Influence of Human Factors on the Adaptation of a Security Culture: Evidence from a leading IT company operating in Sri Lanka

S. V. Gammampila
Cardiff Metropolitan University
shehan.gammampila@live.com

T. L. Sajeevanie
University of Sri Jayewardenepura
tlsajeevanie@sjp.ac.lk

Abstract

Despite the immense research on information security, the human factor has been neglected in most of the research communities with majority of the security research leaning towards the technological aspects of information technology system. With the rapid development and introduction of new technological solutions to combat the growing threat on information security, the human factor is still subject to continuous attacks. The human factor plays a significant role in security aspects. Behavior of an individual is greatly influenced by the user's perceptions on security risks and understanding, whereas, these are directly linked to organizational culture and its environment. This research evaluates the potential human factors influencing a security culture in an organization through the creation of a hypothesis. The research was conducted in a leading software organization to understand the level of established security culture also to identify area that have shown improvements. The study focused on employees to validate two main concepts of human factors and adaptation of a security culture. Data was collected through a structured questionnaire where 90 participants responded and the data was evaluated using the Likert scale. The results have shown that human factors have a significant role in adapting a security culture for an organization and that relationship between the depicted human factors and adaptation of a security culture is moderately strong and positive in context.

Key words: Data security, human factors, information security, organizational culture, security culture

Introduction

With the rapid growth in technology, numerous technical advances are regularly take place ensuring that business environment is secure and thus minimizing the possibility of security breath. However, this does not guarantee a secure environment where the management could entirely be dependent on the technical controls placed in an organization. Therefore, information security cannot be described as merely a technical problem but an issue belonging to the human factor. Computers and systems are operated by people and it directly influences how an individual interacts with information systems which is often detrimental. Evidently, the sole implementation of IT (Information Technology) security controls is unlikely to prevent

security breaches. Organizations need to adopt and maintain a culture where positive behaviour of people towards security is emphasized and valued. This means the education and awareness of the importance of security play a vital part in an organization to incorporate behavioural training. How an employee reacts to information security is dynamic and complex. Individual differences, personality, norms, beliefs and cognitive abilities are some of the factors which may impact the decision towards information security by an employee. These are important considerations to assess and identify why an individual makes certain decisions and behaviour.

Despite the significant investments on information security in organizations Cybercrime is still prevalent with massive breaches reported daily. According to IBM (International Business Machines) cost of data breach study, average cost for lost or stolen data is at $148 million whereas the average total cost of data breach is at $3.86 million, which is a 6.4% annual increase (Phonemon Institute LLC, 2018). Over a quarter, 28% of these breaches are due to insider threats (Verizon Enterprise, 2018). According to the Insider Report, 2018 by Cybersecurity Insiders, 47% of attacks were deliberate while 51% were accidental (Cybersecurity Insiders, 2018). These are evidence to ascertain the uncertainty and significance of the impact which may cause an organization to lose substantial credibility, revenue, market share, reputation and may even cause a business to shut down. One of the major concerns of the security world is the threat of social engineering techniques used by the perpetrator in an attempt to obtain sensitive information of an organization which is subsequently used maliciously to gain access to company data, disrupt work, block accessibility to company data or demand a ransom for release. Social engineering poses a real threat to any organization. To mitigate the risk of exposure, all employees needs to be aware of potential attacks but must also be taught on how to identify a social engineering attempt and chances of becoming a target.

The concern of employees from IT industry has increased the attention among researchers (Nilashini and Sajeevanie, 2018). This study focuses on how the human factors affect the journey to combat the uncertain, growing risk of information security by adapting a successful security first culture and make the selected organization identify the importance of the same. Based on the secondary data gathered and empirical evidence, it is reasoned that organizations focus on the human aspects of Information Security which is not adequate and that the investment on human factors to achieve a substantial security focused culture among its employees is insufficient. Despite the well-known “Humans are the weakest link in Information Security” and the undesirable behaviour of system users which is a direct reflection of the organization's culture, most of the organizations still continue to invest in the area of technology infrastructure without the focus on the most important asset of a company, which is Human Resources. Hence, the problem statement of this study is “To what extent lacks of focus on human factors directly affect the security culture which has resulted in increasing incidents of unintentional data leakages, breaches, number of high security incidents, open vulnerabilities and insider threats in the selected organization”. The objectives of the study have been identified as; exploring and determining relevant theories related to human factors directly affecting the security culture of an organization, examining and determine the level of adaptation of the security culture in selected organization through an unbiased study, identifying the relationship between human factors and adaptation of a security culture and

