Electronic Word-of-Mouth (EWOM) Adoption Model for Information Security Awareness: A Case Study in University Students

Adhi Prasetio[1], Puspita Kencana Sari[2], Dian Puteri Ramadhani[3]
Faculty of Economic and Business
Telkom University
Bandung, Indonesia
[1]adhipras@gmail.com, [2]puspitakencana@telkomuniversity.ac.id, [3]dianrdn003@gmail.com

Abstract

In the social media era, relationship and interaction of a person with other people give bigger influence on the mind-set and action. Electronic Word-of-mouth (eWOM) is considered as an effective way to buildbrand awareness in marketing communication. Many tools and techniques, can be used to improve information security awareness, in order to jointly maintain information security within organization. This study aims to formulate an electronic Word of Mouth (eWOM) usage model in to build information security awareness through social media. eWOM is expected to complement the existing techniques in building information security awareness. Methodology used is quantitative with data analysis techniques using PLS-SEM. This research took 100 university students as respondent for a preleminary study. The result showed that source credibility and costumer experience significantly effect eWOM credibility. Meanwhile, eWOM credibility significantly effect eWOM adoption. Finally, eWOM adoption significantly effect Security Awareness.

Keywords: Electronic Word of Mouth, Information Securiy Awareness, Social Media

1. Introduction

By current technological developments, potential threats to information security is getting higher. Information not only becomes an important asset to the company, but also for individuals. Therefore, not only the organizations or companies that need to protect information, but every people must be able to protect the data and information they have. Each individual must maintain confidentiality, authenticity, integrity, and availability of data and information they need to perform the work or daily living activities.

Many cases of information security breaches affecting individual, such as hackers, identity theft, malware attacks (such as viruses, worms, Trojan horse), and the information devices theft (such as mobile phones and laptops). A Facebook account i.e., Cyber Crime released fake accounts on Facebook (on 11 September 2015), which are used by people who are not responsible for committing fraud against others. The actors use the other people photos and identities that have taken from someone's personal account to get acquainted with others. Through the fake account they usually ask for some money to the target by pretending as the unfortunate that require substantial funds. This technique known as Social Engineering. The increase of smartphone users makes this device becomes one of the hackers attacks target. Indonesia is still vulnerable to mobile malware attacks. Statista (2015) indicate that Indonesia included in one of top 10 countries attacked by mobile malware with nearly 11% of smartphone users in Indonesia experienced in mobile malware attacks.

The use of social media that is massively increasing, enabling people to obtain and disseminate information. Social media users can disseminate information related to their personal experiences from their own experience or other people they know, and even information they obtain from websites and other blogs. However, not all social media circulated valid information and trusted by readers. In fact, that information can increase knowledge so they more aware to their personal information security.

Word of Mouth (WOM) as one of the marketing communications modes has an important role in the sales and brand formation (Kotler & Keller, 2012). The use of social media to make WOM in the form of eWOM becoming increasingly important to improve brand awareness. It is already mentioned and demonstrated in various marketing research (Charo, et al.,2015; Jalilvand & Samiei, 2012; Shojaeel & Azman, 2013; Xu & Chan, 2010). In the Charo, et al (2015) research shows how the adoption of online information from Facebook users have an impact on the brand image and the purchase intention. Another research showed that eWOM have a positive correlation with the brand awareness (Shojaeel & Azman, 2013; Xu & Chan, 2010). This can be analogous to the adoption of online information through eWOM by social media users to improve information security awareness and the desire to protect the information they have. In the information security management theory itself, several techniques commonly used to improve information security awareness in the company. However, the use of these techniques have not been tested on improving awareness of security to protect personal information.

The issues that will be discussed in this study include the following items:

1. How eWOM adoption of social media users toward the information regarding information security cases?
2. How eWOM among social media users can influence the level of information security awareness?

To get answers to research questions above, this study will conduct a survey of a number of social media users in Indonesia. The results of this study are expected to contribute to the information security management science field to enrich the tools and techniques that can be used in information security awareness programs. Cyber security becomes a main topic of the Indonesian government, especially the Ministry of Communications and Information Technology (Kurnia, 2015). By searching for an effective way to improve information security awareness in the community is expected to decrease the rate of crime in the virtual world with the information protection independently. The implementation of effective security controls depends on the environment that positively towards safety, where everyone understands and involve in behaviours that are expected of them (Kruger and Kearney, 2006).

2. Literature Review

2.1. Information Security Awareness

Information security is a combination of systems, operations and internal controls to ensure the integrity and confidentiality of the data and operating procedures within an organization (Hong, Et.al., 2003). The purpose of information security is to ensure business continuity and to minimize the loss of business by preventing and minimalize the impact of security incidents (Kruger, et.al., 2010). The information security has three basic components that must be managed, namely (Mitchell, 1999):

a. Confidentiality of sensitive information; protect it from accessed by unauthorized parties
b. Integrity; ensure the accuracy and completeness of information
c. Availability; ensuring that information and vital services are available for users whenever needed.

