PEOPLE: International Journal of Social Sciences
ISSN 2454-5899

Ma'ruf & Rochman, 2019

Volume 5 Issue 2, pp. 863-877

Date of Publication: 04th October 2019

DOI- https://dx.doi.org/10.20319/pijss.2019.52.863877

This paper can be cited as: Ma'ruf, K. F., & Rochman, M. M., (2019). Guidelines for Developing Information Security Training and Awareness Programs in Government Agency: The Perspective of Addie Instructional Design Models (A Case Study in Indonesian Government Agency. PEOPLE: International Journal of Social Sciences, 5(2), 863-877

GUIDELINES FOR DEVELOPING INFORMATION SECURITY TRAINING AND AWARENESS PROGRAMS IN GOVERNMENT AGENCY: THE PERSPECTIVE OF ADDIE INSTRUCTIONAL DESIGN MODELS (A CASE STUDY IN INDONESIAN GOVERNMENT AGENCY)

Kholif Faiz Ma'ruf
Training Center for National Cyber and Crypto Agency, Depok, Indonesia
kholif.faiz@bssn.go.id

Muhammad Machbub Rochman
Training Center for National Cyber and Crypto Agency, Depok, Indonesia
muhammad.machbub@bssn.go.id

Abstract

Ideally, every government agency must be able to develop training programs and information security awareness in its own environment. But the fact is in Indonesia, not all of government agencies have implemented training programs and information security awareness. Thirteen percent of the respondents surveyed said they already had the program but were not structured and had no guidance, so the program was not well organized. This study provides a structured guide to building an effective information security training and awareness program, based on the ADDIE instructional design model approach (analyze, design, develop, implement, and evaluate). The results of the study state that the ADDIE instructional design model can be used to construct training programs and information security awareness in government agencies in a structured manner and can guarantee that training, awareness, education and professional development are

not stagnant and can always be relevant in answering information security issues that occur in organizations.

Keywords

Training Program, Information Security Awareness, ADDIE, Security Awareness Program

1. Introduction

1.1 Background

Humans are still the weakest link of cybersecurity chains (Boulton, 2017). Human factors are very complex parts to control vulnerability. One of the biggest risks to an organization's information security is often not a weakness in the technology control environment, rather it is the action or inaction by employees and other personnel that can lead to security incidents (pci, 2014). If technological factors that can be patched at any time if its weakness is found, but It is different from human factors. Humans are a key factor in achieving good information security (Mann, 2007) and One of the greatest threats to information security could actually come from within your company or organization that was an insider (brodie, 2009). Building information security behavior in organizations can be done by building human capabilities through effective information security training and awareness programs for all employees.

Applying security controls to humans in organizations is one of the information security challenges that must be faced by every Government Agency in Indonesia. The non-smooth outcome of Lemsaneg's Security Awareness Program in some Local Governments has even encouraged research Projections of scenario building and scenario planning in building awareness behavior in the Regional Government through the Security Awareness Program to provide projections to build the future information security in Indonesia (Suprijandoko 2017). In the study mentioned that the information security awareness program designed by Lemsaneg provides substance content in the form of the importance of using official email, the dangers of using social media applications, the dangers of telephone and facsimile use, and tapping activities that can be overcome with counter sensing activities. Security control in humans is facilitated through training and education.

Based on data obtained from the results of interviews by the author (in 2017) with 37 representatives from each agency (at the time of education and training) both the central government and local governments stated that about 87% of respondents stated that their agencies did not yet have training programs and information security awareness, while 13% of respondents

stated that they had implemented a training program and information security awareness in their institutions but were not yet structured and had no guidance, so that they were not well organized. Because it does not have a guide, the program built only contains the consequences and impacts if it does not implement an information security policy. The program is only effective for scaring employees, not to raise awareness of information security behavior in organizations.

According to Jason Townsell (2013) in building a training program of any kind, 3 components must always be implemented to achieve the objectives of the training program, namely Knowledge, Skill and Attitude (KSA) which are usually abbreviated as KSA. Referring to this, then to build a good information technology security awareness program, program design must touch all three aspects of the KSA.

