Need for Compliance With Information Security Policy In Universities: a Preliminary survey

1ST Angraini
School of Computing
Faculty Engineering, Universiti Teknologi Malaysia,
Johor, Malaysia
Department of Information System,
Faculty Science and Technology,
Universitas Islam Negeri Sultan Syarif Kasim,
Pekanbaru, Riau
angraini@uin-suska.ac.id

2nd Rose Alinda Alias
Department of Information System
Azman Hashim International Business School, Universiti Teknologi Malaysia
Johor Malaysia
alinda@utm.my

3nd Okfalisa
Department of Informatics Engineering,
Faculty Science and Technology,
Universitas Islam Negeri Sultan Syarif Kasim,
Pekanbaru, Riau
okfalisa@gmail.com

***Abstract*— Information security has become a significant problem for the use of information technology, especially for universities that have a lot of data. Information security policy is one solution to ensure data security. However, compliance is a classic problem in information security that face by an organization when applied policy. Effect of users who do not comply with information security policies both from internal and external. Research on this subject was surveyed to find out the leadership perspective on compliance with information security policies and to explore the university's need to evaluate user compliance. This research was conducted in a survey using a closed-ended questionnaire given to manager level of the university. The data processed with descriptive statistics. This research founded management realized the importance of compliance with information security policies to reduce information security incidents. Universities need appropriate model to evaluate information security policy compliance. This understanding will help improve predictions of the impact of complying with information security policies.**

Keywords—information security, policy, user compliance, universities, preliminary survey.

I. INTRODUCTION

Increasing threats and information security attacks are a problem for organizations to secure their data. According to Kaspersky's report, malicious code and viruses infect 55.51% of computers in the world during 2016 [1]. And increasing every year, as reported by Symantec in 2017, malware has increased by 80% and multiplied by 200% compared to the previous year. Growing threats in information security that target various types of organizations that have sensitive data, including universities [2,3]. Therefore, the university began to realize the importance of creating information security policies. Information security policies are expected to manage information assets. Information security policy document that contains regulations, rules for users to use, handle, and store data to be safe. Information security policies ensure information and information technology assets are safe with unique procedures to support the organization's goals and objectives [4]. However, still founded employees not comply with that regulation and against the policy. Therefore, increased threat to information security. Previous research found there is numerous causes employees noncompliance with information security policies. Aurigemma (2012) discussions that employees consider the violence of information security as collective behavior, even if it causes financial loss for the organization [4] and increase risk of information security that adverse effects on business processes [5]. There are still possible information security threats because information security threats can come from internal organizations [6,7]The risk of information technology has consequences that can threaten corporate responsibility, loss of credibility and monetary issues [8]. Internal threats come from individuals, and if it occurs continuously, they will interfere with organizational activities[9,10]. Therefore, it is necessary to know the reasons for the inefficient application of information security policies in the university. This research is a preliminary study that aims to determine the causes of non-compliance with information security policies to understand the opinions of users on information security. This paper has six sections starting with the introduction, comprehensive literature review, results, discussion and conclusion

II. LITERATURE REVIEW

Information security policies is a document to ensure information security based on top management's vision related to key strategic business objectives within the scope of management goals and contain basic requirements. Information security policies include rule, guidelines, and control to secure information asset [11]. Information security policy contains regulation used to create an organization’s IT security rule, particular issues, and system policy to address individual systems [12]. The University Information Security Policy aims to ensure that all information systems and information technologies are used in protected areas adequately protected. The university is an organization with various activities and type of users. It becomes a challenge for universities to ensure organizational information, which saved, processed and disseminated with information technology.

Events caused density, high dependence on the accuracy, integrity, and availability of technology-based information resources [13]. Misuse of information technology resources is a significant threat in the information security stage. Compliance with information security policies in institutional higher education is relatively under-examined with less validated evidence. [14]. Some previous studies have empirically tested in universities. However, models can are applied in various type of organization because of university use as case studies. Alshare (2018) uses universities as a case study to examine factors that have an impact violation on universities' employee information security policies based on deterrence theory, neutralization theory, and justice theory. His research findings affirm that procedural justice, distributive justice, severity and fairness of sanctions, privacy, responsibility, and culture of organizational security affect information security violations at universities [15]. Research conducted by Putri (2014) founded information security policy has a significant impact when employees use their personal devices to access organizational resources. The results of this study indicate that the efficacy of responses perceived by employees and perceived perceptions positively affect employees' intentions to comply with security policies. The assessment of perceived security threats was found low, encouraging the intention to comply [16].On the contrary, the threat of autonomy that is felt because the security policies that are enforced negatively affect the employee's intention to comply with security policies. Researchers also found that the costs handled by employees related to compliance behavior positively affect employee perceptions of threats to individual freedom.