providing recommendation and improvement areas to enhance the security culture in IT based organizations. The results of this study would be vital to the leadership of the selected organization as well as the industry to determine the human factors influencing the security posture of an organization and understand the needs for improvement. Subsequently, the corrective actions and enhancements to improve their processes, security posture, awareness, and adopt a security first culture in the organization based on the outcomes will be determined.

Literature Review

Despite significant budgetary investment in tools, controls and technology to fight against rapidly evolving cyber security attacks, threats and data breaches, there's very little investment considered by many organizations on human factors affecting a security culture. Information security is merely a technical issue but a much broader subject which requires the attention of all members of an organization. Among the cyber security community, it is a well-known fact that "Humans are the weakest link in information security". Undesirable behaviour reflects the existing culture of the organization towards information security and the responsibility lies within (Nasrin and Habibi, 2012). There's definitely a gap between the desirable state on an organization's security expectations and the current status. In spite of the continuous increase of security incidents and involvement it has with humans, companies speak of cyber security investment on the technology front foregoing the human factor. Therefore, it is essential that we focus on the previous researches carried out in identifying the factors influencing a cyber-security culture in an organization and what methods can be used in establishing a successful information security culture and change behaviours, attitudes and assumptions of individuals.

As Parsons, et al. (2010) claims that factors such as an individual's cognitive ability, personality traits and differences play a major role in how an individual perceives risks. All of these factors stated are directly influenced by the inherited culture of an organization and the security environment that he/she regularly interacts with. Embedded norms of the groups can also influence an individual's behaviour as they follow group norms unconsciously. If the group does not understand the mindset of the importance and seriousness of information security, it is unlikely that the individual within the group would value and follow the security policies/practices. They also emphasize the importance of human factors in a cyber-security culture apart from the application of technologies to prevent and mitigate the threats.

Furthermore Dul, (2011) in his journal article on human factors in business, indicates the importance of understanding how a workplace can be designed with people in mind, and the benefits which definitely outweigh as an ergonomic approach, can improve the overall performance. According to ENISA (2017), three of the top five cyber-attacks are related to human factors, such as social engineering, human errors and deliberate misuse. In the year 2017, human errors accounted for 19-36% of all breaches. The contribution from the human factors for cyber risk is clear. Imparting knowledge, enhancing awareness and influencing human behaviour to mitigate these risks are difficult and challenging if the human factor is ignored. ENISA notes the psychological factors in changing the behaviour of people and that three parallel processes must take place. There must be dissatisfaction with the current situation;

this dissatisfaction must cause anxiety and/or guilt and employees must be able to adopt new behaviour in a safe environment without compromising their identity or integrity.

Hafizah, et al. (2015), in their systematic literature review on the subject of information security culture, claim nine factors influencing security culture. Namely security behaviour, security awareness, top management, cultural differences, trust, information sharing, security knowledge, security policy and belief. This is based on forty studies conducted in the field. The study also defines security culture as an enabler for minimizing security risks and incidents.
Alavi (2016) too in his study showcases that security is not a technical problem but human and it affects the management of security. Alavi identifies the human factor being divided into two categories as direct and indirect. Direct being factors such as stress, error, awareness, skills, experience, apathy, ignorance and negligence whereas the indirect speaks of budget, culture, communication, management support, security enforcement policy, incentive and disincentive policy. Karwowski and Glaspie (2018) discuss the link to employees' willingness towards information security policy compliance is more adhered to when the reward/incentive or punishment (deterrent) is enforced by the management. There's a high level of certainty that the employees would adhere to the organization's security policies and procedures when management presents evidence of implication of security breaches such as financial and business loss, bad reputation it carries, impact on compensation, etc. Subsequently, this leads to an individual to make the right decision and that his moral beliefs/social pressure plays a role when the compliance decision is made. Inclusion (Karwowski and Glaspie, 2018) in conclusion states, "regardless of deterrence or incentives, adherence to information security policy is a major factor in cultivating an information security culture".