KSA can be given as a whole series of unity between awareness, training, education, and certification of professional development (Wilson, M. Hash, J. 2003). The combination of awareness, training, education and professional certification can touch KSA directly both for the highest level of leadership in organizations, middle leaders, CIO (Chief Information Officer), CISO (Chief Information Security Officer), IT managers, staff who deal directly with devices IT, regular staff, outsourced employees, contractors and organizational stakeholders.

Ideally, every Government Agency must be able to develop training programs and information security awareness in its environment, given the work culture and work objects in each agency are different. This study provides structured guidance for building effective information security training and awareness programs, using the ADDIE instructional design model approach (Analyze, Design, Develop, Implement, and Evaluate). The ADDIE model is used because it has been proven to have been implemented in every government agency both central and regional to develop training programs both in the Center /Center / Training Agency. Like other training programs, training programs and information security awareness can also be built using this model.

1.2 Problem

The problem that will be discussed in this study is to answer the question: How can the ADDIE instructional design model help build training programs and information security awareness in Government Agencies?

1.3 Purpose

The purpose of this research is to provide structured guidance for Indonesian Government Agencies to develop training programs and information security awareness in their Institutions.

1.4 Benefit

The theoretical benefit of this research is as a literature on the development of knowledge about methods of building training programs and information security awareness in Government Agencies. While the benefits of this research broadly are the realization of structured information security training and awareness programs in each Government Agency of the Republic of Indonesia.

2. Literature Review

2.1 ADDIE Instructional Design Models

The ADDIE model emerged in the 1990s which was developed by Reiser and Mollenda, then re-developed by Dick and Carry (1996) to design learning systems. This model uses 5 phases of development, as follows:

a. Analysis

The first phase is the need and performance analysis. Needs analysis is a step needed to determine the abilities or competencies that trainees need to learn. Performance analysis is carried out to find out and clarify whether the performance problems faced requiring a solution in the form of implementing a learning or improvement management program.

b. Design

The design phase is related to learning objectives, assessment instruments, content, analysis of learning planning materials and learning media. This stage must be systematically designed.

c. Develop

This phase is carried out to detail and build learning material. Material can be created, purchased, modified as long as it reaches the learning objectives.

d. Implement

Implementation phase aims to implement a program that has been designed and has been developed. At this stage learning objectives must be measurable and attainable.

e. Evaluation

The final phase is the evaluation which aims to improve the system by processing data that has been obtained from the previous stage. The results of the evaluation must be documented and an action plan implemented for program improvement.

Every phase of the ADDIE Model must be passed, implemented and documented. The success of this model depends on the success at each stage carried out.

2.2 Components of the Information Security Training and Awareness Program

Before developing information security training and awareness program relatively, an agency must be aware that the program needs to cover four components of activity, namely awareness, training, education, and professional development certification. These four components must be prepared, designed, budgeted and properly documented to achieve a comprehensive training cycle and information security awareness cycle.

2.2.1 Awareness

The information security awareness program is a program that focuses on providing knowledge and security policies, threats and vulnerabilities in the workplace, sanctions for security violations, and explaining the latest developments in security issues. This program must continually be able to include information security messages for each employee in various formats, to create an information security attitude pattern. The format that can be used in this program is only limited to the level of know-what and does not reach the level of know-how. Some formats can be used in awareness programs such as posters, flyers, events, e-mails, briefings, meetings, websites, pocketbooks, and broadcast announcements via loudspeakers containing information security advice.

2.2.2 Training

Information security training focuses on developing the competency skills and attitudes of employees involved in the information security process to carry out their duties and responsibilities to secure information. Training is designed based on competence in the duties and responsibilities of information security for each employee. Every employee who has the same duties and responsibilities can follow the same training curriculum. However, the more technical the tasks and responsibilities, the more technical the level of training. Training programs can be divided into several skill levels such as basic, intermediate and upper. Its implementation can be in collaboration with the education and training center of agencies or private training institutions with a customized curriculum.