Furthermore, Hina (2016) measures the awareness of users to comply with information security policies using surveys with a Likert scale. The results found users realized they exposed to security threats if they did not comply with information security policies [14]. Most models tested in universities aim more at testing theories or developing theories to find factors that influence behavioral intentions to comply with procedures. Different results obtained when the experiment applied because several researchers used different methods, a different number of samples and different user characteristics. Lack of models examinees to evaluate or measure compliance using the variables they find. Future research needs more in-depth study to create models that can determine user compliance in the context of the university.

III. RESEARCH METHODOLOGY

This study conducts to confirm the research problem is a problem that occurs in reality. A preliminary examination is a process of collecting various initial information related to the research plan either from the field or library, which is carried out to explore the problem more systematically or intensively as an introduction before carrying out the procedure for further research. Survey uses a written questionnaire or formal interview to gather information on the backgrounds, behaviors, beliefs, or attitudes of some people. This research will test the assumptions that management believes users always adhere to information technology security policies, especially at universities. This opinion because of the university considered as an educational institution and not have crucial data. universities necessary consider with information security policy Compliance because they are giving a lot of number of information technology services provided by universities [17]. A study was undertaken by giving -questionnaires consisting of 12 closed-ended questions to policymakers from several universities who gathering at Indonesia association of higher education in informatics and computing event.

Questionnaires were delivered to policy-makers directly to avoid misconception. Respondents who participated in this preliminary study were as many as 55 participants consisting of university leaders, heads of IT departments, and academics from private and public universities in Indonesia. Detail of respondent describes at fig.1

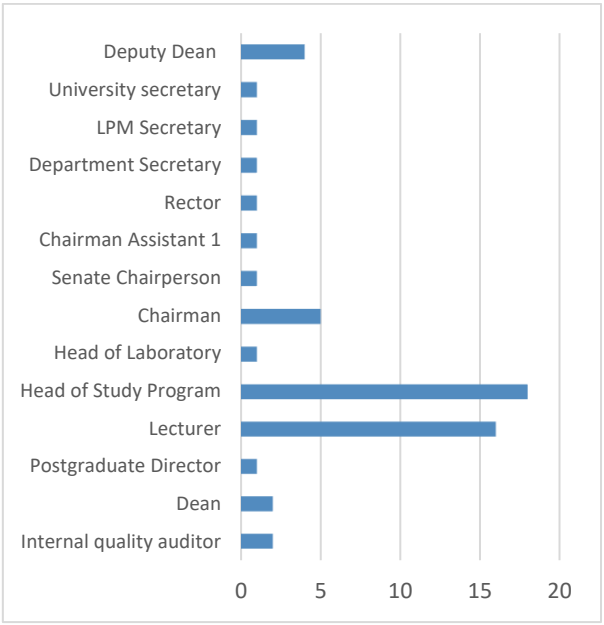

Fig.1.Respondent demographic

The distribution of respondents in this research dominated by lecturers and heads of IT departments. Lecturers become respondents because they have been involved in developing information security policies. Other respondents came from management who engaged in developing, implementing and overseeing policy implementation. After data collection, continually with description result from a survey. Result explained using the graphic to representative data and better understanding.

IV. RESULT

The results of the survey will be explained based on the questions given. The first question is, "Q1. What do you think about the implementation of information security policy at your university?" Data from the survey shows that the implementation of information security policies in universities has become a proper implementation.

The majority of universities consider they have implemented policies well. The data shows only 3 of the 55 universities that do not have information security policies at their institutions, and ten universities have very well implemented information security policies.

