moderate +ve
H2	0.591	0.000*	Significant	Moderate +ve
H3	0.631	0.000*	Significant	Moderate +ve

hypotheses described moderate relationship strength among information security requirement (Confidentiality, Integrity and Availability) in Digital Social Media.

The strongest moderate positive relationship level integrity and availability of information will cause the cybersecurity risk in Digital Social Media. Thus, the level of moderate influences between integrity and availability of information in Digital Social Media. Information integrity does not influence much to the information availability that could cause the cybersecurity risk in Digital Social Media. Meanwhile, the weakest moderate relationship was between information confidentiality and availability for cybersecurity risk in Digital Social Media. Last but not least, the others moderate positive relationship between confidentiality and integrity for cybersecurity risk in Digital Social Media.

The moderate level of relationships among three core elements of information security requirement stored, transferred, and shared in Digital Social Media still contributes to the cybersecurity risks incident that could cause a catastrophic impact to human and the entire structure of cyberspace.

6 Conclusion

This study has empirically established the significant relationship between confidentiality, integrity and availability of information in Digital Social Media private and public agencies in Malaysia. However, the moderate level of relationship influences between each of information security requirement contributed to the cybersecurity risks incident in Digital Social Media. Other findings explore the level of cybersecurity risk awareness among cyber communities. The empirical evidences show the need the comprehensive cybersecurity risk awareness program for digital societies. By identifying the relationship between these cores component of information security requirement will assist the technologist, cybersecurity expert, and practitioners to mitigate the possible impact of the risk. Additionally, cyber community will gain the full benefit from Digital Social Media platform.

Acknowledgements This work was supported in part by Malaysian Ministry of Higher Education under RAGS Grant. Special thanks also to Faculty of Creative Technology and Heritage; Universiti Malaysia Kelantan; and Global Entrepreneurships Research and Innovation Centre (GERIC) for facilities support for this research.

References

Anderson J (2008) Security engineering: a guide to building dependable distributed systems, 2nd edn. Wiley, Indianapolis, IN, p 1040. ISBN 978–0-470-06852-6. Chapter 2, p 17

Blakley B, McDermott E, Geer D (2001) Information security is information risk management. In: Proceedings of the 2001 workshop on new security paradigms (NSPW'01), pp 97–104

Canal VA (2005) The global voice of information security: on information security paradigms. ISSA J

Carpinella R (2015) Cybersecurity and social media. In: LeClair J, Keeley G (eds) Cybersecurity in our digital lives. Hudson Whitman, pp 57–72

Code of Practice for Information Security Management (2005) ISO17799:2005, ISO Standard

Jacka JM, Scott PR (2011) Auditing social media: A governance and risk guide. Wiley, Hoboken

Khidzir NZ, Mohamed A, Arshad NH (2010) Critical information asset security requirements in ICT outsourcing. In: Proceedings of International IT and society conference, vol 1, No. 1. pp 88–95

Parker DB (2002) In: Bosworth S, Kabey ME (eds) Toward a new framework for information security, computer security handbook, 4th edn. Wiley, New York

Social Networking Sites (2011) Cyber security Malaysia. http://www.cybersecurity.my/data/content_files/11/918.pdf

Valerică GS, Oana S (2014) Social engineering a general approach. Informatica Economică 18 (2):5–13

Vorster A, Labuschagne L (2005) A framework comparing different information security risk analysis methodology. In: Proceedings of the South African Institute of Computer Scientist and Information Technologist on IT research in developing countries, pp 95–103

Wikipedia (2016) The free encyclopedia, social engineering. Retrieved from http://en.wikipedia.org. Accessed 6 Feb 2016

Wikipedia (2016) The free encyclopedia (May 2016). Information security: basic principles, key concepts. Retrieved from http://www.wikipedia.org