2.2.3 Education

The Education Program integrates all competency skills into knowledge so that they can be studied at universities and produce the output of employees who specialize in information technology security. Education will produce employees who specialize in information security.

The implementation of this component in government agencies can be given through Bachelor, Post-Graduate or Doctoral Scholarship programs, both study assignments, and school permits.

2.2.4 Professional Development

As a form of employee professional development tasked with securing information in government agencies, certification needs to be done. Certification can be in the form of International Exams or competency tests conducted by agencies to prove that the employee has earned a certificate of expertise. If the standard of employee expertise has been tested, the guarantee that the employee will work according to the duties and responsibilities of information security is increasing. Certification can be carried out both at the level of awareness, training, and education through an assessment mechanism so that direct behavior can be reflected in the security of information in the workplace based on daily knowledge and work experience.

3. Methodology

The research method used was qualitative research with descriptive data presentation and guided by the ADDIE instructional learning development technique. ADDIE was used because it world widely proven used and it fits in Indonesian learning development context. There are 4 steps in this research, as follows:

Steps 1. The initial stage of the research was carried out by pre-research data collection to get an overview of the Information Technology Security Awareness and Training program in government agencies.

Steps 2. Conducting a literature review to review the structure of training programs and information security awareness is associated with the ADDIE instructional model.

Steps 3. Develop steps/guidelines for government agencies to build an Information Technology Security Awareness and Training Program by the ADDIE instructional design model.

Steps 4. Take conclusions and suggestions from this study, as well as follow-up for further research.

The data source is taken from the experience of agencies and literature studies both book sources, international standards, journals, websites, and information security teaching materials. Data collection techniques using interview techniques to a sample of 37 agencies at the time of training is ongoing, as a simple random sampling. The data sources were then analyzed and developed into a guide for developing an information security training and awareness program using the ADDIE model through the 4 research steps mentioned.

4. Result

4.1 Phase 1 ADDIE: Analysis

The initial stage of developing information security training and awareness program was Needs Analysis. Most information security awareness programs fail to reach their goals due to the misunderstanding of the objectives of the needs analysis itself. The presumption that arises is that information security awareness programs from one agency can be directly adopted by other agencies with some adjustments. Yet the fact is each organization has different needs in providing awareness, training, education and professional development to each employee. The work culture and main tasks of the organization also determine the theme of the information security awareness program to be developed.

Needs analysis must also be able to help identify gaps between current information security awareness achievements and the ideal outcomes that they want to fulfill (Gap analysis methods can be used in this section). Therefore at this stage, at least 5 main aspects must be identified as a form of gap analysis, as follows:

a. Ideal needs for each awareness, training, education and certification program for agencies;
b. Activities that have been carried out to achieve these ideal conditions;
c. Status of success of activities carried out by the agency;
d. The gap between the ideal needs and what has been done; and
e. The priority sequence is to fill gaps in awareness, training, education and professional development/certification programs.

In conducting a needs analysis, key personnel from each line of the organizational sector must be involved (Wilson, M. Dan Hash, J. 2003). A minimum of 5 key personnel must be involved, among others:

a. Executive Management;

Is the head of the organization in government agencies, in this case, are the Minister, Head of LPNK (Non Department of Government Institution), the Governor, Regent and Chancellor of the University. Organizational leaders are people who best understand the direction of the goals, vision, mission, and business processes of the organization. So that they can provide direction related to regulations and fundamental matters regarding information security programs that are aligned with the organization's mission and the duties and responsibilities set by the leadership of the organization. They also need to ensure that each of their staff must implement and adhere to an information security awareness program.

b. Security Personnel;

In government agencies commonly referred to as CISO (Chief Information Security Officer), or Head of Information Security Officer, or Head of the Office of Encoding, or Head of Information Technology Security. In some agencies, CISO is held concurrently by the CIO (Chief Information Officer). CISO will act as an expert consultant from within the organization because it is considered to be very knowledgeable about information security policies in its institution, under its task which is to enforce information security policies. As a consultant, CISO will observe the needs of users and provide advice and recommendations in the form of the best alternative learning methods.

c. System Owners;

