TELKOMNIKA, Vol.12, No.2, June 2014, pp. 493~500
ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013
DOI: 10.12928/TELKOMNIKA.v12i2.2015

Measuring Information Security Awareness of Indonesian Smartphone Users

Puspita Kencana Sari*, Candiwan
Faculty of Economic & Business, Telkom University
Jl. Telekomunikasi 1 Bandung, Indonesia
*Corresponding author, e-mail: puspitakencana@telkomuniversity.ac.id, candiwan@telkomuniversity.ac.id

Abstract

One of the information security management elements is an information security awareness programme. Usually, this programme only involves the employees within an organisation. Some organisations also consider security awareness for some parties outside the organisation like providers, vendors, and contractors. This paper add consumers as variables to be considered in an information security awareness programme as there are also some threats for the organisation through them. Information security awareness will be measured from a user's knowledge, behaviour, and attitude of five information security focus areas in telecommunications, especially related to smartphone users as one segment of telecommunication providers. For smartphone users, information security threats are not only from the Internet, but also from phone calls or texting. Therefore, the focus area in this research consists of adhering to security policy, protecting personal data, fraud/spam SMS, mobile applications, and reporting a security incident. This research uses an analytic hierarchy process (AHP) method to measure the information security awareness level from smartphone users. In total, the result indicated that the awareness level is good (80%). Although knowledge and attitude dimension are good criteria of the awareness level, the behaviour dimension is average. It can be a reason why there are still many information security breaches against smartphone users despite a good awareness level.

Keywords*: information security, awareness, measurement, smartphone, users*

1. Introduction

There are three fundamental things that should be considered when applying information security management in an organization: (1) confidentiality of sensitive information by protecting it from unauthorised disclosure or intelligible interception, (2) integrity, by safeguarding the accuracy and completeness of information, (3) availability, by ensuring that information and vital services are available to authorised users when required [1]. These may lead to an achievement of information security intention, which is to ensure business continuity and to minimise business damage by preventing and minimising the impact of security incidents [2].

Any potential threats in an organisation are subjects that influence information security management. Those threats can be detected by identifying circumstances or activities that may cause loss or harm for the organisation, such as financial loss, absence of data or resources, or even loss of company credibility [1]. Many products have been developed to guarantee the security of information. Because of the openness of the network, the vulnerability of operating systems, the security risks in hardware and software, and network viruses and network attacks is constantly variedand each day these threats are getting more difficult to eliminate; so there is no chance to build an absolute security network system [3]. The most important thing in information security management is awareness programmes themselves. The programmes are to ensure that all employees obey the information security policies and procedures established by the organisation. Kruger and Kearney said that "*The initial aim or objective of information security awareness was to ensure that computer users are aware of the risks associated with using information technology as well as understanding and abiding by the policies and procedures that are in place"* [4].

Reported by Symantec, the telecommunication sector is in second rank (10%) after retail (27%) that has a risk in data breaches that could lead to identity theft (top 10 sectors by number of identities exposed) [5] in which Indonesia is in eighth rank of countries with the highest cost per capita of a data breach. The Indonesia Computer Emergency Response Team

Received February 2, 2014; Revised May 6, 2014; Accepted May 26, 2014

(ID-CERT) surveyed, with some of the respondents from telecommunication providers, that 53.1% of incidents reported from March to April 2013 were about network incidents; 15.4% are intellectual property rights; 12.1% are malware incidents; and 11.4% are spam [6]. In 2012, the number of network incidents has reached 76.53%. Therefore, all preventative actions to reduce these incidents should be improved and strengthened by internet service providers, including the telecommunication industry [7].

