Proc. 1st International Conference on
Machine Learning and Data Engineering (iCMLDE2017)
20-22 Nov 2017, Sydney, Australia
ISBN: 978-0-6480147-3-7

Information security training and awareness program: An Investigation

Roshan Dhakal[1], Rafiqul Islam[2] and Champake Mendis[3]
[1]Student, School of Computing and Mathematics, Charles Sturt University,Wagga Wagga, NSW, Australia
[2]Lecturer, School of Computing and Mathematics, Charles Sturt University,Wagga Wagga< NSW, Australia
[3] Lecturer, Computing in Mathematics, University of Melbourne, Parkville, VIC, Australia

Email: droshan_2005@yahoo.com;mislam@csu.edu.au;cmendis@csu.edu.au

Abstract

Information security training and awareness program is a bottom line in preventing the information security incidents in an organization. The success factor of this program would be unknown unless its efficiency is measured. Prior to implementing the information security training and awareness program, organization management should identify the organizational needs, metrics to measure the efficiency of the program and update the activities in the program. Information security training and awareness program teaches the employees how their knowledge, attitude and behaviour affect organization's overall performance. This paper is not proposing any specific information security products, but giving practical suggestion to organizational management and users regarding information security. This paper also proposes that it's everyone's responsibility to secure organization's information system. This paper measures the success factor of the information security training and awareness program and ensures organization management that investment in such program is valuable in long-term. This paper discussed on research methodology, outlining the experiment and statistical analysis and measuring the effectiveness of information security training and awareness program. This paper further analyse on some other factors that contributes in making training and awareness program effective and also provide suggestion for future research.

Keywords: training and awareness program, metrics, knowledge, attitude and behaviour

1. Introduction

Today information technologies are all reliant on users and information security is all about the user's behaviour rather than technical measures. Users planned actions or accidental actions can tempt undesirable results which information security experts to prevent. Regardless of the promotion about the requirement of information security products from stakeholders, there are numerous sensitive information security, a performance that is not and could not be computerized. Information technologies are designed to permit an information security in a long run, which depends upon the successful employment and undertaking those technologies by qualified users. This signifies that organizations are heavily dependent upon the users in order to carry out the safe environment. Employees are still believed to be the weakest link in an organization and are the biggest threats to organizations. Organizations should implement enough policy to ensure that their employees are getting proper knowledge on organizational information security policy and procedures (Stephanou & Dagada). The aim of educating and training users is to make sure that the user implements essential policy and procedures and also user are not abused or users do not mishandle the organization's information security policy.

According to Sans (Russell, 2002), the aim of the information security training and awareness program is to teach users about their roles and responsibilities in securing confidentiality, integrity and availability of an organization's information and properties. Therefore, information security is not just about the responsibility of information technology or any information security department, but it is the responsibility of all users. So it is necessary to know by every user how to secure the organization's information system and also what happens when users fail to do so?

According to ABC news (Edwards, 2015), more than three-quarters of a million Australian populations (3.1% of the total Australian population among the age group in between 25-34 years) have been a victim of identity theft. And according to the Australian Bureau of Statistics (Identity Theft, 2016), one-fifth of identity theft victims have been encountered same incidents again and again in previous years (Braue, 2014). The common way that identity theft happens in Australian is through phone calls, messages, email and internet, door to door salesperson, etc. Among these victims around half percentages does not know how their personal details have been collected.

It is now clear that information security training and awareness acts, as the first line of defence for any organization which brings down the organization's information security threats and risks into the acceptable level. And today every organization has its own organization information security policy and procedures and training and awareness program. But how does the organization know that the training and awareness program they are implementing is achieving the goals unless measures the effectiveness of training and awareness program (Stephanou &Dagada). The main purpose of this paper is how the efficiency of information security training and awareness program is measured in the real computing environment.

Furthermore, this paper tries to find the success factor of the training and awareness program. This paper also assists organizational management to decide whether the training and awareness program that has been implemented is the right or needs to reassess (Measuring Outcomes). After gathering the information and knowing the effective methods, an organization can decide which area needs more attention and focus so that ongoing funding would be supplied. This paper is structured as follows: Section 2 represents Background; Section 3 represents Motivation; Section 4 represents Related Work; Section 5 represents Methodology; Section 6 represents Finding and Discussion; Section 6 represents Conclusion.