The owner of the system at a government agency is the head of the Work Unit in the organization. Usually held by Echelon II or High Leadership Position. This person is the person who best understands the overall business process in his work unit and masters the details of the need for information security or control applied in his work unit. At this stage, the Head of the Work Unit is one of the targets (user feedback) whose needs will be analyzed for the information security program in his work unit.

d. System Administrators dan IT Support Personnel;

Personnel who have the highest authority on IT operations and information systems are critical in the organization. These personnel is the ones who need to be given the highest education related to information security programs. Not enough at the level of understanding, but it needs to reach the stages of Education and Professional Development / Certification. By presenting them at the time of needs analysis, it will be clearly illustrated what needs are needed by the organization to achieve effective information security / IT implementation. Every expressed need will be communicated with CISO / CIO to achieve the ideal needs of the organization.

e. Operational Manager dan System Users;

Senior personnel in the organization and system users. These personnel is the ones who most need the need for information security awareness and training in security controls, as well as safe behavior during interactions with the system / daily operations. This personnel will be analyzed for their needs regarding habits, behavior, culture and operational information security controls.

4.2 Phase 2 ADDIE: Design

The design phase is essentially compiling a complete plan, which consists of strategies, priorities, material complexity, and funding in every aspect/component of the program (awareness, training, education, and professional development/certification).

4.2.1 Building Learning Strategies

The strategies developed to play an important role in determining the success of awareness, training, education and professional development/certification programs. The strategy developed includes at least the following, among others:

a. Incorporating awareness, training, education and professional development/certification programs into organizational policies in the form of Ministerial Regulations, LPNK Head Regulations, Governor Regulations, Regents Regulations or University Chairposts stating that training and information security awareness programs must be held in government agencies and must be followed by every employee;
b. The scope of the program that has been identified at the needs analysis phase;
c. Duties and responsibilities for each person involved in the program, starting from personnel who design, build, implement, manage, maintain, evaluate to the technical level such as personnel who ensure employees follow the program and read the material shared;
d. Output and outcomes of each program component;
e. Participants target for each component of the program;
f. Determine the parts of the program that are mandatory or optional;
g. Learning objectives of each component of the program;
h. Topics of material that must be studied in each session;
i. Learning methods used in each component of the program;
j. Documentation, feedback, and evidence from all aspects in each component of the program;
k. Material evaluation and renewal in each program component; and
l. Duration of learning from each activity.

4.2.2 Determine Priorities

After the design of the learning strategy is formed ideally, then at the time of application sometimes the organization will be hit with budgetary problems and the availability of other resources, not to mention if it is constrained by the problem of a busy schedule of activities. Therefore it is necessary to determine the priority of implementing the strategy. This condition can

be very complex and depends on the level of availability of resources (man, money, method, material, market), the direct impact of the strategy on the organization, the maturity level of information security and the number of organizational activities.

4.2.3 Material Complexity

In designing material complexity it is necessary to pay attention to the target participants and their position in the organization and the skills needed in that position. Not every employee must start training from the lowest level, if the employee's information security skills in an agency are assessed to have reached the intermediate level, then it can be started for awareness, training, and education from that level.

This stage applies to the components of awareness, training, and education. In the awareness and training component, adjustments to material complexity can be easily determined through information security policies and competencies that must be achieved. Whereas in the Education component, complexity is sometimes difficult to adjust because of adjusting to the university curriculum. This can be resolved with the pattern of education in cooperation/partnership with government agencies by applicable regulations.

4.2.4 Funding

Designing a plan with high funding can hinder the approval of the program. Therefore a CIO must arrange funding so that the priority of the program can be made according to the availability of the budget in the organization. If the budget is very limited, it is highly recommended to be able to cooperate with information security technical implementing agencies in Indonesia, in this case, BSSN (National Cyber and Crypto Agency).

4.3 Phase 3 ADDIE: Develop

After the design phase is created, the next step is to develop the material needed for awareness programs and information security training. The program will be more effective if the material presented is attractive, bikini-clad, and the content created is intended specifically for participants according to their duties and responsibilities (not general material).