The Indonesia Internet Profile in December 2012, released by APJII, informed that 65.7% of internet users in Indonesia utilize smartphones as their devices. Smartphone users in Indonesia are predicted to reach 71.6 million people in 2015, jumping from 23.8 million in 2012. This phenomenon is possibly because of the cheapening price of gadgets and services provided by telecommunication providers. But on the other hand, the use of mobile technology also increases the threats of information security. Furthermore, with faster development of the internet and cloud computing, the security issue has become an overwhelming problem for cloud service providers. In order to make the use of the cloud benefits to the full extent, these issues need to be addressed first [8]. In 2010, Yayasan Layanan Konsumen Indonesia (YLKI) recorded that 17.1% of 590 consumers' complaints are about the telecommunication service, where it is infirst rank in that period. About 46.7% of those complaints are about stealing customers' balance. In the end, this will not only break the trust of the customers, but also the credibility of telecommunications, which is one of the concerns in information security management.

Users often have inadequate awareness of how to utilise their gadget securely, or they do have sufficient knowledge but do not implement it properly [9]. Mobile users often save their personal and financial information in their phone. It makes them excellent malware and phishing targets. In November 2010, a virus was spread out to a million mobile phones in China.The virus was sold to mobile users as an anti-virus application, but in fact turned the mobile phones into zombies and began sending spam SMS to people in the phone book [10]. Based on a Symantec security report, the topthree mobile threats in 2012 are 32% stealing information, 25% traditional threats, and 13% sending content. Stealing information includes stealing device data, banking trojan, Ddos Utility, Hacktool; traditional threats include downloader, backdoor; and sending content includessending premium SMS and spam [5]. In this smartphone era, there are new threats developing such as vishing attacks and smishing attacks. Vishing attack is phishing by verbal message, while smishing attack exploits SMS messages; compromised text messages can contain email and website addresses that can lead the innocent user to malware site [10].

As described by many experts, the objects of information security awareness programmes are focusing on employees within the organisation. Other security standards, such as BMIS from ISACA, define the people element of information security management consisting of employees, contractors, vendors, and service providers [1]. Meanwhile, they also define that primary people within BMIS are those who are employed or otherwise associated with the organisation [11]. Moreover, ISO27001 stated that people who work under an organisation's rules should be aware of information security; and all employees of the organisation as well as contractors should receive appropiate awareness education and training and regular updates in organisational policies and procedures connected to their job function [12].

In this paper, consumers are involved as the people element in information security management. Consumers of some organisations also have access to communication networks which means they can obtain some organisational information. As Peltier said, "S*ystem owners have the responsibility to share appropriate knowledge about the existence and general extent of control measures so that other users can be confident that the system is adequately secure"* [13]. Furthermore, as stated in BS ISO 27001, detection, prevention and recovery controls to protect against malware should be implemented and combined with appropiate user awareness [12]. Around 40% of social network users are attacked by malware; and in December 2010, one of the first android botnets (called Gemini) was discovered and the code was wrapped inside a legitimate android application whose developers did not realise was spreading malware.Again in March 2011,Google discovered a botnet called "droiddream" [10]. "*It is essential to keep the public aware of the security threats and educate them towards using good practices in order to get greater security"* (Al-Shehri) [9]. Finally, this writing is proposing a measurement of information security awareness from consumers of telecommunication providers, especially smartphone users. By knowing the level of awareness from consumers, organisations can

establish appropriate security policies and procedures to provide better protection for its consumers.

2. Proposed Method

This research is conducted by using the Kruger & Kerney Model [4]. It adapts a social psychology theory as a tool that proposes three components to measure a favourable or unfavourable manner to a particular object; these are cognition, affect, and behaviour [2]. The components were used to develop three equivalent dimensions known as knowledge (what does a person know), attitude (how do they feel about the topic), and behaviour (what do they do) [1]. Each of these dimensions was then subdivided into five focus areas: (a) adhering to security policies, (b) protecting personal data, (c) fraud/spam SMS, (d) mobile applications, and (e) reporting security incidents. Below is the proposed method adopted from Kruger & Kerney's model.