2. Background

Measuring the user behaviour is anonymous that cannot be considered entirely. User's thinking level, understanding level and the aptitude of transforming and confronting is not same. Therefore, to combine users with all these attributes, there is only one formal document which is known as information security policy and procedures (Brodie, 2008). There could be confusion that information security policy and procedures regarding job performance (which means that information security policy and procedures do not teach others how to do the job, but it does teach how users can perform their job safely and securely) (Giovanni, 2015). Moreover, information security policy and procedures also teach users about the result to arise from doing the job inappropriately, how to report any incidents and users' rights in an organizational information system (Maqousi, Balikhina, & Mackay, 2013). In information security education, training and awareness program, there are three attributes: information security education which teaches the users on organizational information security policy and procedures, information security training trains users how doing the job safely and securely and information security awareness which is designed to change the performance of the users (Stephanou & Dagada). All three attributes have the same importance according to the need of organization and it would be unethical to isolate any of these attributes from the information security training and awareness program (Ally, 2015). There are some other motivational factors that encourage this research to be carried out and are briefly discussed below:

i. Improper management:

When there is no support from organization management, information security training and awareness program are always unsuccessful. Moreover, there is ignorance by senior managers regarding information security training and awareness program and also there is no specific budget for those programs. In some organizations, the management isolates the need of organization and implements the training and awareness session. This kind of practice of management believed that organization has implemented the best training and awareness program but does not deliver the desired result and blaming either employees or the training and awareness program organiser (Chelsa, 2002).

ii. The inappropriate way of delivering the message:

Delivering the message and information about training and awareness program plays a vital role in success of the program. Many researchers and organizations believed that online videos, presentation and lectures are the effective tools for training and awareness program, but online presentation and videos are often ignored by the users and classroom lectures are boring. Computer-based training method and instructor based training method are two types of training method, but the user should be given freedom to choose the training method otherwise rather than focusing the training session user will be more focusing on completing the training session and getting the completion certificate.

iii. Implementing the incorrect metrics to measure the efficiency:

Prior to implementing the information security training and awareness program, the three factors need to be considered: what needs to be measured; how to measure and when to measure? Which will be the correct methodology for data collection while measuring the user's knowledge, whether the survey will be the best method for data collection or the interview (Schroeter, 2014)? It has been also stated that one survey questions or an interview question do not decide or measure the knowledge, attitude and performance of people (Chen, Li, Hoang, & Lou, 2013). Which statistical theory best suit for analysing the collected data? How frequently or what would be the time interval for collecting the data again for the periodic review of measuring the efficiency of information security training and awareness program (Kahraman)?

3. Motivation

Employees are considered as the biggest threats to an organization and are the main reason for security infringement. Prior to implementing information security training and awareness program, organizations must discuss with organizational users regarding data and information security and what benefits will be to the organization and its users after implementing the information security training and awareness program (Herold, 2010). Highly trained and aware employees are always the basis of secure and reliable that every organization is insisting. So implementing effective and worthy information security training and awareness program helps in improving the employee's performance, which at the end improves the performance of an organization (Kadel, 2004). Generally, in most of the organizations, it is believed that the information technology department is responsible for any information security incidents (Karjalainen, 2011). But this paper clarifies the misunderstanding that the information technology department of an organization is only responsible for information security incidents and other department and employees are isolated from the security incidents, but it is every employee role and responsibility to address those incidents (Allen, 2013).

The initial purpose of the information security education, training and awareness program is to give away a clear message that employee is familiar with their own terms (Hight, 2005). Information security training and awareness program must concentrate on how to protect the organization and its asset, why it is necessary to protect that and what happens if fail to protect the organizational information and asset (Knapp & Ferrante, 2015). Information security training and awareness program should draw user's interest on organization's information security policy and procedure which helps in developing the information security culture in an organization and reaffirming users about information security policy, its results and user's responsibility in security policy (Khan, Alghathbar, Nabi, & Khan, 2011).