One of the most important parts of information security management is an information security awareness. Information security awareness is a control or rules designed to reduce the incidence of information security breaches, as a result of negligence or the actions that have been planned (Whittman & Matord, 2011). The primary objective of information security awareness is to ensure that computer users are aware of the risks related to the use of information technology and also an understanding of the policies and procedures (Kruger and Kearney, 2006). This information awareness programs need to be done by the owner of the system as part of the management of information technology. The system owner bears responsibility to provide qualified knowledge about the existence and the general level of control that is used so that all users be sure that the system is secure (Peltier, 2014) .

According to Kruger and Kearney (2006), there are three components that can be used to measure the level of information security awareness, namely “What users know” (Knowledge), “How they feel about the topic” (Attitude), and “What they do” (Behavior).

Several methods can be used to improve information awareness, include: Educational presentation, E-mail

messaging, Group discussions, Newsletter articles, Video games, Computer-based training (CBT), and Posters. From previous studies (Khan, et.al., 2011), it considered that the most effective method is group discussion, which meets all the criteria in measuring the effectiveness of methods of awareness (knowledge component, changes in attitude, subjective norm, intention, and behavioural changes). In that study, group discussion is an informal gathering where there is no one-way communication and each member in the group can take advantage of knowledge and experience exchange (Khan, et.al., 2011). The methods of this character is almost the same by word of mouth in a community where members can exchange information on a such as giving review (knowledge) and testimonials (experience).

2.2. Electronic Word of Mouth (eWOM)

Electronic Word of Mouth (eWOM) appears with the development of computers, internet and social media. EWOM an enhancement of WOM. The existence of internet and social media make eWOM become an important part of corporate communications. Electronic word of mouth (eWOM) refers to any statement which is shared by consumers through the Internet (e.g. web sites, social networks, instant messaging, news feed) about a product, service, brand or company.

eWOM help marketers to reduce advertising costs because any information shared by people who do not have any relationship with the brand owner is considered more reliable because there is no conflict of interest, especially if it is obtained from sources considered credible by the message recipient. This makes a marketing message received through this eWOM more effective than conventional advertising (Jansen et.al., 2009). Integrated marketing communications model by Kotler and Keller (2012) which was further developed by Xu and Chan (2010) showed that eWOM have a direct positive correlation with brand awareness.

According to Fan et al. (2013), eWOM adoption influenced by eWOM credibility that perceived by consumers. Fan et al. (2013) offers a model to measure eWOM credibility that determined by:

a. Source Credibility
b. eWOM Quantity
c. eWOM Quality
d. Consumer Expertise
e. Consumer Involvement

Based on those literature reviews, this research uses the following hypotheses:

H1: Source Credibility increases perceived eWOM Credibility
H2: eWOM Quality increases perceived eWOM Credibility
H3: eWOM Quantity increases perceived eWOM Credibility
H4: Consumer Expertise increases perceived eWOM Credibility
H5: Consumer Involvement increases perceived eWOM Credibility
H6: Perceived eWOM Credibility increases eWOM Adoption
H7: eWOM Adoption increases Information Security Awareness

2.3. Research Framework

This study will adopt the model offered by Fan et.al (2013) to measure eWOM adoption level and Kruger & Kearney (2006) model to measure information security awareness level. The new model that will be examined is correlation between eWOM adoption and information security awareness level. eWOM adoption is influenced by perceived of eWOM credibility that constructed by source credibility, eWOM quantity, eWOM quality, consumer expertise, and consumer involvement (Fan et.al, 2013). Meanwhile, Information security awareness is measured by knowledge, attitude, and behaviour of consumer (Kruger & Kearney, 2006). In this study, consumers are the social media users that will be influenced by adopting the eWOM.

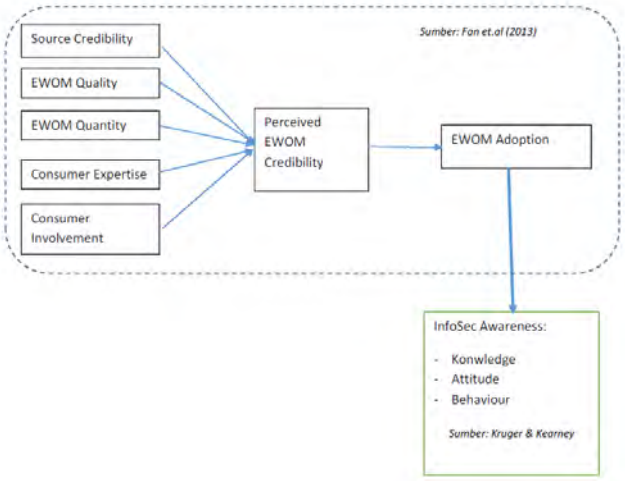

Fig. 1. Research Framework

3. Research Methods

The research method used is quantitative method. Data analysing will be used Partially Structural Equation Modelling Least Square (PLS-SEM) techniques. The operational variables used include:

