ISSN 2278-3083
Volume 9, No.6, November - December 2020
International Journal of Science and Applied Information Technology
Available Online at http://www.warse.org/ijsait/static/pdf/file/ijsait02962020.pdf
https://doi.org/10.30534/ijsait/2020/02962020

Designing Integrated Data Security System

Raden S.B.Cokro[1], Ryan Tofani[2], Gunawan Wang[3]
[1]PT.PLN (Persero) Pusdiklat UPDL Jakarta, Indonesia. 11440,
[2,3]Information Systems Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Jakarta, Indonesia, 11480.
[1]radencokro@pln.co.id,[2]Ryantofani12@gmail.com, [3]gunawan.wang@binus.ac.id

ABSTRACT
By looking at what happens to the world today, we need to know that the issue of information security has become a common problem that is very important to note. Especially for organizations or companies that have a high level of risk to data and possible losses with loss of data. Many data breaches continue to occur due to accidental, deliberate and human factors that cause financial loss or company reputation. The approach towards improving behavior and culture is by applying awareness activities of how important data security information systems are in progress. This journal presents an approach to identifying factors related to human security by incorporating people into the design and implementation of information system security awareness. The author presents six steps in progress that can be done in business activities and evaluate the author's approach to the business case study. The authors' findings suggest that an information-centered approach to information security awareness has the capacity to adapt to the time and resources required for its implementation in the business, and offers a positive contribution to reducing the risk of information security through awareness of the importance of that security.

Key words: Security; Information System;

1. INTRODUCTION

By looking at what happens to the world today, we need to know that the issue of information security has become a common problem that is very important to note. Especially for organizations or companies that have a high level of risk to data and possible losses with loss of data. For a large number of internal data violations that may occur are still directly linked to human factor problems, whether intentional or unintentional. Companies that are engaged in business can no longer rely solely on processes and technologies to reduce the risk of security issue but it is necessary to consider more a process of information systems to the technology[1]. We should provide some security education and training on equality to support a common understanding of the importance of knowing the security of information systems. In a case we can usually apply the importance of confidentiality to store data integrity and have controls for reducing the occurrence of a risk. Human factors are most often actually involved in information systems security issues[2]. While as we know to run a business of human interaction is very important so that their understanding of security awareness needs to be handled effectively. People as users can also be useful for identifying threats, vulnerabilities and areas of potential risk in their given environment[3]. Therefore, in order to adjust the importance of security we need something relevant and business content observation. People are among the indicators we can incorporate into the case of the importance of knowing the information system itself, or potentially used to modify other processes and procedures or the security and purpose of risk assessment[4]. For security awareness, we must describe an approach in which manufacture and application is used to address the specific factors of human business in the importance of security. The approach here is how to use people as a tool to identify needs and objectives for data security awareness information. We have to get people integrated into a situation so we can think about how important it is about security, then the steps we take to design and implement in the six-step program the importance of information system security. In providing an overview to support the approach then begins by first considering the existing framework and communication to know the importance of security in the information system. In this case the author considers the current challenges, benefits and shortcomings, and how to use them so they can be integrated. This research will then be discussed into a process for a person-centered methodology. Integrate to help analyze and mitigate risk through adjustment of the importance of security. Testing elements with business case studies, referred to as XYZ Company, will be detailed as well. Then the observation of the application by means of the design of the importance of security requirements, which aims to reduce the problem for information system security.

2. LITERATURE REVIEW

2.1. Importance of Information System Security

Raising awareness and changing security behavior can be a challenge. Some approaches depend on fear of changing behavior, or result in lack of motivation and ability to meet unrealistic expectations, which may come from poorly designed systems and security policies[1]. The purpose of the importance of security is clearly identified and communicated. But many people find it unnecessary to trace

the internal security of guidance because users do not believe they have security issues[5][6]. The design process is tailored to the needs of the business. Consider the effectiveness of different sexes, generations or roles, focus on communicating how to achieve it, rather than dictating what should not be done [7]. Notice of violation or statement may need to be increased, for clarity in order to avoid many problems. Awareness programs should use simple rules consistent with employee behavior, offering improved perceptions of control and better acceptance of suggested behaviors. Cultural differences in risk perceptions should be considered when embedding positive security behaviors with support, knowledge and awareness [8].

