Information System Security: Human Aspects

Zaied Shouran, Tri kuntoro Priyambodo, Ahmad Ashari

ABSTRACT: Numerous organizations recognize that their workers, who are usually thought of the weakest link in information security, also can be great assets in the effort to reduce risk associated with data security. Information security has not been given enough consideration among the writing as far as the human issue impact; researchers have involved a lot of examination throughout this area. Human factors assume a noteworthy in computer security. all through this paper, we target the relationship of the human factor in information security showing the human weaknesses which can cause unintentional harm to the organization and discuss, be that as it may, information security awareness may be a major tool in overcoming these weaknesses.

Keywords: security awareness, human aspects, information security.

1 INTRODUCTION

Organizations' significant reliance on information systems (IS) needs them to manage the risks related to those systems. Today, risks associated with information security are a serious challenge for several organizations, since these risks might have dire consequences, including company liability, loss of believability, and monetary dame. The human factor has a tremendous impact on the success and failure of our efforts to secure and defend our businesses, services, systems, and information. if security loopholes are incomprehensible by the process designer, the strength of the IT system becomes a weakness which will be exploited by an offender a weakness which will be exploited repeatedly in just a small amount of your time. A major concern inside information security is the threat of social engineering attacks. Assailants utilizing social engineering try to increase sensitive information focusing on human vulnerabilities that are weaknesses in an organization's security as a result of the attributes and behaviors of people [1]. security awareness becomes an important point of human being aspects of information and technology [2]. Information security awareness can be defined as the level of comprehension that users have about the importance of information security best practices. Generally, employees in any organization have varying levels of security awareness, They are also increasingly engaging in dangerous online activities such as social networking, blogging and instant messaging g with a considerable number of them unaware of their exposure to security risks while doing so [3]. this review will explore about the security awareness, compare between the natural and intervention studies based on the previous research, also make the comparison between developed countries and developing countries because these countries have some different cultures that make different perspectives about security awareness.

- *Zaied Shouran is currently pursuing a Ph.D. degree program in Computer and Electronics Science, Department, UGM, Yogyakarta, Indonesia. E-mail: Shouran.zaied@mail.ugm.ac.id*
- *Tri kuntoro Priyambodo is currently Associate Professor of Computer Science and Electronics, Universitas Gadjah Mada - Indonesia. E-mail: mastri@ugm.ac.id*
- *Ahmad Ashari is currently Associate Professor of Computer Science and Electronics, Universitas Gadjah Mada - Indonesia. E-mail: ashari@ugm.ac.id*

The higher security awareness will impact the better practice in the human life both in the business cycles and in the government area, drawing on the fact that both information security awareness programs and safety awareness programs seek to manage risk by influencing individual behavior, we identify and analyze security-related biases from contiguous disciplines (such as behavioral economics and health and safety). We then discuss the implications of these biases on formulating risk perceptions and shaping information security behavior and finally propose a set of recommendations for designing security awareness programs so as to accommodate the traits of security decision-making through HAIS model. Also, will add the new analysis about human aspects such as demography, psychography, and self-efficacy and its effect on security awareness. key strategies that can be used as a reference for eGovernment information security [4]:

1.1 Aspects of Data Types and Services

Sorting / classifying the types of data/information that will be used in eGovernment services. If the data/information to be displayed/exchanged lead on data privacy and confidential nature, it must be ensured that there is infrastructure which could guarantee the security both in terms of the eGovernment service provider and from the user community services.

1.2 Policy Aspects

It requires establishing integrated policies such as the concept of a single sign-on for all eGovernment services. Also, It needs a clear policy regarding the application on the concept of the security system and control toward every level of the user. The application of the concept of General security policy that in the current status as security measures and contingency plans.

1.3 Aspects of Infrastructure and Technology

It needs support and commitment to the implementation of a number of security standards such as ISO 27001: 2009 for computer security and the ISO 14443 standard for interoperability. It requires a deeper study on the adoption of the latest security technologies such as context awareness to improve comfort in the security aspect. Also needs the policy to control the quality of security that is applied to various types of technology device which is used widely in the community.

1.4 Human Aspect

It needs continuing education to educate about the importance of keeping the privacy of personal identity that is stored in the Smartphone. Need an education in choosing the various type of computer device that technologically supports security system implemented in eGovernment. In the following, we

focus on the five human factors determined by [5] [6] that have serious implications to end users' behavior :

1.4.1 Lack of Motivation

[7] believe that "Employees need to be motivated to adopt secure behaviors and practices, and management needs to be able to identify what motivates their staff". According to Koh et al. motivation occurs when security issues are shared and clients are engaged with basic leadership so as to pursue security strategies.