The main purpose of this paper is to investigate and measure the efficiency of information security training and awareness program. This paper helps in developing the continuous steps in judging the employees in an organization which is possible only through measuring the efficiency of information security training and awareness program (Lavrakas, 2010). Organizational users who are directly involved in information security system are more probable advantageous from this paper (Elkhannoubi & Belaissaoui, 2016). Thus, investing in information security training and awareness program indicates that there will be a probability of less information security incidents and make certain that the business status is operating as anticipated (Safianu & Twum, 2016).

Based on the above scenario, this paper addresses the following research problems.

How measuring Information Security Education Training and Awareness framework is effective in minimizing the organizational information security incidents?

To achieve the best solution the research question has been divided into following sub research questions are listed below:

1. How information security training and awareness framework are evaluated and its success factor is measured?
2. How employee's behaviour affects the overall information security in an organization?
3. How employee's behaviour will be changed after implementing information security training and awareness program?

4. Related work

The literature review involves in recent and previous literature, investigate and analysis for verification. The current literature review comprises of information security training and awareness factors and explaining the employee’s information security related incidents and its outcomes. The literature review concentrates on re-evaluating the confidentiality, integrity and availability of information security attributes. This literature also re-examines the information security training and awareness program and organization’s information security policy from an employee’s position. This literature review is inherent from the limitation of previous research which instigates the source for this paper. This literature review rationally explores the relationship between organizational information security incidents, employee’s behaviour on organizational information security and the necessity of information security education, training and awareness program (Poepjes & Lane, 2012).

According to Nurul (Molok, Chang, & Ahmad), organizations are experiencing more information security incidents from organizations employee’s negligence and lack of knowledge, but this lacks the study of information security incidents from external attack and management point of view. Agata (McCormac, Parsons, & Butavicius, 2012) agrees that investing in information security is the investment in technological aspects and training and awareness session as well. Hekkala (Hekkala, Vayrynen, & Wiander, 2015) insists that information security professionals are only responsible for information security incidents in an organization, but by saying so do not signify that other employees are isolated from the information security incidents. Information security incidents in an organization do not only disrupt the organization’s information system but also compromises the employee’s privacy and security. Straub and Welke (Straub & Welke, 1998) agree that information security training and awareness program are frequently ignored by the organizational management and even by employees as well. Information security training and awareness program should not only focus on educating and changing the behaviour of employees but also should focus on its return on investment in the organizational business. Stephen (Stephanou & Dagada) agrees that most of the information security incidents arise in an organization from employee’s lack of knowledge. To address this issue, the organization must implement information security training and awareness program and make it part of organizational information security policy. The outcomes dramatically reduce the information security related incidents by half in the first phase, but this is not the total solution as information security training and awareness is a continual process.

According to Kreicberga (Kreicberga, 2010), organizations are implementing the information security training and awareness program without realizing the need of organization and also without knowing the employee’s level of understanding. In addition to this, the organization implements the inappropriate metrics to measure the efficiency which results in zero outcomes. Therefore, this literature addresses all of the above-mentioned issues and attempts to fulfil the gaps that have been addressed.

5. Methodology

5.1 Data collection

The survey was carried out online through survey monkey and the participants were mostly from the United States. The required candidates for this survey were around 100 but only 55 responded. Among them, approximately 65% were above the age of 45 and the remaining were in the range of 18- 45. In comparison to gender, female participants were more than a male. The Quantitative research method was implemented as a research methodology because the survey was considered as a data collection method. The survey questions were designed to measure employee’s knowledge and behaviour and how employees respond to the information security incidents. The survey questions were categorised into three different sets: first set of survey questions for Information Technology professionals, second set for all employees and management and third of the control group (here control group refers to the group of employees who are participating in the data collection but they would not be receiving any kind of training and awareness program). Survey questions were prepared and were approved by the principal supervisor and co-supervisor for the verification. In every set of questions employee's knowledge and behaviour in relation to information security is measured. The questions were multiple choices and one more option was added in case if participants would like to express their own opinion. The survey questions that were asked to participants were authorized and certified by qualified and knowledgeable experts in the area of social science research as well as information technology security professionals. All three set of survey questions were handover to participants on the same day and allowed two days to complete the survey.