1. Information Security Awareness (adopted from Kruger & Kearney, 2006); consist of Knowledge, Attitude, and Behavior
2. e-WOM (adopted from Fan et al, 2013); consists of Source Credibility, EWOM Quantity, EWOM Quality, Consumer Expertise, Consumer Involvement, Perceived EWOM Credibility, EWOM Adoption

Data collection will be done by distributing questionnaires to respondents through online media. The population of this study is the social media users, especially university students, who have read or receive information about information security, either a case of threat or protection campaigns. The sampling technique used is nonprobability sampling with targeted sample of about 100 people.

4. Result and Discussion

Responses from 108 students were analysed. Most of them are from several universities in Bandung and Medan. Social media that are used by most of respondents are Instagram and Facebook. 92.6% of respondents ever read post(s) about information security in their social media shared by their friends. 69.4% of respondents sometimes re-share the post to their timeline and 26.9% of them never do that.

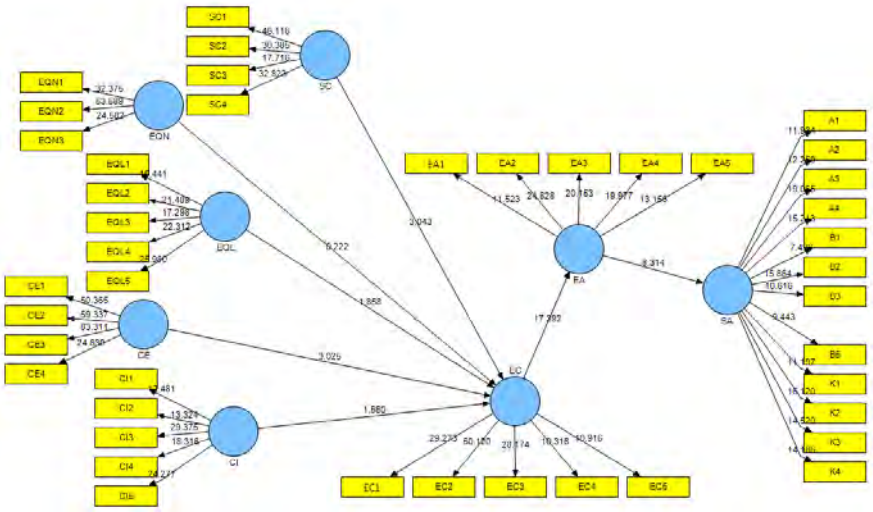

Fig 2. PLS Result for Structural Model

Figure 2 shows the result of structural model (inner model) test that was conducted by observing t-value for each exogenous construct. Table 1 shows the Hypothesis testing results captured from Smart-PLS. The results show that hypotheses H1, H4, H6, and H7 are supported since their t-values are greater than 1.96 (significant at 0.05 level).

Table 1. Hypotesis Testing Results

Hypothesis	t-value	Supported
Source Credibility → eWOM Credibility	**3.043**	**Yes**
eWOM Quality → eWOM Credibility	0.222	No
eWOM Quantity → eWOM Credibility	1.858	No
Customer Expertise → eWOM Credibility	**3.025**	**Yes**
Customer Involvement → eWOM Credibility	1.560	No
eWOM Credibility → eWOM Adoption	**17.392**	**Yes**
eWOM Adoption → Information Security Awareness	**8.314**	**Yes**

Data analysis results showed that two factors affecting eWOM Credibility in the context of information security campaign in social media. Those factors are source credibility and customer expertise. Eventhough its hard to verify the credibility of source in online social media (Fan et.al, 2013), but this result support previous study that source credibility significantly affects eWOM credibility (Fan et.al, 2013). Eventhough Customer expertise could have negative impact on eWOM credibility (Park and Kim, 2008)(Bansal and Voyer, 2000) and found has no significant effect (Fan et.al, 2013), but for students who used to search for information in academic environment, it seems that the more expertise they are the more they perceived eWOM credibility.

On the other side, the other factors such as eWOM Quality, eWOM Quantity and Customer Involvement are not affecting eWOM Credibility. Eventhough eWOM Quality and eWOM Quantity found to have siginificant effect on eWOM credibility (Fan et.al, 2013), and found to have various effect on different hotel categories (Blal & Sturman, 2014), but in this research, both factors found to have no significant effect on eWOM credibility. Customer involvement didn't have significant effect on eWOM credibility, and this result support previous research by Fan et.al (2013).

