ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 501-509 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

# Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of Indonesia

Mainar Swari Mahardika[*,1], Achmad Nizar Hidayanto[1], Putu Agya Paramartha[1], Louis Dwysevrey Ompusunggu[1], Rahmatul Mahdalina[1], Farid Affan[2]

[1]*Faculty of Computer Science, Universitas Indonesia, Jakarta, 10430, Indonesia*

[2]*Faculty of Economics and Business, Universitas Indonesia, Jakarta, 10430, Indonesia*

ARTICLE INFO

*Article history:*
*Received: 20 March, 2020*
*Accepted: 14 June, 2020*
*Online: 21 June, 2020*

*Keywords:*
*Information Security*
*Measuring IS Awareness*
*HAIS-Q*
*AHP*
*Palinfo*
*Judicial Commission*

ABSTRACT

*The Center for Analysis and Information Services (Palinfo) at the Judicial Commission closely related to the management of information systems which are used to process organizational internal data and information systems on public services. Data processing and network management have an information system security risk. The Judicial Commission seeks to reduce risk and improve the quality of information security. This study aims to measure employee awareness of information security at the Center of Analysis and Information Services at the Judicial Commission, which also includes the Data/IT department. The study was conducted through an arranged interview with three experts and the dissemination of information security awareness questionnaires to all Palinfo employees, amounting to 25 persons. The results of the questionnaire were evaluated using The Human Aspects of Information Security Questionnaire (HAIS-Q) and the Analytic Hierarchy Process (AHP) method. The results showed that the level of information security awareness in Palinfo and the Data/IT section was at the "average" level. There is one focus area that shows a "good" level. While in the Data/IT department, several sections that show a "good" level. Based on these results, we recommend being used in maintaining information security, namely seven policies, ten information technology approaches, and socialization/training conducted in various ways.*

## 1. Introduction

Information is a valuable asset for an organization because information is a strategic resource in increasing business value. Therefore, the protection of information security is an absolute matter that must be taken seriously by all highest ranks of leaders to employee concerned. With the overall safety of the environment where the information is located, the integrity, availability, and confidentiality of information in the company will be guaranteed. To maintain the continuity of an organization's business, the organization needs the availability of data and information as one of the influential factors [1].

Information system security threats are actions taken both from within the system and from outside systems that can consider the balance of the information system. Threats to information security arise from individuals, organizations, connections, and events that can cause damage to information sources. Security threats to information systems not only related from outside the company such as business opponents or other individuals and groups but can also be used from within the company [2].

According to data reports on information security incidents based on reports in 2017 showed that at the Judicial Commission there was a hacker attack that crippled several application systems and ransomware virus attacks that attacked several computers connected to the Internet network. The report shows that the role of human error is a contributing factor to information security incidents. Human error involved in information security can be in the form of opening insecure websites, opening attachments/links carelessly, downloading files without scanning, using passwords easy to guess, sharing passwords with others, losing devices or losing access to mobile devices, often connecting devices to public networks [3]. The occurrence of the security incident shows that

[*] Mainar Swari Mahardika, Universitas Indonesia, Jakarta, Indonesia.
Email: mainar.swari@ui.ac.id

https://dx.doi.org/10.25046/aj050362

employees are not expected to have an awareness of information security. Therefore, research needed to measure the level of employee awareness of information security.

According to the January-December 2018 Annual Report ID-SIRTII/CC found that in 2018 there were 16,939 website incidents/defacement and the .go.id domain ranked first with 30, 75% more often affected by defacement. Based on the monitoring results, there are 4,499 phishing links, of which 1,654 Indonesian domain websites have been affected or indicated for phishing. Data leak monitoring in 2018 obtained data leakage of 785,967 from domains and records. The number comprises 785,906 records / lines from 61 various .id domains. One of the domains obtained from data leakage is the domain go.id [4].

The Judicial Commission of the Republic of Indonesia is vested with two constitutional authorities, namely to conduct a selection of candidates for Supreme Court Justices and other authorities to maintain and uphold the dignity and behavior of judges [5]. With these two authorities, the Judicial Commission must be able to utilize the use of Information Technology (IT). Utilization of IT aims to make public services easily and cheaply accessible to the public. With the increasing use of ITs in carrying out their authority functions, making information security issues an important aspect.

The Center of Analysis and Information Services (Palinfo) is a center with three functions, namely the Analysis section, the Information Services section, and the Data/IT section. The Analysis section manages the analysis of decisions. Information Services section implements management and control of information relating to the internal use of the government and the general public. The Data/IT section manages and controls the information and communication technology sector. The Center of Analysis and Information Services closely related to the management of information systems that are used to process organizational data internally and information systems relating to public services. For this reason, information security awareness is very important to be carried out within the Center for Information Services and Analysis.

The background of this research stems from information security issues in the Judicial Commission that were not as expected. We divide the problem into 3 aspects, namely organization, inadequacy, and people. From the organizational aspect, the problem that occurs is that not yet implemented a comprehensive information security management system policy and not yet implemented ISO 27001 regarding information security in all sections. From the aspect of inadequacy, the problems that occur are lack of training on information security, lack of security of access to information in each room, and lack of knowledge regarding the importance of information security. And from the aspect of people, the problem that occurs is that there has not been much socialization to improve employee information security understanding, and Measuring the level of employee information security awareness has never been carried out. From the background of this problem, the thing that most concerns the researcher is the problem in the aspect of people, namely the measurement of employee awareness of information security has never been carried out. We need measurement of information security awareness level to be carried out to determine the level of awareness of Judicial Commission employees, especially Palinfo, which level they are at. We can see the background of the problem in the fishbone diagram in Figure 1.