2.2. Information System Security Platform

The four cornerstones of security are responsibility, trust, communication, and cooperation. The importance of information system security must be tailored to the organizational context of the company's employees, observing specific security requirements continuously for strengthening in order to instill security practices into normal routines of safe-mindedness [9]. Other similar life cycle approaches include security frameworks [10] that offer generic approaches to promote the importance of information systems data security. All this aims to organize and provide corporate action involving the right people to enter into the cycle of how to build trust about the importance of data an information system. Relevant activities and topics, then plan, run, measure and revise the program [11]. Otherwise, the Security Awareness Cycle establishes basic metrics, identifies relevant audiences, desired behaviors and high risks, and solutions to facilitate risk-reducing behavioral changes [12]. Where, the framework by Maqousi et al. [5] have similar steps, but provide a specific focus of computer-based security delivery methods. Awareness programs can also be approached as branded marketing activities that promote the security of information to employees.

2.3. Understanding Information System Security

Many of the reviewed frameworks rely on some form of data collection to understand the environment in varying degrees, societies and cultures. A typical description of the user who accomplishes the goal - can instead be used as a tool primarily within the design phase to address this area. An interesting perspective provides an approach story to visualize character descriptions using the narrative building of the story, middle and end stories[13], supported by the context of stories and scenarios [14]. When creating people, the design team tends to include a variety of roles [15] that may be started by acquiring and analyzing background information and data from multiple sources, leading to a view of the user's focus area. This view is likely to be debated, agreed upon and refined which leads to representatives of people who can be constructed in accordance with relevant supporting scenarios[13]. People must be generative and involved, using scenarios to apply them to the relevant situations. Atzeni et al. [16] provides an approach that aims to develop so that attackers can not use data collection processes, reference elicitation, affinity diagrams for problem space graphics, which help with the development of characteristics, and end with the creation of people. In short, for their successful people to be based on data relevant to their business and employees, and support the participatory focusing requirements or cooperative designing methods that focus on the user.

3. RESEARCH METHOD

While considering research on the importance of information systems data security, while there is a security approach, many focus on standard compliance topics related to the identification of specific and business-specific factors based on actual security needs of people interacting with processes and technologies to support business goals. People also offer potential security requirements to identify risks [17]. The concept of people's use for data security information systems has been discussed [3]. To align the importance of security, the authors consider it a benefit area for integrating people to identify users' specific business needs and objectives. Aims to provide means of addressing human factors related to risk security, leading to an approach tailored to security awareness activities. Human risk addressing means of risk, leading to an approach adapted to security awareness activities. From a review of the current awareness approach, the authors identify the challenges and strengths of program steps and communication approaches. The general steps and considerations should be the foundation of the methodology that the authors propose. By following the methodological steps, the authors aim to provide a specific, measurable, achievable framework, realistic and timely goals to achieve goals.

3.1. Steps

To achieve this goal, a business decision to commit must go on. Awareness Information security of information systems data should be given support and commitment. The importance of representative teams from key departments throughout the business should start, conducting meeting introductions to form teams and goals.

1. Needs

To focus on the outcomes, the activities used to derive business needs and objectives on the importance of information system data include survey and focus group assessment that is building business and security needs through culture, location, risk, roles, responsibilities and resources. The threat of the importance of current information system data should also be noted, along with issues or violations in which human behavior is likely to be the root cause.

2. Target people

Interviews are used as targets to obtain the necessary data. This step may be the most important given its dependency of integrating people as a tool for identifying human factors and security risks. This should begin by organizing interviews with a random selection of users from across the

business. Interviews are used as a basis for obtaining the data needed to build people.

3. Analyze

Critical analysis is carried out on the identified behavior and characteristics of each person. It is considered based on business needs, risks and requirements to build and prioritize the need for the importance of data information systems. Using a simple consistency of desired behavior and behavior rules can be considered with realistic expectations to integrate the needs of people context-based business risk scenarios.

4. Design and Development

The design requirements for addressing identified security risks are derived from critical analysis and topic-specific research. Methods of delivery and resources must agree to consider ease of use, scalability, interactivity, and accountability elements. Awareness involving personal-level people should be applied, which can motivate and empower employees to take an active role in the Security Information. Content requirements are specified for consistent messages delivered across multiple channels. Branding can be aggregated, creating relevant material and dilocated with organizations, goals and people, promoting Information Security to employees as a product.

