THE IMPACT OF SOCIAL MEDIA FACTORS ON INFORMATION SECURITY COMPLIANCE

[1]RYOWHOA LEE, [2]INHO HWANG, [3]SUNGHO HU

[1]Department of education, Chung-Ang University, Korea
[2]School of Knowledge-Based Management, Chung-Ang University, Korea
[3]Department of Psychology, Chung-Ang University, Korea
E-mail: [1]seachim95@hanmail.net, [2]hwanginho@nate.com, [3]powerrcy@gmail.com

Abstract - The purpose of this study is to verify effectiveness of social media factors on information security compliance. As a result, social media factors has become an important part of integrated marketing. The model divided process of social media marketing into three links which were information sources, information processing and security. In this process, social media marketing, level of information, perceived risk, degree of involvement would influence the user's information security compliance through a complex path. Finally, it found that the root causes of information security were consist of the external area (social media information) and internal area(level of information).

Keywords - Social Media, Information Security, Information Security Compliance, Level of Information, Perceived Risk

I. INTRODUCTION

Almost people are indeed more interested in social media; social media is definitely not only satisfied with the young people for the entertainment and social needs. Using social media that we have instant access to millions of peoples and we have new ways of interaction. We can share our experiences with each other, be updated with our friends' statuses, support them when they need it, and read their statements. Within social networks we can read about people's recommendation on a product we want to buy or on a hotel in which we indent to spend our next holiday. People use social media for different reasons. According to the study "Why People Use Social Media Sites" (2009), 31% of social media users said that they want to get in contact with new people, 21% said that they want to keep in touch with their friends, and 14% mentioned general socializing as their reason[1].

People are becoming more comfortable using the Internet [2]. One common problem on social media web sites is over-sharing whereby people disclose too much information which in the long run might have unintended consequences. With social media people are now sharing information about their exact location, but sharing location-based information just means there is another layer of personal information exposed which may not always be really necessary. If you allow messages between different social networks, what you intended to be private can become public. For example, you might relate your Foursquare location to your public Twitter account and by doing this expose the message to the whole world [3].

Social media include social network services, video (photo) sharing networks, cooperation term network, news sharing network, the contents selection media, and its well-known manifestations are micro-blogging (Twitter, Sina micro-blogging, etc.), social networking (MySpace, Facebook, Kaixin net, Renrennet, etc.), content communities (YouTube, Youku, etc.). The core values of social media is that information was reprocessed and re-dissemination process by internet users, this process is not only created the value by producing new information, but also by integrating and filtering the original information, which makes internet users play a gatekeeper of information.

Now, the development trend of internet dissemination of information is the coexistence of social media and traditional portals, traditional portals still focus on information collection, information processing, information creation, information dissemination, and social media more emphasis to compensate for the lack of traditional portals, focusing on information "interactive" and "personalized".

But, social media is used also by criminals for fraud, gathering business intelligence, stealing sensitive information etc. Social media security risks include [4]: insufficient authentication controls, cross site scripting, cross site request forgery, information leakage, injection flaws, information integrity, and more. The main cyber-attack methods are: Spear Phishing, Social Engineering and Web Application Attacks. Spear Phishing is an attack which targets a specific user or group of users, and attempts to deceive the user into performing an action, such as opening a document or clicking a link, that launches an attack [5].

The use of abbreviated URLs on sites like Twitter makes it easy for cybercriminals to mask and direct users to malicious web sites. Social Engineering, which relies on exploiting the human element of trust [6], obtains or compromises information about an

organization or its computer systems [7]. Social media sites such as Facebook provide the ability for a user to maintain his or her own web page and share content with their personal connections. By breaching the trust user has with his or her online network, hackers are able to embed malware into friends' content and cause yet more people to fall victim to the malicious link [8]. Recent advances in Web Application technologies allow attackers to use new techniques to target users [9].For example, a user may grant a malicious web application access to his or her Facebook account, which may compromise the account or may download unauthorized software to the user's computer.

As long as social media sites share information with other social media sites, location-sharing is allowed and people are becoming comfortable with disclosing such information, then anyone will readily be able to get sensitive information. Combine this with overly enthusiastic users, who intentionally or not, share too much personal information and developers who can access private information, then social media presents a very severe security risk [2].