1.4.2 Lack of awareness

Lack of awareness is related to a lack of general knowledge about Attacks. Common examples of a lack of awareness could be the following: Users do not know how to see a sign of a spyware on their computer, and how important is to specify a strong password, they cannot protect themselves from identity theft, and social engineering and they do not know how to control the access of others to their computer.

1.4.3 Belief

The term conviction could be translated as the Users' Risky Belief for CIS.[8] led a subjective investigation of clients' view on data security and displayed different wrong convictions. For instance, Albrecht Sen underlined that users usually "felt their behavior was in compliance with the documented system due to the belief that the rules and guidelines are common sense". Common examples of risky belief are the following: Users believe that the installation of anti-virus software is not crucial for their information, or on the other hand, they are prepared to tap on a connection while they get an email from obscure people.

1.4.4 Behavior

The term behavior could be deciphered as the users' hazardous behavior or the loss of counteractive action behavior. Such behavior could be made by a few variables. [8] claims that "Documented requirements of expected information security behavior have little impact alone on user behavior". It is worth of referencing the accompanying finish of Albrechtsen: "The users consider a user-involving way to be much more powerful to impact user awareness and behavior".

1.4.5 Inadequate Use of Technology

Indeed, even the best innovation can't prevail with regards to taking care of information security issues without consistent human collaboration and the successful utilization of this technology. Regular instances of improper employment of technology are the accompanying: making unapproved reconfiguration of systems, getting passwords of others, recovering unseemly information.

1.4.6 Computer security risks

Information security breaches can be categorized in a number of different ways. [5] in view of a few examinations performed by different specialists exhibited 13 assaults which cover the majority of the PC security chance variables, and in the long run, characterized 9 factors (that) can cover all risks as main factors. These factors are Excess Privilege, Error, and Omission, Denial of Service, Social Engineering, Unauthorized Access, Identity Thief, Phishing, Malware, and Unauthorized Copy.

2 INFORMATION SYSTEM SECURITY AWARENESS

Information system security is strongly related to the concept of risk. According to [9], risk is an event that may negatively affect the accomplishment of business objectives. The International Organization of Standardization (ISO) defines risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets. The impact of the relative severity of the risk is proportional to the business value of the loss or damage and the estimated frequency of threat. In general, the principal reasons for providing IS security may include protection of resources, maintaining management control, ensuring safety and integrity, implementing policies and laws, and attaining operational advantages and economies. Security failures can be costly for any institution. Losses may be suffered as a result of the failure or as a result of the cost incurred for recovery, followed by more cost to secure systems and prevent further failures. It is worth noting that managers and employees also tend to think of IS security as a second priority compared with their own efficiency or effectiveness matters because these have a direct and material impact on the outcome of their work [9]. [10] have investigated different aspects of cybersecurity, and they asserted that although information security and cybersecurity have substantial overlap, these two concepts are not totally analogous. The general definition of information security comprises availability, integrity, and confidentiality. Cybersecurity incorporates extra measurements, which stretch out past the formal limits of information security, incorporating human in their own ability and society on the loose. It tends to be harmed or influenced; while this is not really the situation with data security, where harm is constantly circuitous. The security objectives cannot be met by technical and procedural protection only; an educated security attitude of employees, management, and external IT users and partners is also vital to ensure effective IS security. As highlighted in [11] , previous studies on IS security have focused on software for detecting IS security abuses, the measures for preventing IS security abuses, perceptions of IS security adequacy. IS security planning models for management decision-making? Except for a couple of interpretive investigations, these examinations will in general disregard authoritative variables that may somewhat clarify the degree of IS security manhandles. IS security approaches can be classified into two categories. Studies which consider IS security awareness to mean attracting users' attention to IS security issues, or studies which consider IS security awareness to mean users' understanding of IS security and, optimally, committing to it [12]. The need to promote IS security standards within an organization requires IS security awareness training. All the users should be aware of disciplinary actions resulting from non-compliance with the organizations IS security procedures. IS awareness training and education is an essential part of defending IS security [13]. A survey reported in [14] confirmed the mediating role of employees' organizational commitment to work motivation and job performance. Offering training is one of the factors that increase employees' level of satisfaction. [3] and [15] show that the proper information security behavior, besides the technological aspects of information security, mitigates the risk of information security breaches in organizations. Previous studies have revealed that employees' information security awareness plays a vital role in mitigating the risk associated with their behavior in organizations. [16] divided users into