As explained by Parsons et al. (2010), it is important that the management identifies motivational factors of employees in order to motivate them to build a secure culture: For example, the understanding of response to intrinsic and extrinsic motivators whether the reward scheme for positive behaviour works better for the punishment or vice versa. It also suggests that the employee's motivation occurs when he feels the responsibility for information security. Feldman (1999) in his book states that an individual's response to stimuli that produces a satisfactory or a pleasant state of affairs in a particular situation are more likely to occur again in a future situation. Conversely, the response that produce discomfort, annoyance or unpleasant effects are less likely to occur in a future situation. Feldman (1999) highlights both a reinforce and reward increases the probability that a preceding response will recur. In contrast, negative reinforcement teaches an individual that taking an action removes a negative condition that exists in the environment. By applying this to the corporate environment, an organization should identify what the appropriate stimulation its employees or groups require and initiate programmes for incentives for positive response and deterrent for negative unacceptable response.

Farahmand, et al. (2008) points out that not all incentives have a positive impact on performance and caution against not using the method efficiently. Efficient incentives encourage many users to act for a common cause (Bulgurcu, et al., 2010). An employee's willingness and determination to comply with the information security policy of the organization depends on his/her attitude. Attitude is influences by many variables such as benefits, cost of compliance and cost of non-compliance. Benefit of compliance is based on safety and rewards whereas the cost of compliance, by work impairment. Non-compliance is

based on intrinsic cost and sanctions. Chen, et al. (2012), in their study, confirms the level of reward and punishment significantly affect the intention to compliance from employees. This is further reinforced when there is a certainty that the incentive or deterrence will be enforced by the organization without any bias. In addition, when there is an intention to comply, it is greater when the reward is low. Based on the previous literature reviewed by the researcher, it is evident that there is a need for the research selected in identifying human factors influencing the successful adaptation of an Information Security Culture. Therefore, a conceptual model/framework was created in continuing the study. With the interest of the time, the study is narrowed down to a renowned technology service company in Sri Lanka. ISACA Journal (2017) states that the key part of the journey in gaining employee adoption to the information security culture is to show the employees what is in it for them. This can influence the behaviour of employees and attract them to do the right thing. Unfortunately, there are only a handful of organizations that maintain a robust incentive programmme which is linked directly to the company culture.

Conceptual Framework of the research

In synthesizing the research, a conceptual model of the framework was identified by considering the facts in literature review to examine the factors affecting the successful implementation of a security culture. As dispatched in figure 1, the model includes the following factors: Training and Awareness, Leadership Support, Deterrent and Incentives as the independent variables to the dependent variable of successful cultivation of an Information Security Culture.