II. METHOD

2.1. Samples

This investigation began in late July 2017, 728 users sample from Seoul were selected to measure questionnaire. Excluded non-effective questionnaires, 728 copies were valid questionnaires, including the 612 recycled electronic version and 126 recycled paper questionnaires, recovery rate was 99.28%. User samples included 306 males and 422 females, detailed results are shown in Table 1.

Classification		Participants
Gender	Male	306
	Female	422
	Total	728
Educational background	Senior	155
	Junior	180
	Sophomore	232
	Freshman	161
	Total	728

Table 1. Research sample characteristics

2.2. Materials

We needed to use SEM to test the construct validity of the measurement model. We used confirmatory factor analysis to examine the convergent validity and discriminant validity of the latent variable.

In order to test convergent validity, first, scale data was analyzed by confirmatory factor to get the standardized factor loadings; then examine the standardized factor loading coefficient of each indicator variable is greater than 0.5, greater than 0.5 means that the common variance between indicator variables and its potential variables greater than the common variance between the indicator variables and the error variance; the last inspection were average variance extracted (AVE) and the composite reliability, if AVE were greater than 0.5, that means the variance percentage of indicator variables explained by the latent variable is greater than 50%.

Table 2 is the table of convergent validity, each factor loading greater than 0.5, for each latent variable, the AVE were greater than 0.5, the composite reliability of each latent variable were greater than 0.8, convergent validity meet the relevant requirements.

Construct	Items	Factor loadings	AVE	CR	Cronbach's Alpha
Social media marketing information	Q1	.832	.55	.88	.84
	Q2	.816			
	Q3	.743			
Degree of involvement	Q4	.773	.58	.85	.91
	Q5	.835			
	Q6	.729			
Level of information	Q7	.821	.61	.87	.87
	Q8	.813			
	Q9	.781			
Perceived risk	Q10	.822	.57	.91	.79
	Q11	.823			
	Q12	.782			
	Q13	.761			
	Q14	.721			
	Q15	.703			
Information Security Compliance	Q16	.839	.63	.85	.88
	Q17	.822			
	Q18	.766			

Table 2. Convergent Validity

2.3. Models

The analysis of this study consists of two mediating models. The first model is that degree of involvement has a mediating role between social media marketing information and information security compliance (H1: Figure 1).

H1a : Social media marketing information(SMMI) has a positive influence on information security compliance(ISC)

H1b : Social media marketing information(SMMI) has a positive influence on degree of involvement(DoI)

H1c : Degree of involvement(DoI) has a positive influence on information security compliance(ISC)

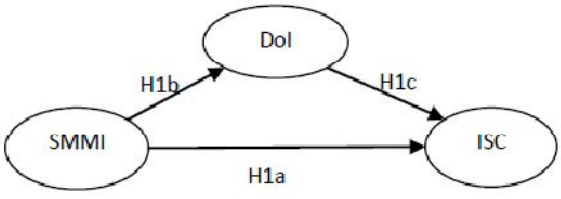

Figure 1. Mediation Model 1

The second model is that perceived risk has a mediating role between level of information and degree of involvement. (H1: Figure 1).

H2a : Level of information(LoI) has a positive influence on degree of involvement(DoI)
H2b : Level of information(LoI) has a positive influence on perceived risk(PR)
H2c : Perceived risk(PR) has a positive influence on degree of involvement(DoI)

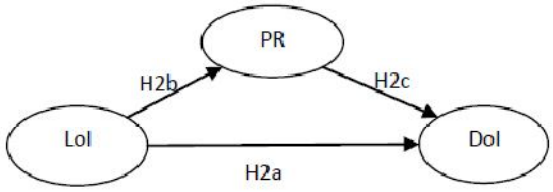

Figure 2. Mediation Model 2

Then, we suggest combination model of hypothesis 1, hypothesis 2 and the above analysis, it leaded to the ultimate hypothesis model like figure 3