Complete data regarding the implementation of information security policies can be seen in fig.2

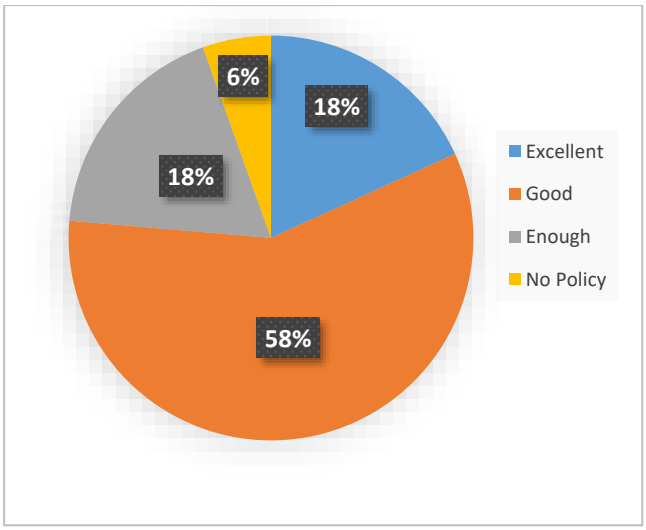

Fig.2.Data finding for question 1

Answers from the questionnaire questions Q1 said as many as 53% had implemented an information security policy. However, evidence of the application of security policies is not able to provide information security policy documents. The implementation of policies is still not well documented. Especially for private universities and universities that don't have a good reputation. While for universities that have been excellent in implementing information security policies, they say that they cannot provide policy documents because of its confidential documents. The second question is, "Q2. Does university socialize the information security policies?". Three-quarters of respondents said their universities always socialize the policies they make to improve user compliance. However, there is finding as many as 13% of universities do not disseminate their policy. Next question (Q3) was related to the previous question about user compliance. Data finding almost user will comply with the procedure if they do appropriate socialization. Fig.3 describes the data from question number 2 and number 3.

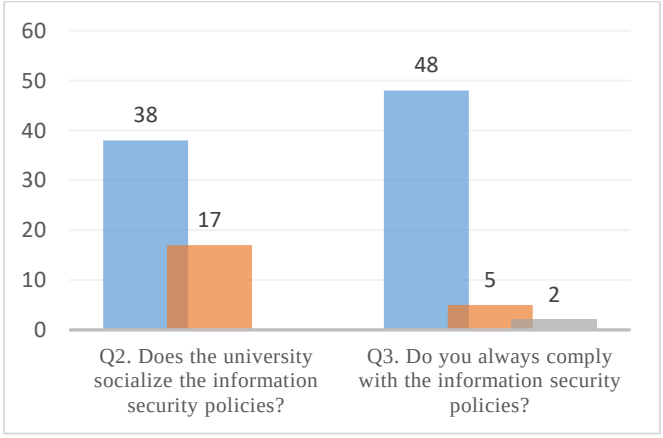

Fig.3 Data finding for question 2 and 3

The next question relates to the impact of compliance with information security policies. The fourth question is whether the user ever ignores information security policies, the answers given are 37 respondents who have never ignored information security policies. Whereas when asked whether they had ever received an incident caused by non-compliance, the answers given were almost balanced, namely 53% never and 47% answered ever. One of the fatal errors in information security management was not aware of the organization information security policy [18]. Therefore, it is essential to know whether users ignore or care about information security policies. The study found that there was a contradiction between the user's concern and the occurrence of the incident. Complete survey results presented in fig.4.

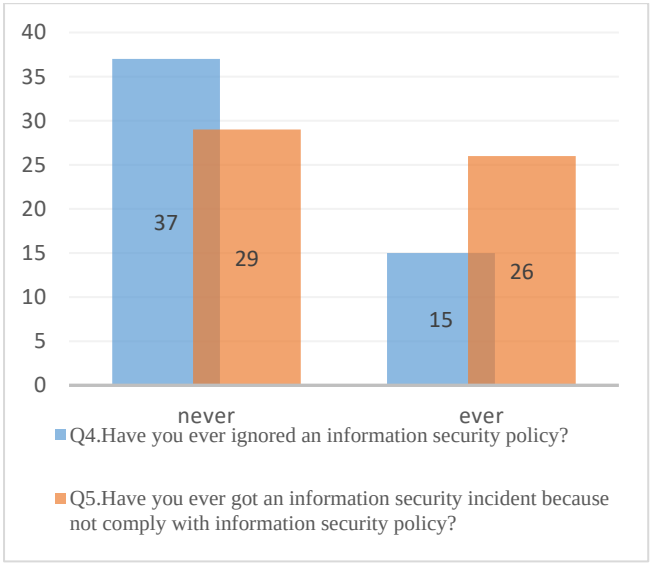

Fig.4.Data finding for question 4 and 5

The University is conscious of incidents occurring from non-compliance with information security policies. Therefore, on the subject of the 6th questionnaire asked what incidents are often experienced by users in the use of computers. The results showed that from 7 events, the results obtained almost balanced at two answers. The highest incidence is a virus, followed by viruses and malware. During hardware and software, the damage is below 10%. Fig.5 presents a graph of the incident that occurred when the user did not comply with the information security policy.