Therefore, the research needed to measure the level of information security awareness to identify the focus area of information security which still needs to be improved to develop a strategy for information security awareness methods. Many frameworks are used to measure information security awareness. We finally chose The Knowledge Attitude Behavior (KAB) theory developed by Kruger and Kearney (2006) and AHP (Analytic Hierarchy Process). KAB theory has often been used as a model for measuring information security [3]. We chose AHP in this research because of its superiority in terms of decision making and accommodation over attributes both qualitative and quantitative. Besides, AHP decision making able to provide more consistent results, easy to understand and use [6].

The purpose of this research is to measure the level of information security awareness among employees at the Center of Analysis and Information Services (Palinfo) of the Judicial Commission Republic of Indonesia. The author would like to measure the level of information security awareness of employees and recommend increasing information security awareness in the Center of Information and Analysis Services (Palinfo) of the Judicial Commission Republic of Indonesia.

The systematic writing of this paper consists of Introduction that contains background topic selection in the paper, Literature Review that contains theories related to selected topics, Research Methodology which contains the methodology used and the results, recommendations and conclusions of the research.

## 2. Related Works

Various studies related to the measurement of information security awareness have been carried out by several researchers, especially in Indonesia. Sari et al. (2014) conduct an information security awareness study for smartphone users. In this study, they developed the KAB framework. The KAB model that they use only takes on the dimensions of knowledge and behavior. Then the data they have obtained from the dimensions analyzed using the CFA model [7].

In the following year, Sari et al. (2015) conducted a similar study of smartphone users. However, there are differences with previous research. They use the KAB framework with dimensions of knowledge, attitude, and behavior. Then they do the analysis using AHP calculations [8].

Sari et al. conducted research using the same method as the researchers, the KAB and AHP methods. The difference with researchers, Sari et al. studies smartphone users while researchers study government employees in Indonesia.

Other research has been conducted by Kusumawati (2018) who researched government agency employees in Indonesia. This research uses the KAB model and MCDA calculation method. This study uses 5 focus areas [9]. The difference in research conducted by Kusumawati (2018) with researchers is that researchers used 7 focus areas and AHP calculation methods.

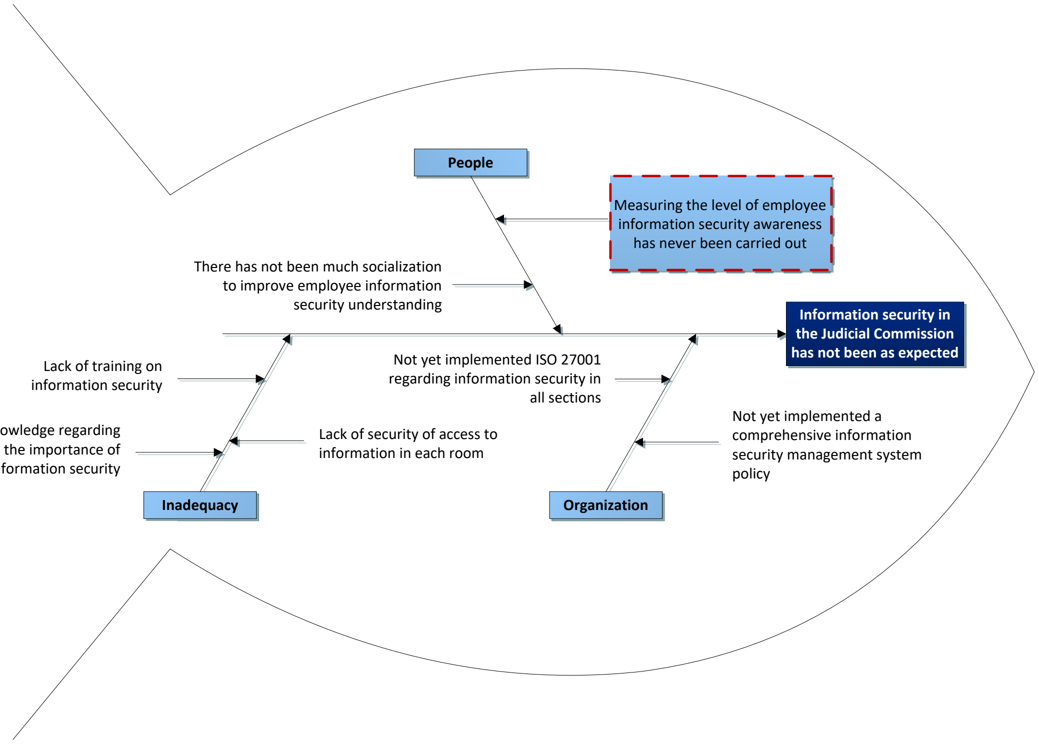
People
Measuring the level of employee information security awareness has never been carried out
There has not been much socialization to improve employee information security understanding
Information security in the Judicial Commission has not been as expected
Lack of training on information security
Not yet implemented ISO 27001 regarding information security in all sections
Lack of knowledge regarding the importance of information security
Lack of security of access to information in each room
Not yet implemented a comprehensive information security management system policy
Inadequacy
Organization

Figure 1: Fishbone Diagram Analysis

Subsequent studies have been conducted by Puspitaningrum et al. (2018) which used as the main reference for researchers. Puspitaningrum et al. (2018) conducted a study of SDPPI employees under the Ministry of Communications and Information of the Republic of Indonesia. They use the HAIS-Q framework and AHP calculations [3]. The difference from the research conducted by the researchers is that the researchers do not use the KAMI Index framework and the researchers research employees within the Judicial Commission of the Republic of Indonesia. The researcher also made a comparison among information security awareness between non-Data/IT employees and Data/IT employees.