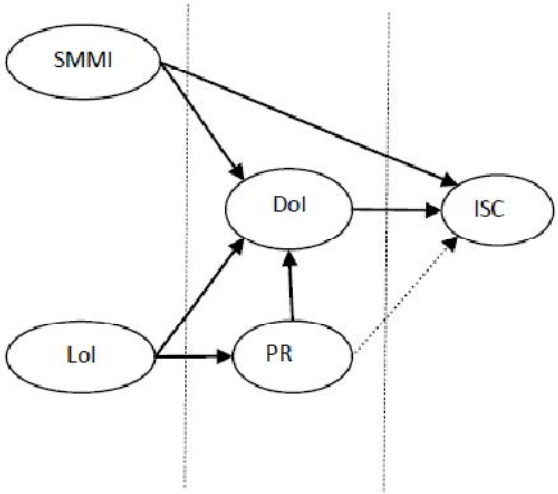

Figure 3 Combination Model

III. RESULTS

3.1. Hypothesis analysis results

This analysis present the t-test results of model standardized structure coefficient. We found that the t test results of the path in hypothesis 1 and hypothesis supported the original hypothesis, detailed results are shown in table 3.

Hypothesis	Standardized structural coefficients	t value
SMMI →ISC	0.41	4.24**
SMMI →DoI	0.71	7.23**
DoI→ISC	0.63	5.92**
LoI→DoI	0.22	2.45*
LoI→PR	0.61	6.35**
PR→DoI	0.51	5.21**

*p<.05, *p<.01

Table 3. Hypothesis t-test Results

H1a is supported : Social media marketing information has a positive influence on information security compliance (t=4.24). As a medium for the dissemination of information, social media could meet user' desire for information; it reduced information asymmetries between users and manufacturers as media tools which have not appeared previously. Therefore, the user is influenced by social media marketing easily is not surprising. However, since restricted by spread debris and low credibility, the influence of social media marketing is difficult to match the traditional media in the short term.

H1b is supported : Social media marketing information has a positive influence on degree of involvement (t=7.23). As a new marketing tool, Social media marketing has a series of features such as interactive, interesting, these features make social media marketing has not obvious advertising feature, users have not natural exclusion for this new type of marketing tool, therefore, relative to traditional advertising, it is easier for users to generate greater degree of involvement in social media marketing information. However, we should also see social media marketing have difficult in self-innovation and development, and because of the content format, it is difficult to reform in image and content. If the user "immune" this marketing tool, social media marketing will be difficult to exert its influence continually.

H1c is supported : Degree of involvement has a positive influence on information security compliance (t=5.92). We see that, in the process of marketing information, the users with high degree of involvement have more positive brand attitude and willingness to act evidently than the users with low degree of involvement. Thus, degree of involvement is really important factors for users to the next step of user'sinformation security complianceattitudes and behaviors.

H2a is supported : Level of information has a positive influence on degree of involvement (t=2.45). Users with high level of information have a lot of general information about such privacy and could capture more information in social media than users with less level of information. For users with high degree of level of information, a certain type of information previously stored in the memory of the experience enable them smoother social media marketing information, and easier to be a high degree of involvement in social media marketing information.

H2b is supported : Users with level of information have more perceived risk of the product in financial,

functional, physical, psychological, social and time(t=6.35). The higher level of information, the more understand of risk and trap in the market, so that, users' acceptance and interpretation of information have a very careful process. Thus, fully understand with related information caused users perceived risk improved significantly.

H2c is supported : Perceived risk has a positive influence on degree of involvement (t=5.21). The perceived risk of information will affect user their degree of involvement in products, because users had to spend effort to circumvent the possible risks of financial, functional, physical, psychological loss. Therefore, the upgrade of perceived risk will enhance degree of involvement in process of users consumption at the same time.

3.2. Model fitness analysis results

We assessed the convergent and discriminant validity of the measurement model through SEM analysis using AMOS 24.0. The fitness between the traits of the measurement model and dataset was examined in order to purify the measurement model. The overall fit of the measurement models was based on a number of factors including the relative $\chi 2$ ($\chi 2$ /df), the goodness-of-fit index (GFI), the adjusted goodness-of-fit index (AGFI), the comparative fit index (CFI), the normed fit index (NFI), and the root mean square error of approximation (RMSEA). The GFI, NFI, CFI higher than 0.90 [10], AGFI higher than 0.8 [11], and RMSEA lower than 0.06 indicate a good fit. In addition, the value of $\chi 2$/df is expected to range lower than 2 [12].

The result of SEM analysis showed that all fit indices of the models were appropriate as advised ($\chi 2$ = 191.24, df = 129, $\chi 2$/df =1.48 < 2, RMSEA = .06 GFI = .97, AGFI = .93, NFI = .95, RFI = .95,IFI = .95, TLI = .93, CFI = .92).