5.2 Research process

The initial survey questions were designed to know the employee's level of understanding regarding the information security education, training and awareness and information security policy. After the survey questions were designed then the survey questions were uploaded into survey monkey for the survey. The requested amount of participants was 100 but only 55 responded and the survey was closed by survey monkey team after 2 days. Closed-ended questions were asked in this group and one more option was added if participants want to express their own opinion. The participants can choose the options from three multiple choices and if they have any opinion in regards to the survey question then they can select the additional option and write down their opinion. The authenticity as apparent by the participants needs to be discussed in terms of meaningful replies in relation to the component of the area of the research participants were enquired about. The response requires various sources of participant's intelligence which also involves in observing their values, cultures and the method they explain and know this.

The second set of questions was designed after analysing the result of the initial survey. In the initial survey participants level of knowledge and understanding in relation to information security was measured. Based on those result the survey questions were designed. If the data was not collected through online mode then there needs to implement some sort of information security training and awareness program to the participants but it was not possible in the online method of data collection. Therefore, there is a need to implement new techniques for conducting information security training and awareness session, which includes some useful and real-time scenario for the participants in every question and participants, has to respond based on those scenarios. The purpose of introducing the scenario is to make participants aware of the information security policy and information security education training and awareness program. The second survey questions will be implemented after analyzing the result of the initial survey. The result of this survey will be compared with the initial survey and result will be analyzed.

The third set of questions will be same as the second set, but the only difference is that there will be no scenario. The survey will be conducted after a couple of month's time interval after conducting the second survey. The purpose of this survey is to measure whether participants are keeping in mind the information security policy and applying it in the workplace or is participating closing the eyes to information security policy and procedure. This survey also measures the number of information security incidents that had happened in the past and have occurred recently.

This research also surveys another group known as the control group. In the control group, participants will be invited for the initial survey and final survey within the time interval of 3 months, but the participants would not be participating in any information security related training and awareness program. These survey results were then compared to survey results from the other two groups who received the information security training and awareness. The purpose of this comparison is to know whether changes in organizational security culture forces or motivates the employees to change their behaviour or not. If the change in the organizational culture motivates the employees for changing their behaviour by sticking with the organizational information security policy then there will be the minor necessity of information security education training and awareness program.

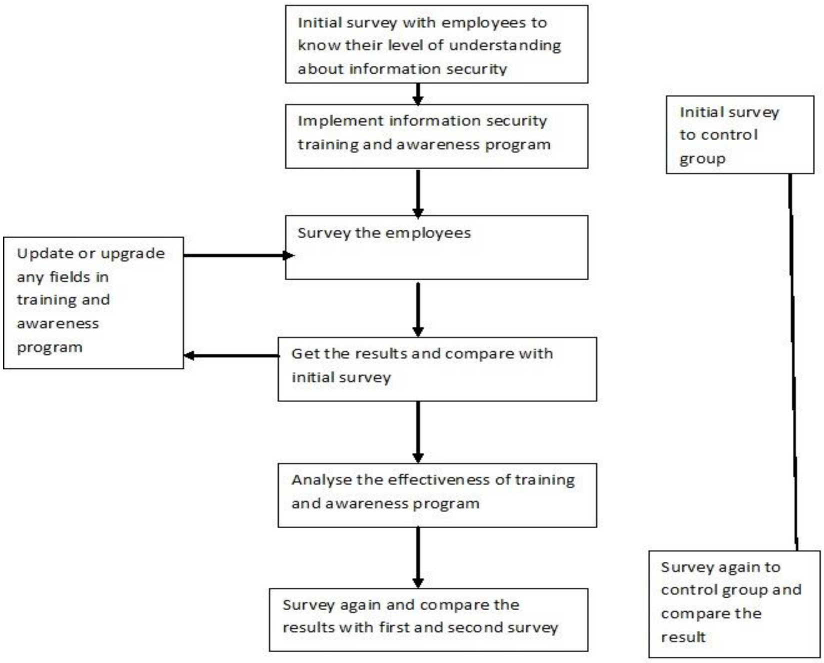
Initial survey with employees to know their level of understanding about information security
Implement information security training and awareness program
Survey the employees
Update or upgrade any fields in training and awareness program
Get the results and compare with initial survey
Analyse the effectiveness of training and awareness program
Survey again and compare the results with first and second survey
Initial survey to control group
Survey again to control group and compare the result