For the framework used in this study, researchers used research written by Lund (2018) for the use of the HAIS-Q Questionnaire which contained 63 questions divided between knowledge, attitude, and behavior, and 7 focus areas [10]. Examples of questionnaires can be seen in Table 3.

## 3. Literature Review

### *3.1. Information Security*

Information security is the protection of data, information, and equipment from unauthorized parties so that the information resources remain safe from all types of threats and risks. Information is an important resource in an organization, used as a material for decision making. Because of this, information must be quality. The quality of information is determined by three factors namely relevance, timeliness, and accuracy [11].

It may also be interpreted that Information is a description, statement, concept, and sign that contain values, meanings, and messages, whether data, facts or explanations that can be read, heard and seen in various forms in according to the times [12].

Information security means protecting data or information systems from prohibited use or access, and also focuses on maintaining the integrity, confidentiality, and availability of various information related to where information is stored on electronic media, paper, or other forms [12].

### *3.2. Information Security Awareness*

According to NIST (2011) Information Security Awareness is a condition where the concern focused on information security problems. It can also be interpreted as using Information Security Awareness as a bulwark of a company in the face of current information security threats [13].

Information Security Awareness also defined as a situation in which people have a responsibility to use information derived from knowledge about information security that has been obtained. The person must also be aware of the importance of information security goals, threats, and risks. [14].

Information Security Awareness can be measured using the Human Aspect of Information Security (HAIS-Q) instrument. HAIS-Q can measure information security behavior and its validity has been recognized by many studies [15].

### *3.3. HAIS-Q (Human Aspects of Information Security Questionnaire)*

HAIS-Q (Parsons et al., 2013) is a tool that could be used to measure employee knowledge, attitude and behavior, namely KAB Component. KAB is a benchmark for organizations that can solve various problems. For example, the use of KAB to determine the condition of an organization's information security and the use of KAB for making an organization's information technology strategy. HAIS-Q has seven focus areas including Password Management (PM), Email Use (EU), Internet Use (IU), Social Media Use (SMU), Mobile Devices (MD), Information Handling (IH), and Incident Reporting (IR). These focus areas have their sub-focus areas [16] as can be seen in Figure 2.

### *3.4. AHP (Analytic Hierarchy Process)*

AHP is a model that uses human subjects who are experts in their fields to make decisions. The human subject is the only input in the AHP model. Expert criteria refer to people who understand the problem posed correctly. Because it uses qualitative inputs (human perception), this model can process qualitative things besides quantitative things. Make AHP as a comprehensive decision-making model, taking into account quantitative and qualitative matters immediately [17].

Based on Thomas L. Saaty (1990), AHP is a framework for making effective decisions on complex issues. AHP helps simplify issues and speed up the decision-making process [18]. AHP is a global framework that arranges variables into hierarchies, provides relationships and values for these variables so that decision-makers can consider them and provide alternative solutions [19].

Based on Taylor (2004), AHP is used globally in a variety of problem conditions in the private and government fields. AHP is a method used to facilitate the selection of criteria and provide ratings so it can facilitate decision making [20].

## 4. Research Methodology

To achive the objectives of this study, we first conduct a literature review on theories related to the topic of this research. We then compare the various measurement models to find suitable models for measuring information security awareness. Next, we finally selected the model that will be used in this study based on previous studies is the HAIS-Q model by Parsons et al. for a table of questions. HAIS-Q model has a detailed focus compare to the others. HAIS-Q measures 7 focus areas related to measuring of employee awareness levels for information security in the organization. HAIS-Q provides a questionnaire to identify the level of information security awareness [16]. The flowchart showing the research process can be seen in Figure 3.

### *4.1. Questionnaire Method*

The questionnaire methodology contains 3 lists of issues. The first set of questions tests the knowledge factors, the second about the attitude factors, and the third about the behavior factors. These 3 factors questions were developed by Parsons et al. and compared to 7 focus areas in the HAIS-Q model. Research questions are answered in sequential order, with a clear declaration for each question in the questionnaire using a Likert scale, from 1 shows strongly disagree until 5 shows strongly agree.

### *4.2. Data Collection Method*

Data collection was conducted from October 2019 to December 2019 at the Center for Analysis and Information Services of the Judicial Commission of the Republic of Indonesia. In data collection activities, researchers will conduct research on information security reporting data at the Center for Information Analysis and Services by providing questionnaires to 25 companies related to their security awareness.