Goodness-of-fit indices	Statistical results
χ^2	191.24
χ^2 / df	1.48
RMSEA	0.06
GFI	0.97
AGFI	0.93
NFI	0.95
RFI	0.95
IFI	0.95
TLI	0.93
CFI	0.92

Table 4. Model Goodness-of-fit test Results

DISCUSSION

Social media is a public participate and interactive media, its effectiveness of marketing should go through information sources, information processing and information security. In these processes, social media marketing information, level of information, perceived risk, and degree of involvement will influence information security compliancethrough complex path relations. Observing factors in model, we find that the root causes of information security compliance are the users' external information (social media) and internal (level) of information, these two aspects could be changed through the media by the corporate. In short, whether the information provided by the media or individual levelpercept, the reason affect user attitudes and behavioral tendencies is the long-term process of marketing information dissemination.

Researchers should clarify the mechanism of information affects the individual, and understand with the mutual relations among social media marketing information, level of information, perceived risk, degree of involvement and information security compliance. Businessman need to understand that the only one influence user's information security compliance. Regardless media information or users' self-storage information, this information through direct or indirect way and ultimately forms the marketing effectiveness, also known as information security compliance.In the era of social media, companies should strive to change the information in two aspects:

One hand, individual enterprises should pay attention to social media marketing information and optimize social media content, such information is not only impact on user attitudes directly, and also influence user attitudes through indirect ways. Enterprises should improve the content from interesting, interest and interaction continuously; they should understand that as a marketing tool, media information dissemination should be a long and arduous task. They need use the variety advantages of low-cost, high-yield characteristics especially, and accelerate scientific and systematic utilization of social media.

The other hand, the user's own level of information could influence information security compliance through indirect means, level of information is not formed in short-term, it need enterprises and even a number of enterprises to create a good environment of product knowledge to enhance the majority of users' information storage and memory. Due to the higher level of information, the easier to have a better attitude in the social media marketing process, therefore, enterprises should be concerned about the users' information security needs in the social media marketing, increase the rich and professional product information, so as to stimulate the potential

compliance behavior become real compliance behavior.

Media is not all means of marketing, but undeniable, media is an integral part of the marketing activities. As the most successful social media, micro-blogging has become an important means of corporate information security compliance.

REFERENCES

[1] P. B. Brandtzaeg, & J. Heim, Why People Use Social Media Sites, Lecture Notes in Computer Science Volume 5621, 2009, pp. 143-152

[2] C. Rose, The Security Implications Of Ubiquitous Social Media, International Journal of Management & Information Systems – First Quarter 2011, Volume 15, Number 1

[3] F. Groeneveld, B. Borsboom, B. van Amstel, Over-sharing & Location Awareness, Center for Democracy & Technology, 2010, February, www.cdt.org/blogs/cdt/over-sharing-and-location-awareness

[4] Wu He, A review of social media security risks and mitigation techniques, Journal of Systems and Information Technology, Vol. 14 No. 2, 2012, pp. 171-180

[5] M. Jakobsson& S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, Wiley, Hoboken, NJ. 2006

[6] S. Granger, Social Engineering Fundamentals, Part II: Combat Strategies, 2002, www.securityfocus.com/infocus/1533

[7] S. Abraham & I. Chengalur-Smith, An overview of social engineering malware: trends, tactics, and implications, Technology in Society, Vol. 32 No. 3, pp. 183-96, 2010.

[8] M. Huber, S. Kowalskiy, M. Nohlbergz, & S. Tjoa, Towards automating social engineering using social networking sites, Proceedings of International Conference on Computational Science and Engineering, 2009

[9] CDC, Social Media Security Mitigations, 2009 www.cdc.gov/socialmedia/tools/guidelines/pdf/securitymitigations.pdf

[10] P.M. Bentler, Comparative fit indexes in structural models. Psychological Bulletin, vol107, no 2,1990, pp. 238-246.

[11] C.Fornell&D. F.Larcker, Evaluating structural equation models with unobservable variables and measurement error. Journal of Marketing Research, vol18, no 1, 1981, pp.39-50.

[12] D.L. Goodhue, Understanding user evaluations of information systems. Management Science, vol41, no 12,1995, pp. 1827-1844.

★★★