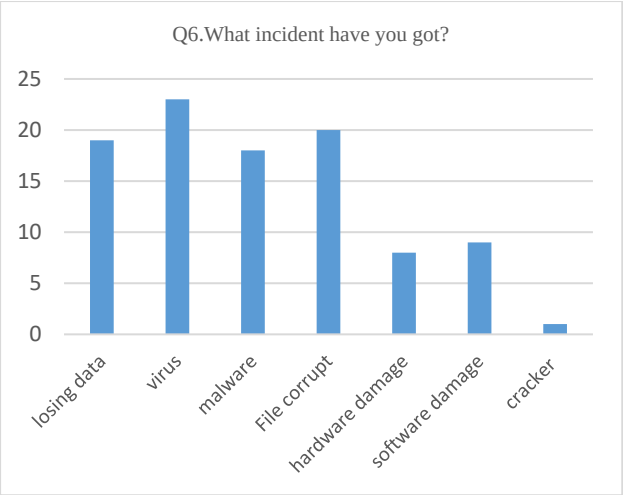

Fig.5.Data finding for question 6

Every information security incident occurs, a user can take many actions the survey shows 41% user selects perform self-repair the damage that occurred, while 33% would report the incident to the IT department, and the other just asking about the handling of the problem to the technician. The complete results of the survey about user actions if an incident occurs can be viewed in fig.6

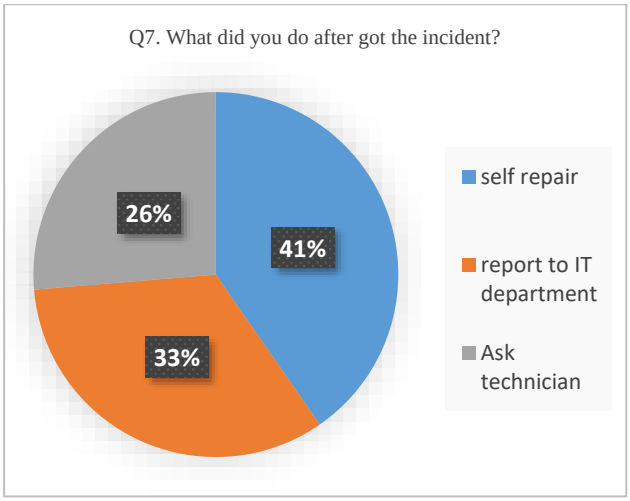

Fig.6. Data finding for question 7

After identifying the incident that occurred due to non-compliance with the information security policy, then it is necessary to understand whether the policymakers know about the importance of complying with the information security policy. The survey shows that there are two answers obtained, namely critical and essential. Nearly three-quarters of respondents know that met with a necessary procedure, even as many as 35% said user must give more attention to information security policy because it's critical. The overall percentage can describe in Fig.7

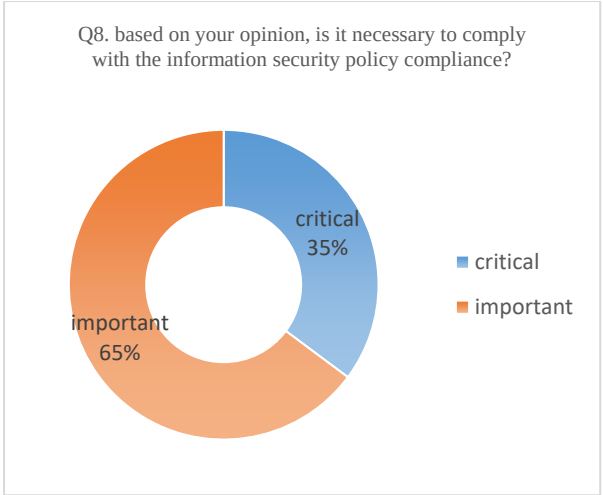

Fig.7. Data finding for question 8

The last four items are questions about policymaker's opinion regarding compliance with information security policies. Management realizes the importance of always complying with information security policies so that almost 95% know the statement. Periodic evaluations also need to be done to determine the level of compliance with information security policies, as many as 57% say universities always conduct a regular assessment. But when asked a question about whether the university cares about users who are still obedient to the policy, 40% pay little attention. This data is contrary to the next question about the university's commitment to implementing information security policies, which is equal to 83% feeling the university commits to a policy. This information can be seen further in fig.8