5. Implementation

Timely implementation, launch strategies should be made to consider the availability of required staff and other business priorities. Delivery of customized content and communication methods around other priorities should be planned and implemented as the basis relevant to the awareness cycle should be established, and the effectiveness of certain elements of awareness activities when necessary.

6. Final Results

Stages of results and conclusions are useful for identifying the effectiveness, benefits, shortcomings, and improvements to the cycle of the importance of information systems security. Ongoing effectiveness may use feedback mechanisms, such as manual, automated and automated manual, logging and Internet logging, monitoring and tracking.

4. RESULTS AND DISCUSSION

In order to implement and test certain elements of the methodology, the authors apply the approach to the business case study called the XYZ company. The author specifically helps validate ideas that people use as a tool to address security risk factors, guiding election and customized design. The proposed process steps can be used to integrate the use of people in the importance cycle of information systems security.

1. Needs

Discussions with XYZ companies are needed for requirements and expectations, understanding the culture, and business goals. Specified related topics to be chosen theme. Social Engineering can be described as a tool to manipulate people by deceitfully performing actions or providing information (Mann, 2012) that may pass or undermine the security of other control technologies.

2. Target people

The nature of the business context is a goal-based approach that is largely adopted with some role-based elements of a person. The process for the creation of people can be seen according to Atzeni et al. [16]. In preparation for initiating the process, interview questions are made to allow data collection to leave scope for additional questions. It aims to produce relevant information from employees that describe business-related behavior and perceptions and information security. According to Yin [18], randomization is also said to help the validity of the interview data provides day-to-day insights that include the various roles and experiences in XYZ Company, demonstrating the general security-mindedness culture with positive attitudes toward XYZ Company. By doing this, the goal is to strengthen the validity of the data by providing the correct template, which enables further enhancements if necessary. This should reduce the risk of people's characteristics becoming overly diluted or deviating from their data.

3. Analyze

Companies must agree that the need for the importance of information system data applied to each person can be analyzed. Authors should offer detailed and full information to suggest that they enter into output by means of communication. This is achieved by considering how each person will act or respond to their attitudes and understandings can then be analyzed to identify weaknesses toward security. However, the person shows a good level of understanding or awareness. During the analysis this information is further considered in the cultural context, current processes and workload procedures and client types. This may help strengthen awareness needs, thereby preventing or reducing the likelihood and impact of security-based risks, and is a possible consideration for the future.

4. Design and Development

Considering personality and culture, XYZ's company determines the design that most people can accept. Then proceed to support XYZ company development to determine the upcoming cycle. For example making video how important information system data security. For example, where this may pose a risk of distrust between business and its employees. Therefore, the focus prioritizes the implementation approach agreed with the company XYZ based on people.

5. Implementation

The time required for implementation and review should be provided by creating a test time frame with XYZ companies. This implementation should also have agreed on communication methods can be primary and secondary. Much of the time the discussions needed to argue technically how to keep the information systems data security upgraded in the company by using a particular approach or technology. Therefore, it can be said that this need is still to be fulfilled, thereby increasing awareness of how important data system information.

6. Final Results

Based on the final result it is found that the time frame and business priority can be used to measure the effectiveness of how important the data security of information systems. This

suggests that regardless of gender, age or technical expertise, everyone has different attributes in terms of protecting the information system. At the employee level, people are more visible in output, but pay less attention to personality-based awareness. Whereas, at the management level, the benefit of using people as a means to identify human security risk factors is accepted as an approach to awareness of the importance of data security information systems. Based on real data the author can appreciate the benefits of the importance of security in information systems. This is proven where participants can identify with them as other employees.