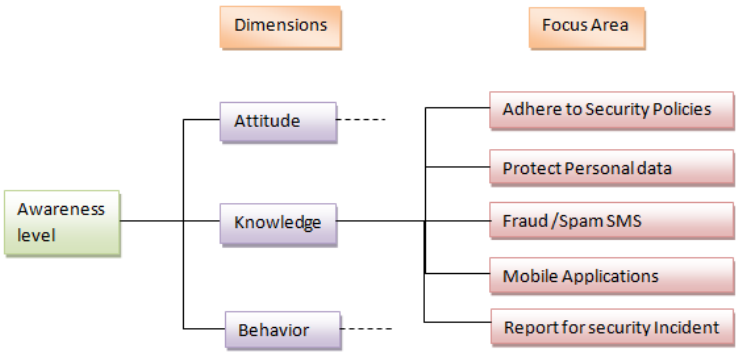


Figure 1. Information Security Awareness Measurement Framework

Five focus areas were extracted from theories, facts and phenomona about information security in Indonesia related to the telecommunication sector. Besides that, areas were defined by an information security expert in telecommunication provision (ISO 27000 auditor). There are two problems mentioned by the expert: (a) adhering to security policies, and (b) reporting security incidents.The first point of awareness in ISO 27001:2013 states that "*persons doing work under the organization's control shall be aware of information security policy*" [12]. That is the reason why security policy as a fundamental aspect in information security management should be discussed as one of the focus areas.

The next focus area is protecting personal data. Nowdays, as written in the introduction, people save a lot of information in their smartphone, including personal and confidential data. They use smartphones not only for texting and making phone calls, but also for doing business and many other purposes. We put areas of protecting personal data to be analysed in this research. The threats of premium SMS or spamming and mobile applications are in accordance with Symantec Security Reports 2013, ID-CERT and also the YLKI complaint report (as stated in the introduction). Symantec mentioned that one of the topthree mobile threats is premium SMS or spamming (sending content); together with YLKI which also reported that in 2010, the most complaintswere about premium SMS. Other mobile threats referred to in the Symantec Report are traditional threats; such as backdoor, malicious code, and so on, that can be caused by a mobile application installation in the smartphone. Although some mobile operating systems now have been implementing the sandbox security mechanism that could separate/isolate each programme, such as iOS and Android 4; in this research we consider that those kinds of smartphone are not the majority of smartphones used in Indonesia.

3. Research Method

This research used the quantative method where data was gathered using questionnaires. Thirty questions were designed to test the knowledge, attitude and behaviour of

respondents concerning the five main focus areas. Each focus area in each dimension has two questions. Some of the questions were answered on a 3-point scale-true, don't know and false (attitude and knowledge dimensions), while others only needed a true or false response (behaviour dimensions), see example question in Table1. The questionnaire was distributed online.

Table 1.Question Examples

To Test	Question	Answer
Knowledge	For protecting my smartphone from malware/virus so I should install antivirus	1. True 2. Dont Know 3. False
Attitude	I aware for protecting my smartphone from virus/malware so I should install antivirus	1. True 2. Dont Know 3. False
Behaviour	I install antivirus for protecting my smartphone from virus/malware that can cause malfunction of my smartphone	1. True 2. False

Data analysis is used as a descriptive method. This method describes or gives an overview of the object under study through the sample data or population as it is, without doing analysis, and making conclusions applicable to the general [14]. The population of this research is people who use smartphones and telecommunication services from Indonesian telecommunication providers. To define the sample, this research uses non-probability sampling with purposive sample techniques.

Operational variables in this research consist of three dimensions, i.e. knowledge (what do they know about the topic?), attitude (how do they feel about the topic?), and behaviour (what do they do?). Each dimension has five focus areas; adhering to security policies, protecting personal data, fraud/spam SMS, mobile applications, and reporting security incidents. Every focus area has indicators, for instance in protecting personal data, the indicators are using passwords in smartphones and logging out from their account after finishing**.** To test the validity of every item in the questionnaire, we used the Pearson Product Moment correlation where every item which has a correlation coefficient equal or more than 0,3 is valid. For reliability testing we used the Alpha Cronbach method, where the coefficient should be equal or more than 0,5.