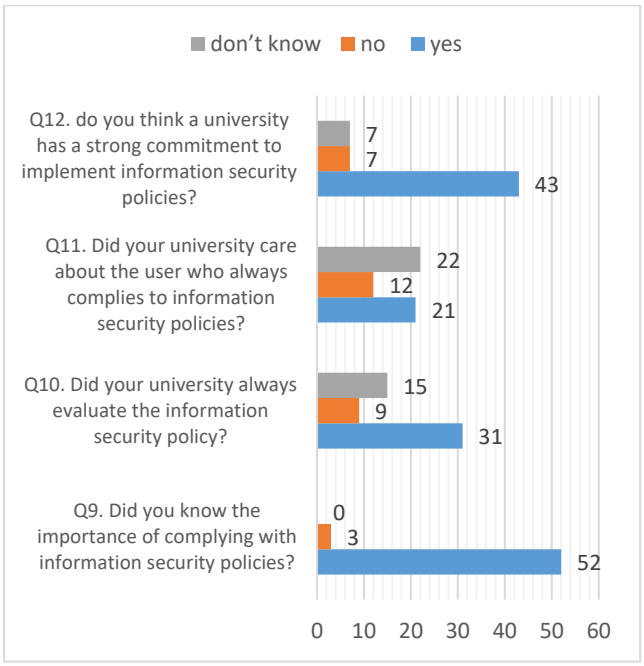

Fig.8.Data finding for question 9,10, 11 and Q12

The results of the initial survey conducted on some policymakers at the university explained descriptively. From these results, some essential points can be a concern that can be used to analyze further research.

Important aspects need to be considered an evaluation of the university, the impact of user non-compliance with information security policies, and the level of university awareness of users who adhere to information security policies. Security policies must continuously be reviewed and updated regularly by considering changes in circumstances, environment, changing needs in the business context and identified risks [19].

V. Discussion

The public university in Indonesia as an educational institution that manages large numbers of student data such as personal information, financial data, and academic data. The number of students who are thousands with various sensitive data in information systems that need to be secured. Universities have amount information technology resources and access given to the public and increase the risk for universities [20]. The implementation of the preliminary survey using closed questions gets results that support the research problem, namely the lack of university attention to information security policies. Some issues have found in the study about the application of information security policies. There is a difference in understanding the concept of compliance with information security policies in several universities. Information security interpreted as a technical problem rather than a managerial problem. However, based on observations, not all universities have an information security policy document. Information about security rules is given based on incidental. The results of the study indicate that there is still low user awareness of information security policies. This shows the contradiction of the answers given by respondents. One of them when the question about whether there was an incident that occurred if the user always obeyed the information security policy if the user has implemented the policy fully should the lower incidence rate even decrease. Therefore a program to increase program security awareness needs to be applied in the organization and an understanding of the importance of compliance and instill the principles of social psychology to improve program effectiveness [21].

In other hands, The educational system has not been preparing the user to deal with the impact and behaviors of the digital world [22]. Moreover, Higher Academic institution with weak policies in information security creates threats for university data. [23]. The public university in Indonesia faces a problem with a security threat. The increasing number of internet users, an industrial revolution, and the changing business processes using information technology must be accompanied by policies that ensure sensitive data is secure. Evidence of compliance with information security policies in higher education institutions relatively poorly examines and without validated. University needs to focus on developing a comprehensive information security policy compliance framework as an information security response effort [14].

VI. Conclusion

The purpose of this study is to determine the importance of user compliance with information security policies. This research has found that policymakers generally apply information security policies without being accompanied by instruments to assess the level of user compliance with the policy. One of the more significant findings that emerged from this study was that there was policy implementation without being accompanied by written documents, and there were still a few universities that had standards in information security policies.

These studies have sought to improve our understanding of the importance of information security policies. A generalization of these results is subject to certain limitations. For example, respondents are only from the middle to top management level. Therefore that the perspective obtained is an ideal viewpoint according to the leadership. Although the current study is based on a small sample of participants, these findings suggest a more in-depth study of factors that influence user compliance with information security policies in universities. This finding provides the following insight for future research to find a model of user compliance with information security policies for universities. Another further research needs to be done is to determine the level of user compliance with information security policies.