4.3.1 Develop Awareness Materials

Information security awareness material can contain specific issues or cases that often occur at the agency. In practice to develop this material, it can utilize the source of material obtained through Seminars, conferences, courses, and other references related to information security. Case examples can also be taken from the public that is considered relevant in the organization, as well as related website sources about information security news.

Significant topics that are often used as material for discussion include:

- Password management, starting from the creation, frequency of change, security and usability;
- Safeguards against viruses, worms, Trojan horses, and other malware along with antivirus scanning and updates;
- Information security policy and sanctions if violating it;
- Email Spam and Spoofing;
- Security of accessing websites from trusted sources;
- Data backup and storage;
- Social media and chating security;
- Social engineering;
- Incident response;
- Shoulder surfing;
- Smartphone and mobile security;
- Laptop security when traveling on business;
- Access control systems and guest;
- Software license;
- Desktop security; and
- Encryption when transmitting data.

4.3.2 Develop Training Materials

Information security training material can be developed based on the decision about whether the training will be carried out in-house or contracted out. So that in developing the material can also use resources from within the organization or use a third party (vendor), or a combination of both. To determine it, there are at least 3 points to consider, as follows:

a. Does the agency have sufficient resources to develop training materials, including instructors with the right skills and have an adequate number of training providers?
b. Which is more effective in terms of budget to organize and develop training materials in-house or through contracted out?
c. Does the material developed contain confidentiality that only the agency should know?

After determining the decision, the training material can be developed based on the competencies to be achieved by the duties and responsibilities inherent in the training participants in the institution. The approach method is competency-based training according to their duties and

responsibilities towards information security. Training material can be developed to several training levels starting from the basic, intermediate and advanced levels. What must be observed at this stage is the accuracy in categorizing the function of the training material specialization.

4.4 Phase 4 ADDIE: Implement

The awareness program and information security training can begin to be implemented only if the previous three stages (Analysis, Design, Develop) have been completed. Program implementation can be adjusted to the model of the application of information security organizations in their respective agencies. Some agencies have implemented a centralized model, where all program resources including training are managed by the CIO. Some are also decentralized where the initial stages (Analyze, Design, Develop) are fully regulated by the CIO, while for the implementation phase they are left to each work unit along with the needs for the resources.

4.4.1 Communicating the Program Implementation Plan

When going to implement an awareness and information security training program, first make sure that the program plan has been well communicated to each party planned to be involved in the program. The purpose of this communication is to ensure commitment to the availability of support both funds and other resources needed during program implementation. The communication conveyed is at least in the form of an explanation of the outputs and outcomes expected of this program, benefits for the organization, and resources needed during the implementation of the activities. After communication runs smoothly, agreed upon, and approved by the Head of Agency, awareness and training programs can be implemented.

4.4.2 Awareness Implementation Techniques

Application techniques for awareness programs can vary and are selected based on the complexity of the material to be conveyed. Awareness material must be interesting, up-to-date, and given repeatedly but using different variations of techniques will work more effectively. Here are some popular techniques that can be applied:

a. Writing short information security messages on office equipment that is commonly used daily (such as post-it notes, notepad, pens, seminar kits, goody bags, etc.);
b. Make posters containing information security content;
c. Screensaver about information security, pop up screens or short messages when the computer is turned on;
d. Daily Tips Flyers;

e. Send emails or short messages to group chats to all employees about information security;
f. Information security videos in public places such as the Lobby;
g. Information security advertisements on agency websites;
h. Make an Information Security Awareness Day event or similar activity;
i. Making information security mascot;
j. Make an information security quiz; and
k. Give appreciation to employees who are considered exemplary in providing examples of the application of information security.