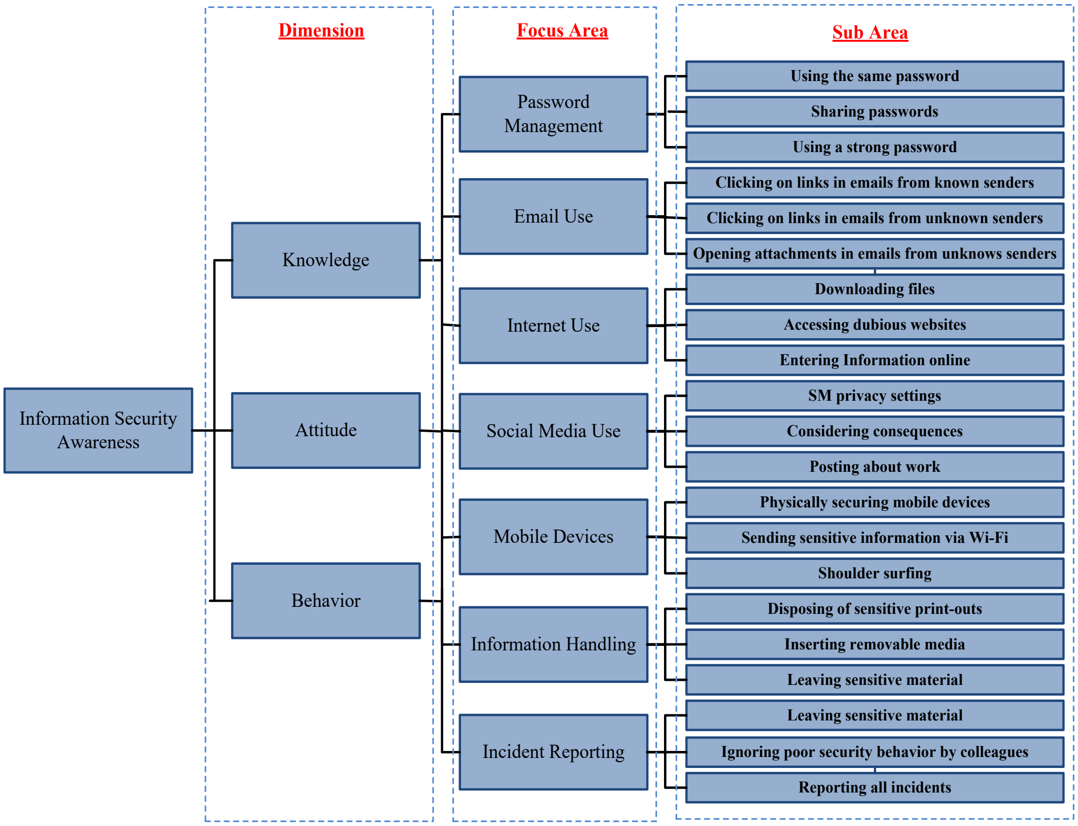
Dimension
Focus Area
Sub Area
Information Security Awareness
Knowledge
Attitude
Behavior
Password Management
Email Use
Internet Use
Social Media Use
Mobile Devices
Information Handling
Incident Reporting
Using the same password
Sharing passwords
Using a strong password
Clicking on links in emails from known senders
Clicking on links in emails from unknown senders
Opening attachments in emails from unknows senders
Downloading files
Accessing dubious websites
Entering Information online
SM privacy settings
Considering consequences
Posting about work
Physically securing mobile devices
Sending sensitive information via Wi-Fi
Shoulder surfing
Disposing of sensitive print-outs
Inserting removable media
Leaving sensitive material
Leaving sensitive material
Ignoring poor security behavior by colleagues
Reporting all incidents

Figure 2: HAIS-Q Focus Area (Parson et al)

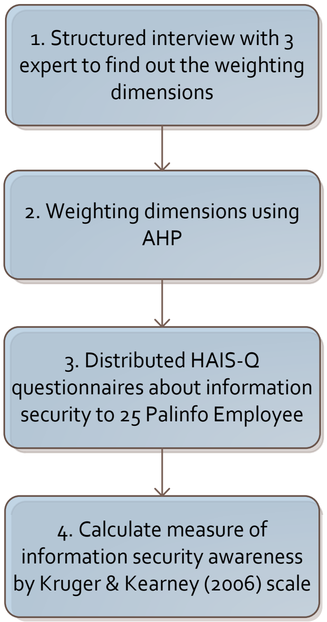
1. Structured interview with 3 expert to find out the weighting dimensions
2. Weighting dimensions using AHP
3. Distributed HAIS-Q questionnaires about information security to 25 Palinfo Employee
4. Calculate measure of information security awareness by Kruger & Kearney (2006) scale

Figure 3: Research Process Flowchart

### 4.3. Measurement of Weight

At the first event, we asked people (experts) with have knowledge in the information security sector to fill the paired focus area matrix. In selecting most matrices, experts compare the important certain focus areas with other people. The level scale using scale 1 indicates the lowest level important, for 3 shows moderate important, for 5 shows strong important, for 7 shows very strong or demonstrated important and for scale 9 indicates the highest level important. The AHP process is used to gain information security awareness about the weight of each focus [19]. Experts fill the paired comparison focus area. The weight will then be ranked to find which focus areas have the highest information security awareness.

Next, at the second event, we calculated the scale of information security awareness after collecting questionnaires from employees. We determined the priority scale of 7 factors in HAIS-Q. While the preference scale used in each question in the questionnaire is a scale 5 which indicates the highest level (very aware) to scale 1 which indicates the lowest level (not aware) for each question in 7 HAIS-Q factors. Then we calculate the scale of 7 factors with percent of knowledge, attitude, and behavior factors. The scale obtained will be matched with a scale by Kruger & Kenney (2006) which divided into 3 levels: poor, average, and good [21] as can be seen in Figure 5.