Figure 1: Data collection process

6. Data Analysis

6.1 Initial survey analysis:

ANOVA test and F-ratio test were implemented in this research for comparing the independent means of the survey grades and marks of the participated employees.

Null hypothesis H0: while comparing the results and conclusion for an initial survey of participants prior to participating in information security training and participants from control groups, there will be no major variation statistically.

Alternative hypothesis H_1: while comparing the results and conclusion for an initial survey of participants prior to participating in information security training and participants from control groups, there will be major variation statistically.

Table 1: Means of initial survey of both group

	N	Mean	Standard Deviation	Standard Error	95% confidence interval for Mean	95% confidence interval for Mean
					Lower bound	Upper bound
1	55	7.69	1.015	0.155	7.40	8.04
2	55	8.26	1.130	0.164	7.95	8.60
Total	110	8.00	1.112	0.118	7.78	8.24

Here both group means the first group who will receive the information security training and awareness program and a second group who won't receive any sort of information security training and awareness(Kim & Homan, 2012) (Zaiontz, 2017).

Table 2: F-ratio of initial survey of both group

	Sum of squares	Df	Mean Square	F	Significance
In between groups	7.105	1	7.105	6.050	0.015
Within the groups	98.785	84	1.171		
Total	105.89	85			

In the initial survey, there is substantial variation statistically in both groups at 0.015 level of significance. The F ratio value is equal to 6.050 with the significance level of 0.015 which is less than the critical value, accepts the alternative hypothesis (Kim & Homan, 2012) (Zaiontz, 2017).

6.2 Final survey analysis:

Null hypothesis H0: while comparing the results and conclusion of participants who participated in information security training and participants who did not take part in information security training and awareness program, there will be major variation statistically.

Alternative hypothesis H_1: : while comparing the results and conclusion of participants who participated in information security training and participants who did not take part in information security training and awareness program, there will be no major variation statistically.

Table 3: Means of final survey of both group

	N	Mean	Standard Deviation	Standard Error	95% confidence interval for	95% confidence interval for

					Mean	Mean
					Lower bound	Upper bound
1	55	7.95	1.041	0.180	7.59	8.32
2	55	8.06	0.800	0.108	7.85	8.30
Total	110	8.03	0.896	0.0969	7.84	8.21

Table 4: F-ratio of final survey of both group

	Sum of squares	Df	Mean Square	F	Significance
In between groups	0.305	1	0.308	0.374	0.540
Within the groups	69.500	84	0.816		
Total	69.805	85			

The table illustrates that there is no major variation statistically in between the participants who participated in information security training and participants who did not take part in information security training and awareness program scores at 0.05 level of significance. The significance level of 0.54 was equal to the value of F-ratio 0.374 and the critical value is not more that level of significance the null hypothesis could not be rejected.

6.3 Efficiency in between training methods

In order to discover the efficiency in between the training methods, five training methods have been selected 1: Instructor based training method 2: Computer-based training method 3: Group discussion 4: Online discussion forum and 5: Another method. Participants were asked to choose one of five training methods. Below is the chart that illustrates which the best training method is.