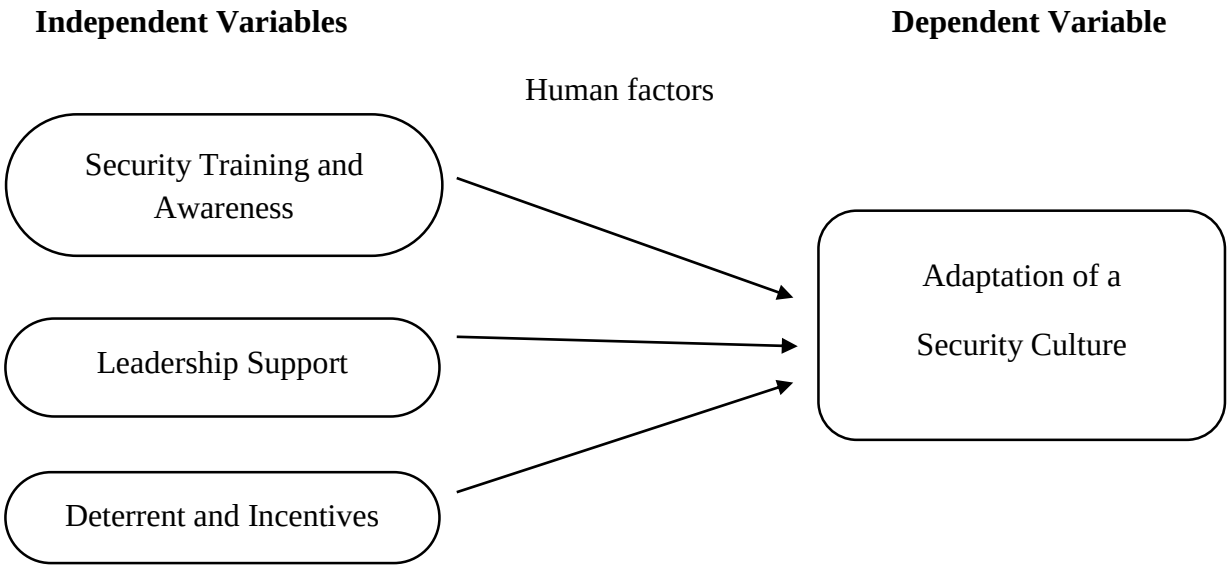

Figure.1: Conceptual model

Security culture defined by Alhogail and Mirza (2014) shows how things are done in an organization with regard to its information security aiming to protect information assets of the company and its clients by influencing the behaviour of employees towards security. The effectiveness of the information security controls significantly depends on the competency and dependability of the people who implement and also use them. The human factor becomes the dependent factor representing the weakest link in information security and this implies the importance and significance of human behaviour. Establishing a security culture in an organization makes security a part of everyday life (Eloff and Da Veiga, 2002). As an interest of the researchers, the dependent variable is taken as the "adaptation of a security culture" with the selected dependent variable researchers intending to measure the variables that change and influence. Training and awareness provide an employee the required skill and knowledge to understand the need of proper use of systems and handling of data and compliance with policies. This is the foundation element for all thriving information security cultures and key to mitigate the risk of breaches caused by human behaviour. It is evident that from the literature review that despite the increase of threats and insider breach, employee awareness is still lacking. Therefore, training and awareness is a key factor for this study. Veseli (2011), in her study, defines security awareness as "the degree or extent to which every member of staff understands". Awareness is intended to allow a person to recognize and understand IT security concerns and to respond to them correctly.

Any effective change in an organization strives from good leadership support. Continuous focus and support from the leadership is essential in developing and cultivating a security first culture in an organization. Support involves budget, technology, human capital, mentoring etc. Top management must deliver clear guidance and promote clear message of its information security policies, goals and expected behaviour from its employees in directing the effort on a successful information security culture. This too is clearly identified through the literature review carried out in this study. Forbes technology council states that the security culture should start from the top (Fredikson and Gene, 2018). CEO and the board of an organization must commit to obtain executive management's support for security programmes. Making security everyone's responsibility should come from the top and senior managers must embody the security culture through their words, communication and actions which will impact the employees.

Based on the above conceptual framework, the following hypotheses are derived for the study:

H1 – There is a relationship between the training and awareness of the organization employees and the adaptation of a security culture.

H2 - There is a relationship between the leadership support of the organization and the adaptation of a security culture.

H3 - There is a relationship between the deterrence and incentive of the organization and the adaptation of a security culture.

Methodology

Research Design

Design of the research is based on deductive methodology where conceptualization and hypothesis are constructed based on previous literature as emphasized by Dewasiri et al. (2018). Testing and validation of the hypothesis have been carried out to derive the conclusion. The purpose of the study is to ascertain whether there is a relationship between human factors and adaptation of a security culture. This research intends to identify the internal human factors affecting the successful adaptation of an information security culture of the selected corporation. Therefore, the target population would be the employees working in a leading IT company in Sri Lanka. As per the data obtained through the Human Resources Department, the number of active permanent employees as at 31st December, 2018 is 2850. Employees are categorized into a tier-based structure which illustrates the hierarchy. Sample size was decided based on $n = N / [1+N (e)^2]$ where n = Sample Size, N = Population, e = Sampling error. Using the method calculation, the sample size for the research is derived as: n = Sample Size, N = 2,850, e = 10%. By applying the calculation of $n = 2,850 / [1+2,850 (0.1)^2]$, it was calculated with the sample size as 97. Sampling of data collection can be carried out using various methods such as simple random sampling, cluster sampling, stratified sampling and systematic sampling. Stratified sampling method has been selected for this research in selecting the sample.