The scale of awareness was determined using the analytic hierarchy process (AHP). The AHP approach makes use of pairwise comparisons to provide a subjective evaluation of factors based on management's professional judgment and opinion [3]. The score for each focus area per dimension is computed and then normalised to the sum of one. The total score, v (a), was determined by using the formula below [4].

$$V(a) = \sum_{i=1}^{n} v_i(a) w_i$$

Each dimension and focus area has weight that will be used in total awareness score computation. Those weights are defined in Table 2 and Table 3 as follows.

Table 2. Weight score for dimensions

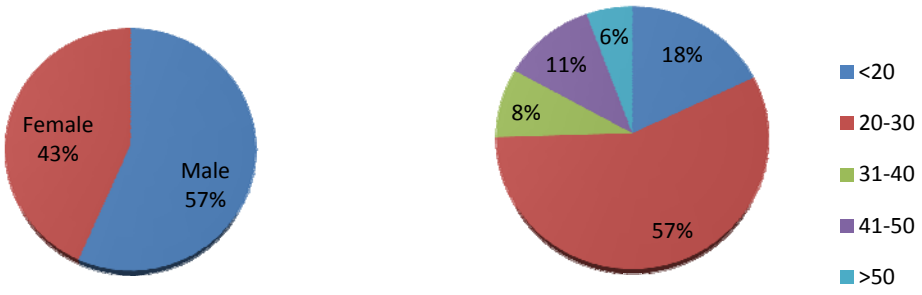
. Dimensions	Weightings
Knowledge	30
Attifude	20
Behaviour	50

Table 3. Weight score for focus area

Focus Areas	Weightings
Adhere to security policies	20
Protect personal data	20
Fraud /spam SMS	20
Mobile Applications	20
Report for Security Incidents	20

4. Results and Discussion

The survey was done for around three weeks, from the 23th December 2013 through 13th January 2014. The total number of respondents was 106 users from several cities in Indonesia; Bandung (64%), Jakarta (17%), Surabaya (6%), Palembang (3%) and other cities (10%). Females who use smartphone in this survey are 43% and males are 57% (Figure 2a).Based on the age range (2b), the majority of respondents (57%) are from the age group of 20-30years of age then followed by the age group of under 20 years old (18%), 41-50 years old (11%), 31-40 (8%) and over 50 years old (6%).



(2a) (2b)

Figure 2. Respondens' characteristic based on gender (2a) and age range (2b)

Regarding the usage of smartphones by the repondents, most of the respondents use their smartphone for browsing (80%), social media (79%),SMS (75%) and email (62%). However only a few users user their smartpohe for phone calls (55%), playing games (44%) and others (5%). Others include navigation, notes for lecture, e-banking, and productivity applications. This usage is suitable with the trend that the use of internet or data is increasing and the use of phone calls is decreasing. This can be seen in the graph in Figure 3.

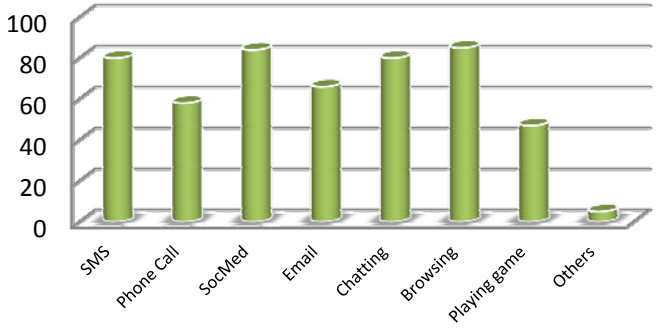


Figure 3. Smartphone usage

Concerning information security breach experience based on the survey, most of the respondents have experience, around82% and those who have no security experience are about 18%. The details of this number experiencing a security breach are as follows; fraud SMS (71%), spam SMS (53%), fraud call (17%), virus (13%) and others (8%). The graph is as shown in Figure 4 and Figure 5.