two groups home and organizational users and they asserted that information security awareness plays a vital role in both groups. This study has also revealed that delivery methods and enforcement components play important roles in this domain. Information security awareness can stem from employees' experience in this domain. Information security experience leads to comprehension, familiarity, as well as the ability and skill to manage incidents [17]. The awareness program should communicate to users the organizations IS security policies and make users aware of the risks and potential losses. [18] take into consideration the user's role when presenting a model for implementing and enhancing the culture of IS security. The model focuses on three levels of organizational behavior: the organizational level, the group level, and the individual level. The model suggests that the organizations are security culture must be improved by taking human behavior into account. It also suggests that each user should be informed, through IS security awareness, of his role in protecting information assets. [19] discussed the implementation of continuous IS a security awareness training program as part of the corporate asset protection program. [20] argue that organizations should introduce IS security awareness and make their ethical policy clear to their employees and ensure that strong deterrents are in place. [21] argues that the incompetence of users who underestimate the dangers inherent in their actions represent the biggest IS security problems. An efficient IS security awareness program can overcome this problem. The organizations are better prepared to screen their information security awareness position, their limits and the day by day weights influencing the organization, therefore enabling them to configuration better-coordinated strategies and procedures to encourage safe operating limits [22]. The information security focus areas included in this organization information security policies are password management; use of email, the Internet and social networking sites; mobile computing; and information handling. However, the maturity levels of these elements varied among focus areas due to a lack of information security policies awareness and compliance among users [23].

3 DISCUSSION

When discussing security, the problems that occur are related to convenience. Security and convenience are issues faced the most by each institution that implements a security system. In this case, there is a security paradox, "The more convenient we tend to make things, the less secure they are; conversely, the more secure we make things, the more inconvenient it becomes" [24]. People, in many cases, are the last line of defense against threats like malicious code, discontent workers, and malicious third parties. Human vulnerabilities are a giant source of information security risks and thus the results of breaches in information security end up in individual and company losses and even to crimes. Raising security awareness is that the key to limiting the number of breaches caused by human weaknesses. Most organizations have quite valuable data and services in the control of individuals who do not appear to be aware of its value, the importance of maintaining its protection, or the implications if that information is exposed. in line with [25], people will only facilitate in preventing security breaches, if they are aware of the risks, and are taught secure behaviors as a part of their traditional work training. in spite of that, a typical hindrance to the creation of an environment wherever management and workers are operating towards the identical info security goals is that the apathy of workers [26]. the security objectives cannot be met by technical and procedural protection only; an educated security perspective of employees, management, and external IT users and partners is additionally important to make sure effective IS security. each organization should promote a culture in which employees share the responsibility of defending the company against attack [25]. we have to take into consideration that once employees feel committed to their job, they're additional likely to feel glad about the job and be motivated to perform at their best. A survey according in [28] confirmed the mediating role of employees' organizational commitment to work motivation and job performance. giving training is one of the factors that increase employees' level of satisfaction. However, employees' training on security risks and measures against attacks ought to be fastidiously organized. [6] indicate that instructions or orders can only impact behavior if they are consciously accepted by each employee so translated into specific goals. once a person perceives that the achievement of a goal is not potential, commitment diminishes significantly. thus, it should be ensured that information security goals are perceived as attainable to make the sure commitment. Policies need to be readily accessible or available to employees to ensure that they will not be ignored. It ought to be clear to all employees what their actual role and responsibilities are regarding security. An organization must address all possible human errors while writing IS because such errors can be critical for any organization if not handled competently Major causes of the occurrence of human errors include lack of knowledge or skills related to IS; thus, managing human error in any organization is vital, and errors must be taken as a serious threat. As such, it is essential to introduce IS to all stakeholders, including end-users, of an organization to ensure compliant behavior [23]. Responsibility, trust, communication, and co-operation are said to be the four cornerstones of an engaging security culture. Using an approach that motivates and empowers employees to play an active role in security is important towards achieving awareness and positive behaviors. Awareness output should be tailored to employees' organizational context, addressing specific security needs on an on-going basis to reinforce awareness, embedding security practices into the normal routine of security-minded culture [29].

4 CONCLUSION

The security of sensitive data is only as strong as the weakest link, which often turns out to be the human user and not the firewall. This makes the users' awareness of the data created as well as the risk connected with data breach critical. Based on the discussion the focus has always centered on training users about specific risk areas. Awareness subsequently shifts from an understanding of complex security procedures to an understanding of organizational pressures. An attempt was created during this study, to assemble and clearly determine the human weaknesses causing security problems and provide suggestions on ways to overcome them. The implication of this study is that information security awareness is that the key to mitigating security threats caused by human weaknesses. Organizations must cultivate and maintain a culture wherever positive security behaviors are valued; they have to instill in their culture that security begins and ends with every person involved with their infrastructures, their businesses, and their services. The challenges related to

information security that employees face on a day after day must be understood and resolved. this suggests that security functions should be substantive and as very little intrusive as possible. additionally, security, policies must be comprehensible and straightforward to locate. Employees' education about the importance of security awareness ought to be a priority of the organization.