4.4.3 Application of Training Techniques

The application of information technology security training can be done in various ways. In modern times, the application of training tends to use information technology. Therefore technology selection must be easily accessible and easy to use by participants, easy to maintain and can be used by various levels of audience, and allows participants to monitor the progress of the training. Training implementation techniques also vary and can be combined according to the capabilities of the resources possessed. Here are some popular techniques that can be applied:

- Interactive video, this technique is effective for applying to distance learning models and is offline;
- Web-based training, this technique is the most popular and the easiest technique to be accessed by participants online. Unlike interactive videos, this technique can present a variety of learning more varied features;
- Computer-based training, this technique requires participants to install software on their computers. The advantage is not to depend on the internet connection;
- Training in the classroom is a conventional method, where participants are required to enter the class to get lessons from the instructor together. Sometimes this technique is more effective at absorbing training material because participants can concentrate more on receiving material and regardless of the participants' boredom towards their work routines. The disadvantage is the difficulty in managing the training schedule, especially for agencies that have a busy schedule of activities.

4.5 Phase 5 ADDIE: Evaluate

The success key of awareness programs and information security training is one that is continuous improvement. Changes in the organization are very reasonable. It could be that as time develops, the IT infrastructure in the Institution also changes. The organizational structure can

change, even the organization's vision and mission can change. These changes can make awareness programs and information security training must be updated immediately. Therefore the evaluation phase needs to be carried out at least by monitoring the implementation of the program, evaluating the program accompanied by follow-up, managing existing changes and making improvements to the program.

The objective that must be achieved is the follow-up on the renewal of the awareness program and training by the development of organizational change. Therefore the evaluation must be carried out with a combination of methods. The following are some methods that can be used:

- Use the Evaluation Form or Questionnaire;
- Focus Group Discussion;
- Selective interview; and
- Benchmarking.

5. Closing

5.1 Conclusion

Based on the results of the study, it can be concluded that the ADDIE instructional design model can be used to build training programs and information security awareness in Government Agencies. By referring to each stage of the ADDIE model, the training program and information security awareness can be structured and ensure that training, awareness, education and professional development are not stagnant and can always be relevant in responding to information security issues that occur in the organization.

5.2 Suggestion

The following are suggestions addressed to BSSN and government agencies, among others:

a. The results of this study can be used as a reference by BSSN in establishing the rules of the Head of BSSN regarding guidelines for building training programs and information security awareness in Government Agencies.
b. Each government agency can use the results of this study as a guide in building information security training and awareness programs in their respective institutions.

5.3 Future Research

The following are some follow-up plans that can be carried out as further research:

a. Make a list of indicators of the success of training programs and information security awareness in Government Agencies;

b. Develop strategic steps that can be carried out by every Government Agency in Indonesia in developing.

References

Boulton, Clint. (2017). *Humans are (still) the weakest cybersecurity link*. Framingham. CIO magazine. https://www.cio.com/article/3191088/security/humans-are-still-the-weakest-cybersecurity-link.html

Brodie, Cindy. (2009). The Importance of Security Awareness Training. SANS Institute Reading Room site. United States.

K. Sari, Bintari. "*Desain Pembelajaran Model ADDIE dan Implementasinya Dengan Teknik JIGSAW*". Prosiding Seminar Nasional Pendidikan. Sidoarjo.

National Institute of Standards and Technology (NIST). (2003). *Building an Information Technology Security Awareness and Training Program*. Gaithersburg: NIST.

National Institute of Standards and Technology (NIST). (2006). *Information Security Handbook: A Guide for Managers*. Gaithersburg: NIST.

National Institute of Standards and Technology (NIST). (2008). *Performance Measurement Guide for Information Security*. Gaithersburg: NIST.

National Institute of Standards and Technology (NIST). (2014). *A Role-Based Model for Federal Information Technology/Cybersecurity Training*. Gaithersburg: NIST.

PCI (2014). Best Practices for Implementing a Security Awareness Program. Security Standards Council. United States.

Prasasti, Trini dan Tarigan, Asmara I. (2014). *Implementing The Addie Model for UT's Tutor Training Program Development*. Prosiding Teaching and Learning in the 21st Century.

Suprijandoko, R. Firman. (2017). *Transformasi Lemsaneg menjadi BSSN: Proyeksi model scenario dalam membangun perilaku awareness pada Pemerintah Daerah melalui Program Security Awareness*. Jakarta. Jurnal Widyaiswara.