## 5. Result, Discussion, and Recommendation

### 5.1. Result of Weighting Focus Area Dimensions

The research first, we create an AHP Hierarchy to determine the criteria used. AHP hierarchy can be seen in Figure 4. After determining the criteria, we conducted the study in an arranged interview with three experts to discover out the weighting results from seven focus area dimensions. The format of the pairwise criteria can be seen in Table 1. We then calculate the focus area that has been weighted by the expert using the AHP weighting with a comparison matrix formula. The results of the study show that the focus area “Incident Reporting” was at first place with the highest weighting of 0,233278921, the focus area “Social Media Use” was ranked next with 0.229004904, the focus area “Information Handling” was in third place weighing 0,15646, the focus area was “Internet Use” was in fourth place weighing 0,131023552, the focus area “Email Use” was in fifth place weighing 0,115031643, the focus area “Password Management” was in sixth place weighing 0,0876223, and the focus area “Mobile Devices” was ranked the last with a total weight of 0,047578679 can be seen in Table 2. The focus areas for Incident Reporting, Social Media Use, and Information Handling are the highest. This is because the Center for Analysis and Information Services is closely linked to the management of information systems, which are used to process organizational data internally and information systems relating to public services, so that the three focus areas must be well managed so that all-important data are maintained.

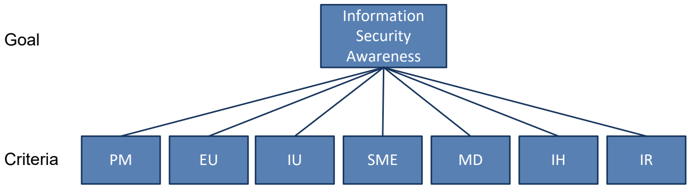

Figure 4: AHP Hierarchy

Table 1: Example AHP Pairwise Criteria

| | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| EU | | | | | | | | | | | | | X | | | | | IU |

### 5.2. Result of Measuring Information Security Awareness

Questionnaires on information security were distributed after expert weighting of focus area dimensions. The research questionnaire was distributed to all 25 employees of the Center for Analysis and Information Services. Example questionnaire can be found in Table 3. The sample questionnaire was then collected for analysis of the data obtained. Respondent data show that the respondent’s work units are divided into sections on analysis, Information Services and Data/IT, each consisting of 8 persons. While the Administration Section consisted of only 1 person. More than half of the respondents held non-functional or general functional positions. The complete demographic of respondents can be seen in Table 4.

Table 2: Focus Area Weight Ranking

| Focus Area | Weight | Ranking |
|---|---|---|
| Incident Reporting | 0,233278921 | 1 |
| Social Media Use | 0,229004904 | 2 |
| Information Handling | 0,15646 | 3 |
| Internet Use | 0,131023552 | 4 |
| Email Use | 0,115031643 | 5 |
| Password Management | 0,0876223 | 6 |
| Mobile Devices | 0,047578679 | 7 |

Table 3: Example HAIS-Q Questionnaire

| Internet Use | | | | | | | |
|---|---|---|---|---|---|---|---|
| Attitude | Knowledge | Behavior | SD | D | N | A | SA |
| While I am at work, I shouldn't access certain websites | Just because I can access a website at work, doesn't mean it's safe | When accessing the internet at work, I visit any website that I want to | | | | | |

Table 4: Respondent Demography

| Variable | List | Total | Percent |
|---|---|---|---|
| Work Unit | Analysis | 8 | 32% |
| | Information Service | 8 | 32% |
| | Data/IT | 8 | 32% |
| | Administration | 1 | 4% |
| Gender | Male | 15 | 60% |
| | Female | 10 | 40% |
| Age | 21 – 30 years | 6 | 24% |
| | 31 – 40 years | 16 | 64% |
| | 41 – 50 years | 3 | 12% |
| | 51 – 60 years | 0 | 0% |
| Position | Structural | 2 | 8% |
| | Functional | 6 | 24% |
| | Non-Functional | 17 | 68% |
| Work Period | ≤ 5 years | 6 | 24% |
| | 6 – 10 years | 11 | 44% |
| | 11 – 15 years | 7 | 28% |
| | 16 – 20 years | 0 | 0% |
| | 21 – 25 years | 1 | 4% |
| | ≥ 26 years | 0 | 0% |
| Education | ≤ SLTA/Equivalent | 0 | 0% |
| | D-I – D-III | 4 | 16% |
| | D-IV / S-1 | 16 | 64% |
| | S-2 / S-3 | 5 | 20% |

To calculate the final measurements, weights and scales are used in Table 5. As explained by Kruger & Kearney (2006), the percentage of 30%, 20%, and 50% determined the weight and scale of information security awareness in this research for each dimension of knowledge, attitudes, and behavior [21].

Table 5: Weight and Awareness Scale (Kruger & Kearney, 2006)

| Dimensions | Weightings |
|---|---|
| Knowledge | 30% |
| Attitude | 20% |
| Behavior | 50% |

The color map by Kruger & Kearney (2006) in Figure 5 is used to show in detail the level of awareness of information security in each focus area. The red color represents the level of "Unsatisfactory", the yellow color represents the level of "Monitor" which has potential needs to be repaired. Green represents the level of "Satisfaction".

| | | |
|---|---|---|
| Good (80% - 100%) | 🟩 | Satisfactory – no need for action |
| Average (60% - 79%) | 🟨 | Monitor – action potentially required |
| Poor (59% and less) | 🟥 | Unsatisfactory – action required |

Figure 5: Scale of Information Security Awareness Colour (Kruger & Kearney, 2006)

The results of measuring the level of information security awareness in the Center of Analysis and Information Services are amount to 78.10 and included in the "average" level, which can be seen in Table 6. These findings indicate that the information security awareness of employees at the Center of Analysis and Information Services needs to be monitored regularly and action taken if needed.