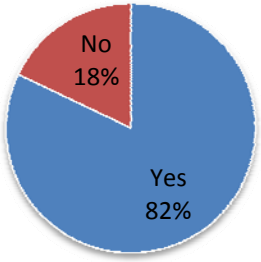


Figure 4. Information Security Breach Experience

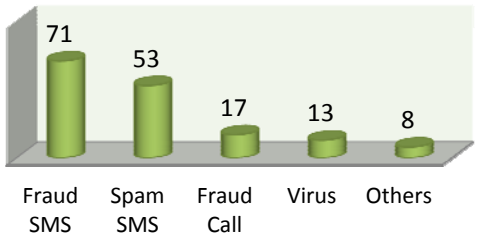


Figure 5. Information Security Threats

The result score of each focus area and dimensions was then grouped as awareness criteria in Table 4. The interval value from that criteria is based on the continuum line value where the maximum score is 100% and the minimum score is 33.33%. Each criteria alsoindicates whether an action plan for improvement is required or not.

Table 4. Awareness Criteria

Criteria / Level	Value (%)	Action Plan
Good	77,78 - 100	No need to action
Average/Satisfactory	55,56 - 77,77	Action potentially required
Poor	33,33 - 55,55	Action required

An awareness level (see figure 6) was used to present the results and the findings of the project. The colour code can give immediate information on which areas are safisfactory, should be monitored, or where action should be taken for improvement (unsatisfactory). So with the colour code, we can conduct which dimension or focus area should be taken for action for improvement in order to increase the information security awareness level.

From the information security awareness level, we can see that:

- The overall awareness level was measured as 80%. This indicates that the awareness level is **good**.
- The awareness level for the dimension of knowledge and attitude is **good**, but **satisfactory** for behaviour.
- The total awareness level for the focus areas adhering to security policies, protecting personal data and fraud/spam SMS are **good**. However the total awareness level for the areas ofthe mobile application and reporting security incidents are **average**.

The result summarised from the information security awareness level suggests that the following focus area would require potential action (average/satisfactory level):

- **Adhere to security policies**
  Behaviour dimension is still at the satisfactory level (75%). Based on the questions asked, some of the respondents may seldom read information on security policy while they are installing applications and they also seldom obey information on security policy. This may take a long time if they read all the items in a security policy while they are installing new applications or creating an account for services in social media, for instance facebook, email, twitter and so on.
- **Mobile aplication with care**
  Both knowledge (76%) and behaviour (61%) dimensions should receive attention in terms of knowledge and behaviour. Based on the questions asked,users don't install an antivirus for protecting their smartphones from viruses or malware that can damage their smartphones as explained in the introduction. Moreover they don't update regularly antivirus applications. In addition, the low level of behaviour may be caused by a lack of knowledge about the antivirus itself.

- **Reporting security incidents**
  In order to reach high levels of awareness, the behaviour dimension should receive more attention. In terms of reporting a security incident, they seldom report to a call centreor complain if theirphone numbers or accountsof social media (twitter, facebook, gmail, yahoo etc.) have experienced a security breach. In addition, they seldom report to the call centreof the telecommunication operator concerning fraud or spamSMS.

Dimensions (weight) / Focus Area (weight)	Knowledge (30)	Attitude (20)	Behavior (50)	Total Awareness/focus are
Adhere to security policies (20)	92	86	75	82
Protect personal data (20)	91	96	82	88
Premium/spam SMS (20)	92	88	84	87
Mobile Applications (20)	76	82	61	70
Report for Security Incidents (20)	81	89	64	74
Total Awareness/dimensions	86	88	73	**80**

Poor
Average
Good

Figure 6. Information security awareness level

Based on the explaination above, it is realised that knowledge and attitude exist in a good level of information security awareness. However, the behaviour dimension is still at a satisfactory level. This means that even though they know about adhering to a security policy and reporting security incidents, they don't do as they know in the usage of smartphones. There are some reasons why this happens, for instance it takes a long time if they read all the items in a security policy or reporting a security incident; maybe, they don't have time to report their problems or they resolve their problems.In the case of a mobile application area, attitude dimension is good but knowledge and behaviour dimension areat satisfactory levels. It means that because of the lack of knowledge, they don't act as the policy requires.