This research also showed that eWOM credibility increases eWOM adoption supporting Fan et.al (2013) results. Furthermore, eWOM adoption increases Information Security Awareness, as it also increase brand awareness (Shojaee & Azman, 2013). Although security awareness and brand awareness is not same, but from this result we can see that eWOM adoption also significantly impact security awareness.

5. Conclusion

This research showed that only two factors namely source credibility and costumer experience significantly effect eWOM Credibility, while the other three factors eWOM Quantity, eWOM Quality and Customer involvement didn't affect eWOM Credibility. Moreover, eWOM credibility proven to be significantly effect eWOM adoption, and furthermore, eWOM adoption significantly effect Security Awareness. This result can be adopted to develop a new tool to increase information security awareness through social media that involved eWOM adoption. For further research, we suggest to study about impact of eWOM adoption to information security behavior specifically because from previous research (Khan et.al, 2011) indicated that most of information security campaign only effecting knowledge aspect as the basic ladder in security awareness.

References

Bansal, H. S., & Voyer, P. A. (2000). Word-of-mouth processes within a services purchase decision context.Journal of Service Research, 3(2), 166-177.

Blal, I., & Sturman, M. C. (2014). The differential effects of the quality and quantity of online reviews on hotel room sales. Cornell Hospitality Quarterly, 55(4), 365-375.

Charo, et al. (2015) 'Determining the Impact of Ewom on Brand Image and Purchase Intention through Adoption of Online Opinions', *International Journal of Humanities and Management Science (IJHMS)*, Vol. 3 Issue 1, pp.41 – 46

Fan et.al. (2013) 'Establishing the Adoption of Electronic Word of Mouth through Consumers Perceived Credibility', *International Business Research*, Vol. 6 No.3, pp.58 – 65

Hong, Kwo-Shing. et al., (2003) 'An Integrated System Theory of Information Security Management', *Information Management & Computer Security,* Vol. 11 No.5, pp.243 – 248

Jalilvand., M.R, and Samiei, N. (2012) 'The Effect of Electronic Word of Mouth on Brand Image and Purchase Intention: An Empirical Study in the automobile industry in Iran', *Marketing Intelligence & Planning*, Vol. 30 No.4, pp.460 – 476

Jansen, B. J., et.al. (2009) 'Twitter Power: Tweets as Electronic Word of Mouth', *Journal of the American Society for Information Science and Technology*, Vol. 60 No.11, pp.2169 – 2188

Khan, et al. (2011) 'Effectiveness of information security awareness methods based on psychological theories', *African Journal of Business Management*, Vol. 5 No.26, pp.10862 – 10868

Kotler, Philip and Keller, Kevin L. (2012) *Marketing Management*, 14th ed., pp.478. Prentice Hall, New Jersey.

Kruger, Hennie., et al. (2010), 'A vocabulary Test to Assess Information Security Awareness' in *South African Information Security Multi-conference*, Port Elizabeth, South Africa.

Kruger, H.A, Kearney, W.D. (2006), 'A Protoype for Assessing Information Security Awareness', *Elsevier Journal:Computers & Security*, pp.289 – 296

Kurnia, Devi. (2015) 'Ini Rencana Pemerintah Perkuat Keamanan Cyber' *Kominfo* [online] 20 Oktober. http://kominfo.go.id/index.php/content/detail/6255/Ini+Rencana+Pemerintah+Perkuat+Keamanan+Cyber/0/sorotan_media (Accessed 10 January 2015)

Mitchell, Ruth C. et al. (1999) 'Corporate Information Security Management', *New Library World* Vol. 100 No.1150 pp.213 – 227. MCB University Press. London UK ISSN 0307-4803

Park, D., & Kim, S. (2008). The effects of consumer knowledge on message processing of electronic word-of-mouth via online consumer reviews. Electronic Commerce Research and Applications, 7(4),399-410.

Peltier, Thomas R. (2014) *Information Security Fundamentals,* 2nd ed., CRC Press, Boca Raton.

Shojaee, S and Azman, Azreen. (2013) 'An Evaluation of Factors Affecting Brand Awareness in the Context of Social Media in Malaysia', *Asian Social Science*, Vol. 9 No.17, pp.72 – 78

Statista. (2015) 'Top 10 countries attacked by mobile malware in the third quarter of 2015 (share of users attacked)' *Statista* [online]. http://www.statista.com/statistics/325201/countriesshare-of-malicious-attacks-2014/ (Accessed 10 January 2015).

Whitman, Michael E., and Mattord, Herbert J. (2011) *Principles of Information Security*, 4th ed., Cengage Learning, Atlanta.

Xu, Jing Bill and Chan, Andrew. (2010) 'A conceptual framework of hotel experience and customer-based brand equity: Some research questions and implications', *International Journal of Contemporary Hospitality Management*, Vol. 22 No.2, pp.174 – 193