5 REFERENCES

[1]. A. McCormac, K. Parsons, M. Butavicius, and L. Ferguson, "Human Factors and Information Security: Individual, Culture, and Security Environment," Sci. Technol., no. DSTO-TR-2484, p. 45, 2010.

[2]. R. Samans and M. Hanouz, The Global Information Technology Report 2016 Preface. 2016.

[3]. J. Abawajy, "User preference of cyber security awareness delivery methods," Behav. Inf. Technol., 2014.

[4]. T. K. Priyambodo and D. Suprihanto, "Information security on eGovernment as information-centric networks.," Intl. J. Comput. Eng. Res. Trends, vol. 3, no. 35, p. 365, 2016.

[5]. N. Badie and A. H. Lashkari, "A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP," J . Basic . Appl . Sci . Res, vol. 2, no. 9, pp. 9331–9347, 2012.

[6]. E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The Human Factor of Information Security: Unintentional Damage Perspective," Procedia - Soc. Behav. Sci., vol. 147, pp. 424–428, 2014.

[7]. M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, and D. Calic, "Factors that Influence Information Security Behavior: An Australian Web-Based Study," in Human Aspects of Information Security, Privacy, and Trust, 2015, pp. 231–241.

[8]. E. Albrechtsen, "A qualitative study of users' view on information security," Comput. Secur., vol. 26, no. 4, pp. 276–289, Jun. 2007.

[9]. ISACA, "IT Standards , Guidelines , and Tools and Techniques for Audit and Assurance and Control Professionals," Professional Ethics. 2010.

[10]. R. Von Solms, J. V. N. & security, and undefined 2013, "From information security to cyber security," Elsevier.

[11]. W. Ben, L. Judith, and W. S. Glen, "This document is downloaded from DR-NTU , Nanyang Technological," 2014.

[12]. D. L. Goodhue and D. W. Straub, "Security concerns of system users: A study of perceptions of the adequacy of security," Inf. Manag., vol. 20, no. 1, pp. 13–27, Jan. 1991.[13] R. Anderson et al., "Measuring the cost of cybercrime Motivation A framework for analyzing the costs of cybercrime Fitting the estimates into the framework," 2012.

[13]. P. T. E. M. (IEEM), 2011 IEEE, and undefined 2011, "Work motivation and job performance of frontline employees: the mediating role of organizational commitment," ieeexplore.ieee.org.

[14]. N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," Comput. Human Behav., vol. 38, pp. 304–312, 2014.

[15]. E. Kritzinger, "Cyber Security for home users: A New Way of Protection through Awareness Enforcement," pp. 1–15.

[16]. N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," Comput. Secur., vol. 53, pp. 65–78, 2015.

[17]. M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," IEEE Commun. Surv. Tutorials, vol. 15, no. 1, pp. 446–471, 2013.

[18]. G. L. Kovacich and E. P. Halibozek, The manager's handbook for corporate security : establishing and managing a successful assets protection program. Butterworth-Heinemann, 2003.

[19]. A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," Comput. Secur., vol. 34, pp. 47–66, 2013.

[20]. S. Allam, S. V. Flowerday, and E. Flowerday, "Smartphone information security awareness: A victim of operational pressures," Comput. Secur., vol. 42, no. March 2018, pp. 55–65, 2014.

[21]. N. A. G. Arachchilage and S. Love, "A game design framework for avoiding phishing attacks," Comput. Human Behav., 2013.

[22]. F. H. Alqahtani, "Developing an Information Security Policy: A Case Study Approach," Procedia Comput. Sci., vol. 124, pp. 691–697, 2017.

[23]. T. K. Priyambodo and Y. Prayudi, "Information security strategy on mobile device based egovernment," ARPN J. Eng. Appl. Sci., vol. 10, no. 2, pp. 652–660, 2015.

[24]. P. Kearney, Security : the Human Factor. IT Governance Pub, 2010.

[25]. K. Thomson and J. Van Niekerk, "Combating information security apathy by encouraging prosocial

organisational behaviour," Inf. Manag. Comput. Secur., vol. 20, no. 1, pp. 39–46, 2012.

[26]. P. Kearney, Security: The human factor. 2010.

[27]. P. Trivellas, "Work motivation and job performance of frontline employees: The mediating role of organizational commitment," in 2011 IEEE International Conference on Industrial Engineering and Engineering Management, 2011, pp. 1878–1882.

[28]. Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S, and Sasse, AM, "Awareness is only the first step," A framework for progressive engagement of staff in cybersecurity, techreport, Hewlett Packard Enterprise.,(2015).