Comparing our research with other research (Kruger's) [4] the focus areas are slightly different. The areas that should be adressed are suitable with the object of the survey. In this journal, the object survey is smartphone users but in Kruger's journal, the object is the employee of an international gold mining company. However, dimension, the weightings, and criteria in this journal are the same as in Kruger's journal.

Regarding information security threats (Figure 5) and the results of information security awareness levels (Figure 6), it seems that there is a contradiction between an information security threat experience with the result of awareness level that the fraud/spam SMS threat experience is high but the security awareness level is good. This may be caused by misunderstanding about fraud/spam SMS where the question is that if users receive an announcement about being the winner of the prize from one provider or someone else, he or she should contact the legal call centre of the provider to check the validity of the announcement. Furthermore, from the SMS there is information about the URL of one of the providers (actually this is the fake URL) so sensitive information of the users can be leaked.

In terms of the focus area of mobile applications it is clearly understood that there is a positive relationship between an information security threat experience (Figure 5) with the result of the awareness level (Figure 6) that the virus threat experience is high and the security awareness level is average (needs potential improvement). This may be caused by using or installing new applications which are actually viruses so this can damage (malfunction) a user's smartphone.

5. Conclusion

Based on our research, it is stated that the level of security awareness for Indonesian smartphone users is still at agood level. This is indicated by the number of total awareness which is about 80% although there are some focus areas that should be addressed in order to have potential improvement. In the behaviour dimension, they are mobile application, reporting a security incident and adhering to security policy. While in the knowledge dimension, there is the mobile application area that should be improved. However in the attitude dimension, all focus areas are at a good level.

By implementing an information security awareness programme for smartphone users, hopefully they understand about security and safeguarding their information in the usage of their smartphone which they usually use for email, services in social media, SMS, chatting etc. This security awareness programmeis important because the number of smartphone users always increases every year and they use it for many purposes.

If user awareness is good and the information security threat is still high, maybe there are other factors that cause it. Therefore, for the next research, it can be developed to analyse thosefactors such as why information security breaches to smartphone users are still relatively high, especially fraud/spam SMS.

References

[1] Sari PK. *A Concept of Information Security Management for Higher Education*. International Conference on Technology and Operation Management, 3rd. Bandung. 2012: 469-477.
[2] Kruger H, and et al. *A vocabulary Test to Assess Information Security Awareness*. South African Information Security Multi-conference in Port Elizabeth, South Africa. 2010.
[3] Zhao J, Zhou Y, Shuo L. A Situation Awareness Model of System Saurvivability Based on Variable Fuzzy Set. *TELKOMNIKA.* 2012; 10(8): 2239-2246.
[4] Kruger HA, Kearney WD. A Protoype for Assessing Information Security Awareness. *Elsevier Journal: Computers & Security*. 2006; 25: 289-296.
[5] Symantec. *Information Security Threat Reports*. Symantec Corporation. 2013; 18.
[6] IDCERT. *Laporan Dwi Bulan II 2013*. Indonesia Computer Emergency Response Team. 2013.
[7] IDCERT. *ID-CERT Annual Report 2012*. Indonesia Computer Emergency Response Team. 2012.
[8] Shabech H, Jeyanthi N, Iyengar N.Ch.S.N. A study on security Threats in Cloud. *International Jouarnal of Cloud Computing and Services Science (IJ-CLOSER).* 2012; 1(3): 84-88.
[9] Al-Sehri Y. Information Security Awareness and Culture. *British Journal of Arts and Social Sciences*. 2012; 6(1): 61-69
[10] Laudon KC, Traver CG. *E-Commerce 2012: Business, Technology, Society*. England. Pearson Education Limited. 2012.
[11] ISACA. *Business Model for Information Security*. USA. 2010.
[12] British Standard Institution. *ISO/IEC 27001:2013 Information Tecnology-Security Techniques-Information Security Management Systems-Requirements***.** Switzerland. BSI Standard Limited. 2013.
[13] Peltier, Thomas R. *Information Security Fundamentals, Second Edition*. Boca Raton. CRC Press. 2014.
[14] Sugiyono. *Statistik Untuk Penelitian*. Bandung. Alfa Beta. 2009.