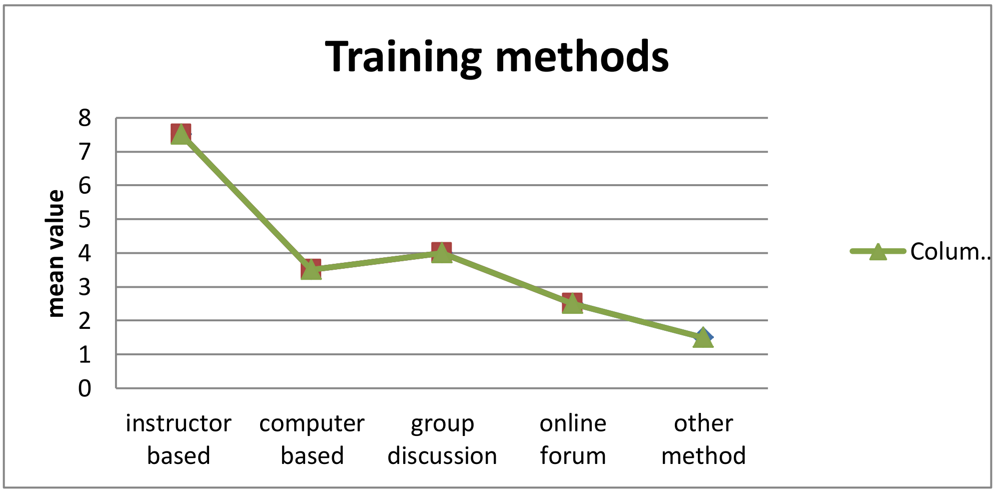

Figure 2: Chart showing the various training methods

7. Finding and discussions

It is clear in this paper that information security training and awareness program is proficient in changing the knowledge, behaviour and attitude of the employees in an optimistic manner. While discussing the training mode, there is not a major difference in training mode according to participant's responses. Despite the benefits and limitations of training methods, organization management should consult with participants, which training method they want rather than forcing them for one method. The organization should look after participant's convenience in delivering training method rather than management because, at the end, participants need to be beneficial for the training. This paper also reveals that participants are now more concerned about information security and organizational information security policy. Participants now believe that it is also their responsibility to ensure the safety and security of organizational information system and also participants are motivated to report any information security incidents. The outcomes further explain that organizational management should play a significant role in either continuing the training and awareness program or implement one-time training and awareness program and whether outsourcing the training and awareness program or create one by consulting with information security professionals. The outcomes also make clear that investment in information security training and awareness program assists in gaining valuable revenue in the long term by increasing the return on investment.

This paper contradicts that one question in the survey does not necessarily measure the performance of the employees. For the success of information security training and awareness program, organization management should ensure that all participants understands the organization information security policy and procedure and apply them in the workplace. But still, how is management measure that participant understands the training and awareness program? One of the effective measures is that let the organizational management be the listener and current participant be the trainer for the new participant. This method assists management in measuring how current participants present the awareness session to the new participants? Has the current participant fully known about the organization's information security policy and procedure and is he/she is being able to make it clear to the new participants about the importance of the organization's information security policy and procedure?

This paper also explores that information security training and awareness program should be reviewed in order to maintain its effectiveness. Prior to implementing the information security training and awareness program did the organization cross investigate the program with other organizations? Was the program successful in that organization? Did the program increase the ROI (return on investment) and changed the performance of organization's security culture? The purpose of reviewing the information security training and awareness program is to analyse whether the training and awareness program that was implemented achieved the goal. Furthermore, the reviewing process involves in critical thinking of what has been succeeded and how to make progress in the future.

It has been stated that successful information security training and awareness program is proficient in changing employee's knowledge, performance and attitude which makes an optimistic transformation in organization security culture, but this is not the only reason for successful information security training and awareness program. There are other factors that need to be investigated and analysed further. The collected data should be analysed through other statistical methods for reliability and validity of the study.