Table 6: Level of Information Security Awareness of The Center of Analysis and Information Services

| Focus Area | Knowledge (30%) | Attitude (20%) | Behavior (50%) | Total (%) |
|---|---|---|---|---|
| Password Management | 82,08 | 79,04 | 79,04 | **79,95** |
| Email Use | 77,01 | 76,25 | 76,25 | **76,48** |
| Internet Use | 80,81 | 72,71 | 68,91 | **73,24** |
| Social Media Use | 78,03 | 78,28 | 78,79 | **78,46** |
| Mobile devices | 81,83 | 77,01 | 78,53 | **79,22** |
| Information Handling | 82,84 | 80,31 | 80,81 | **81,32** |
| Incident Reporting | 80,05 | 76,76 | 77,27 | **78,00** |
| **Total** | **80,38** | **77,19** | **77,09** | **78,10** |

The Center of Analysis and Information Services, as can be seen in Table 6, mostly indicates the level of "average" in terms of information security awareness. But there is an area that shows a "good" level of information security awareness, namely the "information handling" area. The area of "internet use" has the lowest weight, so it needs to be monitored more intensely. Therefore, this area requires attention monitoring to increase employee awareness. Internet use gets a low value on the behavioral dimension. Because maybe employees have the idea to open a website at working hours can become entertainment for them without considering work computers. They can contaminate with viruses through access to certain websites. What they don't know is that certain websites can carry viruses/malware that can turn off their work computers. For this reason, socialization is necessary where each employee must know the importance of maintaining information security. The Center for Information Services and Analysis also needs to develop a policy on Information Security. Not only made, the policy must be implemented effectively and must be understood by all employees. Policies must be easily accessible or available to employees to ensure that they will not ignore the policy. It should also be clear to all employees what their actual roles and responsibilities with regards to information security.

A study was also conducted to compare information security awareness among Data/IT employees. The results of measuring the level of employee awareness of information security of Data/IT are equal to 83,51 or categorized as a "good" level as can be seen in Table 7. For employees in the Data/IT section, out of a total of 8 people, 6 areas indicate the level of "good" information security namely "password management", "e-mail use", "social media use", "mobile devices", "information handling", and "incident reporting". Whereas there is only one area shows the "average" level of information security, namely "internet use". This result shows the level of information awareness among Data/IT employees is higher than that of all employees in the Center of Analysis and Information Services, the graph can be seen in Figure 6. A better level of information awareness among Data/IT employees is possible because starting last year the Data/IT sector is implementing ISO 27001:2013 concerning information security.

Table 7: Level of Information Security Awareness of Data/IT Unit

| Focus Area | Knowledge (30%) | Attitude (20%) | Behavior (50%) | Total (%) |
|---|---|---|---|---|
| Password Management | 87,88 | 86,29 | 87,88 | **87,56** |
| Email Use | 82,33 | 81,54 | 83,13 | **82,57** |
| Internet Use | 84,71 | 79,17 | 76,00 | **79,25** |
| Social Media Use | 79,96 | 81,54 | 81,54 | **81,07** |
| Mobile devices | 88,67 | 83,92 | 85,50 | **86,13** |
| Information Handling | 86,29 | 84,71 | 84,71 | **85,18** |
| Incident Reporting | 86,29 | 80,75 | 81,54 | **82,81** |
| **Total** | **85,16** | **82,56** | **82,90** | **83,51** |

### *5.3. Discussion*

### *5.3.1 Mapping Level of Security Awareness*

Based on the results of the study, Data/IT employees received higher scores than employees of the Center for Analysis and Information Services (Palinfo) of the Judicial Commission of the Republic of Indonesia. These results can be compared to previous research conducted by Puspitaningrum et al. (2018) of SDPPI employees under the Ministry of Communications and Information of the Republic of Indonesia who receive an awareness value of 78,33. From the two research results it can be seen that Palinfo employees have lower information security than SDPPI employees. But the awareness of Data/IT employees are more aware than SDPPI employees. These results can help to map the level of information security awareness among government employees in Indonesia.

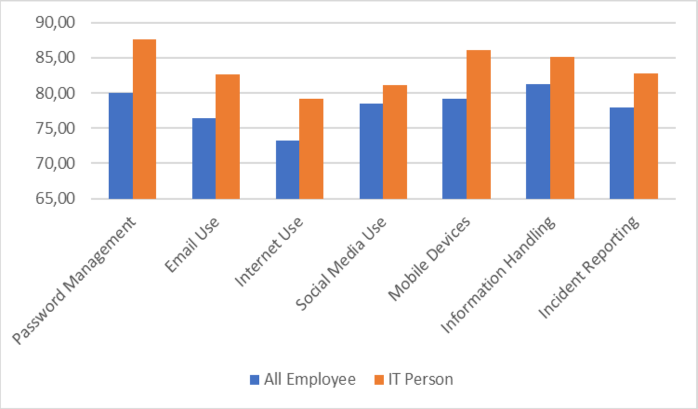

Figure 6: Level Comparison between IT Person and All Employee

### *5.3.2 Lesson Learned*

Lesson learned is knowledge or understanding gained from experience that can be both success and failure. A lesson learned must be significant (or important, a dominant factor, the main cause) and have a real impact or be concluded that it is worthy of learning from an activity. The learning must be valid, factual, technically correct and can be applied in the design, process, subsequent decisions to reduce or eliminate the potential causes of failure, problems whether predicted or not, setbacks, difficulties, bad luck and reinforcing results positive for example in terms of efficiency and effectiveness going forward.