5. CONCLUSION

Development and application of solutions on the importance of information systems security and testing of user design by integrating people about the importance of such information data. A review of the work, people, approach and related framework is underway to understand how such an approach can be combined. From here, a person-centered methodology is designed and largely tested by business case studies. However, his personality The outcome is generally based on more technical roles. Data collection from less technical roles provides balance The spread of business audiences will be more appropriate when fully applying this methodology in a real-world scenario. The role of individual persons can also be used to identify needs at the team or department level, or for other related purposes. Activities, the possibility of this process can be tailored to the needs of business needs, while providing flexibility to grow. It also gives XYZ Company an idea of how other updates can be delivered. The inclusion of computer-based systems training and awareness-based tools is considered a future advantage of expanding awareness. Further work is related to the long-term effectiveness of the program to improve behavior, reduce risk and embedding Security into an unconscious routine, it will also be interesting to validate its long-term effects.

REFERENCES

[1] K. Hong, Y. Chi, L. R. Chao, and J. Tang, "An integrated system theory of information security management," *Inf. Manag. Comput. Secur.*, vol. 11, no. 5, pp. 243–248, 2003, doi: 10.1108/09685220310500153.

[2] A. Kankanhalli, H.-H. Teo, B. C. Y. Tan, and K.-K. Wei, "An integrative study of information systems security effectiveness," *Int. J. Inf. Manage.*, vol. 23, no. 2, pp. 139–154, 2003.

[3] H. Tilwani, "Cloud Business Process Management & Data Security," *Int. J. Comput. Sci. Technol. Inf. Technol.*, vol. 6 (3), pp. 2089–2093, 2015.

[4] M. L. Markus and C. Tanis, "The Enterprise System Experience — From Adoption to Success," *Fram. Domains IT Manag. Proj. Futur. Through Past*, pp. 173–207, 2000, doi: 10.1145/332051.332068.

[5] A. Maqousi, T. Balikhina, and M. Mackay, "An effective method for information security awareness raising initiatives," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 2, p. 63, 2013.

[6] P. Mell, T. Grance, and others, "The NIST definition of cloud computing," 2011.

[7] S. Kraemer and P. Carayon, "Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists," *Appl. Ergon.*, vol. 38, no. 2, pp. 143–154, 2007.

[8] S. Grewal, "ISSUES IN IT GOVERNANCE & IT SERVICE MANAGEMENT - A Study of their adoption in Australian Universities," … *13th Eur. Conf. …*, 2006.

[9] C. Thuemmler and C. Bai, "Health 4.0: How virtualization and big data are revolutionizing healthcare," *Heal. 4.0 How Virtualization Big Data are Revolutionizing Healthc.*, pp. 1–254, 2017, doi: 10.1007/978-3-319-47617-9.

[10] M. Evans, K. Dalkir, and C. Bidian, "A holistic view of the knowledge life cycle: the knowledge management cycle (KMC) model," *Electron. J. Knowl. Manag.*, vol. 12, no. 2, pp. 85–97, 2014.

[11] S. Edy, W. Gunawan, and B. D. Wijanarko, "Analysing the trends of cyber attacks: Case study in Indonesia during period 2013-Early 2017," in *Proceedings - 2017 International Conference on Innovative and Creative Information Technology: Computational Intelligence and IoT, ICITech 2017*, 2018, vol. 2018-Janua, doi: 10.1109/INNOCIT.2017.8319146.

[12] S. W. Hussaini, "A Systemic Approach to Reinforce Development and Operations Functions in Delivering an Organizational Program," *Procedia Comput. Sci.*, vol. 61, pp. 261–266, 2015, doi: 10.1016/j.procs.2015.09.209.

[13] L. Nielsen, *Personas-user focused design*. Springer, 2013.

[14] S. Madsen and L. Nielsen, "Exploring persona-scenarios-using storytelling to create design ideas," in *IFIP Working Conference on Human Work Interaction Design*, 2009, pp. 57–66.

[15] C. Mendez, "The InclusiveMag Method: A Start Towards More Inclusive Software for Diverse Populations," 2020.

[16] A. Atzeni, C. Cameroni, S. Faily, J. Lyle, and I. Fléchais, "Here's Johnny: a methodology for developing attacker personas," in *2011 Sixth International Conference on Availability, Reliability and Security*, 2011, pp. 722–727.

[17] L. Browning, R. N. Gerlich, and L. Westermann, "The new HD Classroom: a 'Hyper Diverse' approach to engaging with students," *J. Instr. Pedagog.*, vol. 5, no. May, pp. 1–10, 2011.

[18] R. K. Yin, *Case study research: Design and methods*. Sage publications, 2013.