Further study should be carried out on how age factor affects in the training methods. Separate analysis should focus on why the younger generation is much interested in computer or web based training rather than instructor based training and group discussion and why middle age group participants are more focusing on the instructor based training method and group discussion. While analysing the training methods, age factor plays a significant role. Young generations prefer computer based training method while middle age group prefers the instruction based and group discussion based training method. The capable of critical thinking, understanding and quick learning is high in the young generation and this feature makes young employees to adjust in computer based training method rather than sitting in lecture for hours. Moreover, young generation is quick to adapt to change and technology is changing. But some organizations could say that it is not necessarily important that age factor affects on the training methods. It also depends on the organizational culture and environment and the employee background as well. For example, it would be beneficial for information security professionals to implement the computer based training methods as they are familiar with the information security terms and acronym. For the normal employee, instructor based training methods would be advantageous because there needs to be someone who can explain any technical words and terms and group discussion would be beneficial for the management people as they can discuss about the problem and find out the right solution. This also assists them in decision making in the future by sharing the experiences and ideas during the group discussion.

As the technology is growing the new threats and challenges to information security is also emerging. Therefore, further study is needed to investigate on new threats and challenges. Rather than blaming the employees, organizations should find out the weakest point of the organization through penetrating testing and ethical hacking. Also,organization should perform phishing attacks, and social engineering to the employees to know how employees react to those incidents. Further investigating needs to be conducted on phishing attacks and penetrating testing.

8. Conclusion

In conclusion, this research paper had examined the research questions of information security awareness and training plan with the purpose of adding up the theory and procedures. This research paper also explores the various types of outlook that are implemented by information security researchers and professionals concerning these essential features of security awareness. This research paper also explores that implementation of security policy and measuring the awareness level in employees. This research paper addresses the gaps that have been identified in the literature review. This paper also addresses the problem which encourages for this research. Therefore, this paper verifies that it would beneficial for the organizational users who are beginning and new to organizational information security system.

References

Allen, J. H. (2013, 5 13). Security Is Not Just a Technical Issue. Accessed via https://www.us-cert.gov/bsi/articles/best-practices/governance-and-management/security-is-not-just-a-technical-issue on 11 October 2017.

Ally, S. (2015, 03 25). Three dimensions of information systems. Accessed via www.slideshare.net/suleymans19/three-dimensions-of-information-systems on 11 October 2017

Braue, D. (2014, 5 7). Cost of Australian IT security incidents rises despite improving information sharing. Accessed via www.cso.com.au/article/544481/_cost_australian_it_security_incidents_rises_despite_improving_information_sharing/ on 6 October 2017

Brodie, C. (2008, 6 30). The Importance of Security Awareness Training. Accessed via www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013 on 9 Ocotber 2017

Chelsa, R. (2002, 10 25). Security Awareness Implementing an Effective Strategy. Accessed viawww.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418 on 13 October 2017

Chen, H., Li, J., Hoang, T., & Lou, X. (2013). Security Challenges of BYOD: a Security Education, Training and Awareness perspective. Accessed via minervaccess.unimelb.edu.au/bitstream/handle/11343/33347/300316_2013_Li_SETA.pdf?sequence=1 on 10 October 2017

Edwards, M. (2015, 4 15). Identity theft: More than 770,000 Australians victims in past year. Accessed via www.abc.net.au/news/2015-04-14/identity-theft-hits-australians-veda/6390570 on 5 October 2017

Elkhannoubi, H., & Belaissaoui, M. (2016, 10). User's Behaviors Influence on Cybersecurity Strategy Effectiveness. Accessed via www.researchgate.net/publication/309560700_User's_Behaviors_Influence_on_Cybersecurity_Strategy_Effectiveness on 10 October 2017

Giovanni. (2015). 10 Reasons Why Employees Need Security Awareness Training. Accessed via www.expertsecuritytips.com/employees-security-education-awareness-training on 13 October 2017

Hekkala, R., Vayrynen, K., & Wiander, T. (2015). Nordic Contributions in IS Research. 6th Scandinavian Conference on Information System,SCIS 2015 , 5-50.