In this research, lesson learned can be taken in the form of successful implementation of information security awareness. Lesson learned can be drawn from the results of information security awareness of employees in the unit of Data/IT that have shown a “good” level. Employees in the unit of Data/IT get a good result, certainly due to several factors. For this reason, researchers conducted additional interviews with the head of the Data/IT unit and Data/IT staff to find out the factors that led to the success of information security awareness in the Data/IT unit. Factors that led to the success of information security awareness in the unit of Data/IT can be seen in Table 8. These factors can be lesson learned for the Center of Analysis and Information Services (Palinfo) who still shows an “average” level awareness or lesson learned for other sections of the Judicial Commission that will implement information security awareness of employees and other organizations in order to successfully implement information security awareness as well.

### *5.4. Recommendations*

The recommendation to increase information security awareness for employees at the Center of Analysis and Information Services is to create policies that can be applied to all focus areas, including:

- Policies about governing password security that include procedures that require employees to apply a password. Passwords must be at least 8 characters in length and a password must consist of numbers, symbols, capital letters, and lower-case letters. Employees are also required to keep their passwords confidential to anyone;
- Policies about governing the use of e-mail, including procedures requiring employees to be aware that not all emails they receive are safe;
- Policies about governing the use of the internet which include procedures for not providing access to employees to be able to download files freely. Also, policies governing employee access rights to certain websites and sanctions that must be applied if employees carelessly enter information about work on certain websites;
- Policies governing the use of mobile devices, including procedures that prevent the use of public networks for work purposes;
- Policies about governing the use of social media, including procedures for employees who cannot freely open social media accounts using office networks and there are sanctions that must be applied if employees carelessly enter information about work on their social media;
- Policies governing the handling of information, including procedures requiring employees to protect all forms of confidential work documents;
- Policies about governing incident reporting which include procedures requiring employees to report all forms of information security incidents that occurring at the

workplace and sanctions that must be applied if employees do things that jeopardize information security.

Table 8: Success Factors Data/IT Unit in Implementing Information Security Awareness

| Dimension | Success Factors Data/IT Unit | Source |
|---|---|---|
| Knowledge | • Data/IT employees have gained knowledge about information security based on ISO 27001<br>• Data/IT employees already have knowledge of the rules for sharing passwords and the rules for using quality passwords<br>• Data/IT employees already have knowledge of the user's responsibility regarding email<br>• Data/IT employees already have knowledge of websites that should not be accessed and the consequences of using these prohibited websites.<br>• Data/IT employees already have knowledge of risks when using public networks<br>• Data/IT employees already have knowledge of USB that can store viruses/malware | Interviews with Heads of Data/IT and Data/IT staff |
| Attitude | • Data/IT employees already have responsibilities regarding the use of quality passwords<br>• Data/IT employees already have responsibilities regarding email security in the organization<br>• Data/IT employees already have a policy regarding the use of licensed software<br>• Data/IT employees already have responsibilities regarding the risks of using public networks<br>• Data/IT employees already have responsibilities towards outsiders visiting the office for interests in the Data/IT unit | Interviews with Heads of Data/IT and Data/IT staff |
| Behavior | • Data/IT employees have implemented information security procedures based on ISO 27001<br>• Data/IT employees are already using passwords for personal use and using quality passwords<br>• Data/IT employees can distinguish safe and non-secure e-mail, and not open any link in the e-mail<br>• Data/IT employees are already using licensed software<br>• Data/IT employees are already using a VPN to work remotely<br>• Data/IT employees accustomed to doing regular backups of important data | Interviews with Heads of Data/IT and Data/IT staff |

Meanwhile, in terms of the information technology approach, we recommend raising awareness in focus areas that are still in the "average" area, especially in Palinfo. Our recommendations are:

- Encrypt sensitive documents/data, emails, and passwords. The recommendation is to increase the level of focus area level on e-mail use and password management;
- Routinely updating software, operating systems, applications, anti-virus, and firewalls. The recommendation is to increase the level of focus areas on internet use, e-mail use, mobile devices, and social media use;
- Use of VPN if the employee wants to access work e-mail from an outside place. This recommendation is to increase the level of focus areas on mobile devices and email use;
- Develop software that can assist employees in reporting information security incidents that occur. This recommendation is to increase the level of focus areas on incident reporting;
- Use spam filters on emails so that spam emails can be blocked. The recommendation is to increase the level of focus areas on e-mail use;
- Perform regular backups of sensitive documents/data using the correct backup procedures. The recommendation is to increase the level of focus areas on information handling;
- Access control over the use of the internet so that employees can only open websites that relate to work needs. The recommendation is to increase the level of focus areas on internet use;
- Creating a multi-layered room security using RFID technology. This recommendation is to increase the level of focus areas on information handling;
- Provides knowledge about downloading files and installing programs. The recommendation is to increase the level of focus areas on internet use and information handling; and
- Provides knowledge about information security standards that refer to ISO 27001. The recommendation is to increase the level of the entire focus area.

Strengthening information security awareness also requires socialization and training of employees about information security awareness, which is very important in organizations. Socialization can be done by various means, such as

- Socialization by sending e-mails to all employees;
- Socialization using media brochures distributed to all employees;
- Socialization by using banner media placed in strategic places which can be seen by all employees;
- Socialization by holding an open seminar attended by all employees;
- Socialization by placing advertisements on the Judicial Commission website so that employees are always reminded to continue to maintain information security. Training on information security also needs to be done, so that information security knowledge among employees increases and can be directly applied in the organization.

Several businesses, such as implementing policies, information technology, socialization and training, do need to be done. But apart from that, many other things need to be done. But apart from that, much more needs to be done so that the relevant preventive and corrective actions can be effectively applied. Learning and reflecting from the experience of organizations that have successfully developed the habit of obtaining information, the following examples are a variety of approaches that can be taken as preventive and corrective action: (1) Implement a system of rewards with a penalty (reward-punishment) for all staff and employees; (2) Top-down approach, where each leader will give instructions to his subordinates periodically to care for and implement information security procedures [22].