References

[1] Kaspersky. Kaspersky security buletin Overall Statistics for 2016. 2016.

[2] Symantec. Internet Security Threat Report - ISTR. Symantec [Online] 2017;22:77.

[3] Symantec. ISTR Internet Security Threat Report. Internet Secur Threat Rep 2018;23.

[4] Aurigemma S, Panko R. A composite framework for behavioral compliance with information security policies. Proc. Annu. Hawaii Int. Conf. Syst. Sci., 2012, p. 3248–57. doi:10.1109/HICSS.2012.49.

[5] Razilan M, Kadir A, Norwahidah S, Norman S, Rahman SA, Bunawan A. Information Security Policies Compliance among Employees in Cybersecurity Khalid S . Soliman International Business Information Management Association (IBIMA). Proc. 28th Int. Bus. Inf. Manag. Assoc. Conf., 2017.

[6] Wiant TL. Information security policy's impact on reporting security incidents. Comput Secur 2005;24:448–59. doi:10.1016/j.cose.2005.03.008.

[7] Safa NS, Maple C. Human errors in the information security realm – and how to fix them. Comput Fraud Secur 2016;2016:17–20. doi:10.1016/S1361-3723(16)30073-2.

[8] Bulgurcu B, Cavusoglu H, Benbasat I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Q 2010;34:523–48. doi:10.1093/bja/aeq366.

[9] Furnell S. Enemies within: The problem of insider attacks. Comput Fraud Secur 2004;2004:6–11. doi:10.1016/S1361-3723(04)00087-9.

[10] Magklaras GB, Furnell SM. A preliminary model of end user sophistication for insider threat prediction in IT systems. Comput Secur 2005;24:371–80. doi:10.1016/j.cose.2004.10.003.

[11] BS ISO/IEC. ISO 27001 - Information Technology, Security Techniques, Information Security Management Systems, Requirements, 2005.

[12] NIST. Glossary of Key Information Security Terms [NISTIR 7298 Rev 2]. 2013. doi:10.1016/0735-6757(85)90039-7.

[13] Doherty NF, Anastasakis L, Fulford H. The information security policy unpacked: A critical study of the content of university policies. Int J Inf Manage 2009;29:449–57. doi:10.1016/j.ijinfomgt.2009.05.003.

[14] Hina S, Dominic DD. Information security policies: Investigation of compliance in universities. 2016 3rd Int. Conf. Comput. Inf. Sci. ICCOINS 2016 - Proc., 2016, p. 564–9. doi:10.1109/ICCOINS.2016.7783277.

[15] Alshare KA, Lane PL, Lane MR. Information security policy compliance: a higher education case study. Inf Comput Secur

2018;26:91–108. doi:10.1108/ICS-09-2016-0073.

[16] Putri F, Hovav A. Employees' Compliance with BYOD Security Policy: Insights from Reactance, Organizational Justice, and Protection Motivation Theory. Twenty Second Eur Conf Inf Syst 2014:1–17.

[17] Kyobe M. Towards a framework to guide compliance with IS security policies and regulations in a university. Proc 2010 Inf Secur South Africa Conf ISSA 2010 2010. doi:10.1109/ISSA.2010.5588651.

[18] Von Solms B, Von Solms R. The 10 deadly sins of information security management. Comput Secur 2004;23:371–6. doi:10.1016/j.cose.2004.05.002.

[19] Calder A, Watkins S. IT GOVERNANCE AN INTERNATIONAL GUIDE TO DATA SECURITY AND ISO 27001/ISO27002. SIxth edit. United Kingdom: Kopan Page; 2015.

[20] Katz FH. The effect of a university information security survey on instruction methods in information security. Proc. 2nd Annu. Conf. Inf. Secur. Curric. Dev., 2006, p. 43. doi:10.1145/1107622.1107633.

[21] Thomson ME, Solms R von. Information security awareness: Educating your users effectively. Inf Manag Comput Secur 1998;6:167–73. doi:10.1108/09685229810227649.

[22] Phippen A, Ashby S. Digital behaviors and people risk: Challenges for risk management. Adv Ser Manag 2013;11:1–26. doi:10.1108/S1877-6361(2013)0000011005.

[23] Ayyagari R, Tyks J. Disaster at a University: A Case Study in Information Security. J Inf Technol Educ Innov Pract 2012;11:85–96.