Herold, R. (2010). Why Information Security Training and Awareness Are Important. Accessed via www.infosectoday.com/Articles/Security_Awareness_Training.htm 11 October 2017

Hight, S. D. (2005). The importance of a security, education, training and awareness program (November 2005). Accessed via www.infosecwriters.com/Papers/SHight_SETA.pdf on 9 October 2017

Identity Theft. (2016, 4 19). Australian Bureau of Statistics: Accessed via www.abs.gov.au/ausstats/abs@.nsf/0/90A4971FB1FC0992CA2579E40012060A?opendocument on 5 October 2017

Kadel, L. A. (2004, 3 24). Designing And Implementing An Effective Information Security Program: Protecting The Data Assets Of Individuals, Small And Large Businesses. Accessed via www.sans.org/reading-room/whitepapers/hsoffice/designing-implementing-effective-information-security-program-protecting-data-assets-of-1398 on 8 October 2017

Kahraman, E. (n.d.). Evaluating IT security performance with quantifiable metrics. Accessed via pdfs.semanticscholar.org/1a28/bab7edab76c234984dd9a3c96eb76d661d3b.pdf on 10 October 2017

Karjalainen, M. (2011, 10 28). Improving employee's information systems (IS) security behaviour: Toward a meta-theory of IS security training and a new. Accessed via jultika.oulu.fi/files/isbn9789514295676.pdf on 9 October 2017

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management Vol. 5(26) , 10862-10868.

Kim, P., & Homan, J. V. (2012). Measuring the effectiveness of information security training: A. Issues in Information Systems, 13 (1), 215-224.

Knapp, K. J., & Ferrante, C. J. (2015). Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations . Journal of Management Policy and Practice vol. 13(5) , 66-80.

Kreicberga, L. (2010). Internal threat to Information security. Accessed via epubl.ltu.se/1653-0187/2010/050/LTU-PB-EX-10050-SE.pdf on 11 October 2017

Lavrakas, P. J. (2010, 5). An Evaluation of Methods Used to Assess the Effectiveness of Advertising on the Internet. Accessed via www.iab.net/media/file/Evaluation_of_Internet_Ad_Effectiveness_Research_Methods.pdf on 9 October 2017

Maqousi, A., Balikhina, T., & Mackay, M. (2013). An effective method for information security awareness raising initiatives. International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 2 , 63-72.

McCormac, A., Parsons, K., & Butavicius, M. (2012, 4). Preventing and Profiling Malicious Insider Attacks. Accessed via www.dtic.mil/dtic/tr/fulltext/u2/a563808.pdf on 8 October 2017

MeasuringOutcomes. (n.d.). Strengthening non profits: Accessed via http://www.strengtheningnonprofits.org/resources/guidebooks/MeasuringOutcomes.pdf on 12 October 2017

Molok, N. N., Chang, S., & Ahmad, A. (n.d.). Disclosure of organizational information on social media: perspectives from security managers. Accessed via www.pacis-net.org/file/2013/PACIS2013-108.pdf on 8 October 2017

Poepjes, R., & Lane, M. (2012). An Information Security Awareness Capability Model (ISACM). Accessed via http://www.ro.ecu.edu.au/cgi/viewcontent.cgi?article=1136&context=ism on 13 October 2017

Russell, C. (2002, 10 25). Security Awareness - Implementing an Effective Strategy. Accessed viawww.sans.org/reading-room/whitepapers/awareness/security-awareness-implementing-effective-strategy-418 on 5 October 2017

Safianu, O., & Twum, F. (2016, 6). Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. Accessed via www.researchgate.net/publication/304066003_Information_System_Security_Threats_and_Vulnerabilities_Evaluating_the_Human_Factor_in_Data_Protection on 12 october 2017

Schroeter, J. (2014, 2 12). Measuring the effectiveness of your security awareness program. Accessed via www.csoonline.com/article/2134334/metrics-budgets/measuring-the-effectiveness-of-your-security-awareness-program.html on 9 October 2017

Stephanou, A., & Dagada, R. (n.d.). The impact of information security awareness training on information security behaviour: The case for further research. Accessed via www.citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.1461&rep=rep1&type=pdf on 5 October 2017

Straub, D. W., & Welke, R. J. (1998). Coping with System Risk. Security Planning Models for Management decision MIS Quarterly, Vol. 22, No. 4 , 441-470.

Zaiontz, C. (2017). Two within subjects factors. Accessed via www.real-statistics.com/anova-repeated-measures/two-within-subjects-factors/ on 13 October 2017