The primary data collection was done through the stipulated questionnaire which was distributed among the staff of the selected organizations in Sri Lanka. The researchers identified the measurement indicators for each listed variable where these were used in constructing the base of the questionnaire. Human factors were operationalized using three dimensions called security training awareness, leadership support, deterrence and incentives (Nikolakopoulos, 2009). The measuring indicators of security training and awareness were; security awareness, security-oriented education and security training. The measuring indicators of leadership support were active involvement, ownership and consistent support and adequacy of resource allocation. The measuring indicators of deterrence and incentives were availability, certainty, intrinsic and extrinsic motivation. The adaptation of a security culture was measured using 'intent to comply, 'all in' mentality and confidence (Hull, 2015; Veseli, 2011; Winnipeg, 2008; Alavi, 2016). The questionnaire was an anonymous one and it contains two parts. Part 1 of the questionnaire consisted of general demographic questions and Part 2 of the questionnaire represented questions pertaining to the identified measurement indicators. All questions were closed ended and answers were given using the Likert scale. After the preparation of the questionnaire, the researcher carried out a pilot validation by selecting a random set of employees of the selected organization to ascertain the validity and the understandability of the questions. Upon the received feedback, and since there was no requirement to change the questionnaire, the researchers distributed it among the intended sample. This helped to improve the quality of the questionnaire and the accuracy. Researchers had records and they collected the feedback from the participants on a given date. The questionnaire consisted of two parts. Part 1 of the questionnaire represented the demographics information such as employees' age, gender, academic qualification, organizational tier and level of computer literacy. Part 2 of the questionnaire consisted of twenty-seven questions across security awareness and training,

leadership support, incentives and deterrence which span across nine facets and the adaptation of security culture with six facets spanning across six questions. A five-point Likert was used to determine the responses of the second section of the questionnaire. IBM SPSS and Microsoft Excel software were used to analyze the data in determining the relationship of the independent variables to the dependent variable.

Analysis and Results

Gender distribution of the sample shows an even distribution with a dominance in the male representation with 57.8% while 42.2% being females. The sample represents relatively a collection of young people where 53.3% of it being below 29 years of age and 33.3% being between the ages of 30 and 39. The sample represents over 80 percent of employees qualified with either a Bachelor's or Master's degree. Majority of the sample, which is 82 percent, has the computer skills at intermediate level and above as the selected company being an information technology company.

The consistency and stability of the two constructs used to assess human factors and adaptation of security culture were measured using Cronbach's alpha values. According to Sekaran and Bougie (2013), reliabilities less than 0.6 are considered poor while those in the range of 0.7 are acceptable and over 0.8 are considered good. Based on the total sample, data was at an acceptable level where all variables were within 0.7 to 0.8. The Cronbach's alpha values increased from the pilot test carried out due to the changes done in the questionnaire and due to the increase in the number of respondents. Table 1 shows the reliability values of the final instrument. Accordingly, all variables were having above .7 Cronbach's alpha values and it ensured the internal reliability of the instrument.

Table 1: Reliability analysis

Variables	**Cronbach's Alpha Values**
Security awareness	0.723
Leadership support	0.860
Deterrence and incentives	0.731
Adaptation of security culture	0.707