## 6. Conclusion

The results of calculating the level of information security awareness in the Center for Analysis and Information Services are at the "average/monitoring" level. This means that there are still many employees at the Center for Analysis and Information Services who do not understand the importance of information security. While the results of calculating the level of information awareness in the Data/IT section are at the level of "good/satisfactory". Information security awareness in the field of Data/IT is better because employees in the Data / IT section have been certified ISO 27001: 2013 on information security. So they understand the importance of maintaining information security. We suggest several solutions for the Center of Analysis and Information Services to increase the level of employee awareness of information security, namely by making 7 policies, by using 7 technology approaches, by conducting socialization using 5 means of approach and by conducting training related to information security for employees. In addition, 2 approaches are also needed which can be done so that preventive and corrective actions can be applied effectively.

For future research, it is a necessary to organize research to measure information awareness among all employees at the Judicial Commission of the Republic of Indonesia, considering that information security is important not only for the Center of Analysis and Information Services (Palinfo) but also important for all employees at the Judicial Commission of the Republic of Indonesia.

## Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this journal.

## Acknowledgment

This study was supported by PUTI Prosiding 2020 grant with title "Evaluasi Master Data Management pada Organisasi, Universitas Indonesia".

## References

[1] Information Security Awareness, ISO 27001:2013 Standard, 2013.

[2] T.H. Purwamto, "Makalah KSI: Pentingnya Keamanan Sistem Informasi", Fakultas Teknik, Universitas Muria Kudus, 2014.

[3] E.A. Puspitaningrum, F.T. Devani, V.Q. Putri, A.N. Hidayanto, "Measurement of Employee Information Security Awareness: Case Study At The Directorate General of Resources Management and Postal and Information Technology Equipment Ministry of Communications and Information Technology" in 2018 Third International Conference on Informatics and Computing (ICIC), Palembang, Indonesia, 2018. https://doi.org/10.1109/IAC.2018.8780571

[4] BSSN, Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center, Pusat Operasi Keamanan Siber Nasional, Jakarta, 2018.

[5] Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, UUD 1945, 2002.

[6] R. Daneshvar, E. Turan, "Selecting The Best Supplier Using Analytic Hierarchy Process (AHP) Method", African Journal of Business Management, 6(4), 1455-1462, 2012. https://doi.org/10.5897/AJBM11.2009

[7] P.K. Sari, Candiwan, N. Trianasari, "Information Security Awareness Measurement with Confirmatory Factor Analysis" in 2014 International Symposium on Technology Management and Emerging Technologies, Bandung, Indonesia, 2014. https://doi.org/ 10.1109/ISTMET.2014.6936509

[8] P.K. Sari, Candiwan, "Measuring Information Security Awareness of Indonesian Smartphone User" Telkomnika, 12(2), 493-500, 2014. https://doi.org/10.12928/TELKOMNIKA.v12i2.2015

[9] Kusumawati, "Information Security Awareness: Study on a Government Agency" in 2018 International Conference on Sustainable Information Engineering and Technology, Malang, Indonesia, 2018. https://doi.org/ 10.1109/SIET.2018.8693168

[10] P. Lund, "Information Security Awareness Amongst Students", System Sciences, Luleå University of Technology, 2018

[11] A. Kadir, Terra Ch. Triwahyuni, Pengantar Teknologi Informasi Edisi Revisi, Penerbit Andi, Yogyakarta, 2013.

[12] R. Primartha, Security Jaringan Komputer Berbasis CEH, Penerbit Informatika, Bandung, 2018.

[13] R. Kissel, NIST IR 7298 Revision 1, Glossary of key information security terms, National Institute of Standards and Technology, US Department of Commerce, 18, 2011.

[14] F.J. Haeussinger, "Information Security Awareness: Its Antecedents And Mediating Effects On Security Compliant Behavior", Georg-August-University Goettingen, 2014.

[15] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A.M. Cormac, T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies", Journal Computers & Security, Volume 66, 40-51, 2017. https://doi.org/10.1016/j.cose.2017.01.004

[16] K. Parsons. Mc Cormac, A. Butavicius, M. Pattinson, M. Jerram. "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAISQ)", Journal Computers & Security, Volume 42, 165-176, 2014. https://doi.org/10.1016/j.cose.2013.12.003

[17] B. Permadi, AHP, Pusat Antar Universitas, Universitas Indonesia, Jakarta, 1992.

[18] T.L. Saaty, "How to Make a Decision: The Analytic Hierarchy Process", European Journal of Operational Research, 48, 9-26, 1990. https://doi.org/10.1016/0377-2217(90)90057-I

[19] T.L. Saaty, "Decision Making with the analytic hierarchy process International Journal of Services Sciences (IJSSCI), Vol. 1, No. 1, 83–95, 2008. https://doi.org/10.1504/IJSSCI.2008.017590

[20] B.W. Taylor, "Introduction to Management Science", Pearson Education Inc., New Jersey, 2004.

[21] H.A. Kruger, W.D. Kearney, "A prototype for assessing information security awareness", Journal Computers & Security, Volume 25, Issue 4, 289-296, 2006. https://doi.org/10.1016/j.cose.2006.02.008

[22] R.E. Indrajit. Keamanan Informasi dan Internet Edisi Kedua, Preinexus, Yogyakarta, 2016.