In determining the level of the security culture adapted in the company, a six-item questionnaire was used. An overall mean value of 3.84 was ascertained by collecting data from ninety participants which indicates that the level is reasonable and is at a moderate level. In comparison to the mean values of the statistics summary, it highlights that the independent variables deterrence and incentives are of 2.96 which shows a moderate level of security awareness, and training of 3.46 which is also at a moderate level and are also lower than the adaptation of a security culture of 3.84. Whereas, the leadership support is slightly higher than the adaptation of a security culture indicating a mean of 3.88. To understand and ascertain

whether there is a relationship between human factors and the adaptation of a security culture of the employees of the selected IT company, a bivariate analysis was conducted. This was done using the variables security awareness and training, deterrence and incentives, leadership support and adaptation of a security culture. Pearson coefficient (r) was used to test the hypothesis which provided evidence to the relationships. Two-tailed method was used to assess the correlation. The significance of the p value = 0.05 is generally accepted indicating that 95% assurance is given; there is a true or a significant correlation between the two variables. If the two variables indicate a $p < 0.01$, we would know that there is a positive relationship and that the probability of not being true is only 1%. (Sekaran and Bougie, 2013).

The first hypothesis of the study was "There is a relationship between Security training and awareness of the organization employees and the adaptation of a security culture". In order to test the relationship, alternative and null hypotheses were defined as given below.

H_1 – There is a relationship between security training and awareness of the organization employees and the adaptation of a security culture.

H_0 – There is no relationship between security training and awareness of the organization employees and the adaptation of a security culture.

Table 2: Pearson correlation of security awareness and training

		Adaptation of security culture	Security awareness and training
Adaptation of Security Culture	Pearson Correlation	1	.436**
	Sig. (2-tailed)		.000
	N	90	90
Security Awareness and Training	Pearson Correlation	.436**	1
	Sig. (2-tailed)	.000	
	N	90	90

**. Correlation is significant at the 0.01 level (2-tailed).

Based on the statistics of the analyzed data, according to table 2, the p-value for security awareness and training was less than 0.01 Therefore, the null hypothesis was rejected and the alternate is accepted. Furthermore, the Pearson coefficient value was at 0.436. Hence, it shows a positive moderate relationship between security awareness and training against the adaptation of a security culture.

Second hypothesis of the study was "There is a relationship between the leadership support of the organization and the adaptation of a security culture". In order to test the relationship between leadership support and the adaptation of a security culture, following null hypothesis and alternative hypothesis were developed.

H_1 - There is a relationship between the leadership support of the organization and the adaptation of a security culture.

H_0 - There is no relationship between the leadership support of the organization and the adaptation of a security culture.

Table 3: Pearson correlation of leadership support and the adaptation of a security culture

		Adaptation of a security culture	Leadership Support
Adaptation of a security culture	Pearson correlation	1	.470**
	Sig. (2-tailed)		.000
	N	90	90
Leadership support	Pearson correlation	.470**	1
	Sig. (2-tailed)	.000	
	N	90	90

**. Correlation is significant at the 0.01 level (2-tailed).

Based on the statistics of the analyzed data, and according to table 3, the p-value for leadership support is less than 0.01. Therefore, the null hypothesis was rejected and the alternative hypothesis was accepted. Furthermore, the Pearson coefficient value is at 0.470. Hence, it shows a positive moderate relationship between leadership supports against the adaptation of a security culture. The third hypothesis of the study was "There is a relationship between the deterrence and incentive of the organization and the adaptation of a security culture". In Order to test the relationship between deterrence and incentive of the organization and the adaptation of a security culture, the following alternative and null hypotheses were developed.

H_1 - There is a relationship between the deterrence and incentive of the organization and the adaptation of a security culture.

H_0 - There is no relationship between the deterrence and incentive of the organization and the adaptation of a security culture.

Based on the statistics of the analyzed data, and according to table 4, the p-value for deterrence and incentives is less than 0.05. Hence, the null hypothesis is rejected and the alternate is accepted. Furthermore, the Pearson coefficient value is at 0.217. Therefore, it shows a positive weak relationship between deterrence and incentives against adaptation of a security culture.

Table 4: Pearson correlation of deterrence and incentives

		Adaptation of a security culture	Deterrence and incentives
Adaptation of security culture	Pearson Correlation	1	.217*
	Sig. (2-tailed)		.040
	N	90	90
Deterrence and incentives	Pearson Correlation	.217*	1
	Sig. (2-tailed)	.040	
	N	90	90

*. Correlation is significant at the 0.05 level (2-tailed).

Findings, Discussion and Conclusion

First hypothesis, resting "the relationship between security awareness and training to the adaptation of a security culture" revealed that there is a positive and moderately strong relationship between the two variables. This shows the importance and the relationship of security awareness, training and education towards building a security culture. The tendency of an individual to act proactively, reactively and positively towards a security incident will be more and the mind-set of the individual would be to safeguard their data always. A similar relationship was found in previous literature reviews (Karwowski and Glaspie, 2018). Hull (2015) also emphasizes the importance of educating the users when they are aware that behaving insecurely is imperative in improving a good security behaviour. It is also vital that the user has the correct mental model to ensure a compliant behaviour.

Second hypothesis in testing the relationship between leadership support and the adaptation of a security culture too showed a moderate strong positive relationship between the two based on the data collected. This proves that the influence of the leadership is of utmost importance in cultivating the right security culture and posture in an organization. The commitment from the seniors in aligning the social mechanism demonstrating through human resources, budgets, awareness and active involvement are some of the factors which could be highlighted with the findings of the literature and questionnaire (Kayworth and Whitten, 2010). The research implies nine integration mechanisms in achieving information security objectives where they give significance to leadership mechanism.

The Third hypothesis was that "Deterrence and incentives prove a moderately strong positive relationship with the adaptation of a security culture". In terms of data collected through the questionnaire, it was understood that there is a lack of deterrence and incentive programmes in the selected company. The deterrence and incentives are important in influencing the intrinsic and extrinsic behaviour of users. Aurigemma and Mattson (2014) emphasize the impact of individuals' behaviour through sanctions and that employees trust the

system in the organization to either punish for non-compliance or reward for good behaviour being carried out cohesively. Answering the primary research objective showed a positive relationship between the human factors and adaptation of the security culture with respect to the collective impact of dimensions of human factors in a security culture.

Recommendations

Recommendations are made to make the audience understand their demographics to define training programmes related to security. First and foremost, learn what the employees already know in terms of security and plan the security awareness programme implementing focus group awareness and training programmes. Keep the security awareness fun and interesting although security is a serious business. Adapt gamification methods and let employees compete for high scores in their security compliance.

Focus more on security education for end user apart from the IT professionals as the survey indicates that the level of awareness within the IT security is significantly higher than the rest and provide them with adequate education to combat security threats by themselves and be confident. Furthermore, continue the training throughout the year and consider a cyber-security newsletter to be circulated monthly among the employees. Based on the survey conducted, it was identified that there is no mechanism within the company to share information pertaining to security assessments and issues with all employees. It is important that the leadership focus on sharing information on security incidents and bring awareness to everyone as it would highlight the importance and the consequences to the company if data is breached. Leadership lacks the consistency in taking action against those who do not comply with security policies. The researcher recommends that control and process are brought into ensure that violators are appropriately punished. Further, to strengthen the human resources with respect to IT security and provide sufficient funding to cater to the needs of security specialists.

It is recommended to implement a reward and recognition programme for those who comply with security policies and who prevent a potential security breach or attack. This would allow the behaviour of employees to adhere to security policies more similar to the deterrent controls implemented. It is evident from the survey that the selected organization lacks consistency in sanctions and lacks a reward/recognition programme. Motivating employees through simple appreciation as reward, not necessarily a material reward it could be a simple public recognition or posting on a newsletter of the company. Further, reward good practices with spontaneous rewards, make security performance of the employee a part of their annual performance appraisals emphasizing that good security is everyone's duty.

Limitations and Future Research Suggestion

The potential errors and social appeal may have affected the accuracy of the data collected in the study. Lack of literature pertaining to Sri Lankan context proved to be another limitation in conceptualizing and operationalizing the study more focused and relevant to the selected organization.

Development of a 360-degree feedback in addition to self-reporting will need to be looked at in future research to obtain data that are more accurate. Research is needed to perceive all human variables that have an impact on security culture as the respective research constitutes only a 30 percent from its independent variables towards the dependent of adaptation of a security culture based on the data collected. Therefore, expanding the research towards identifying all factors influencing the security culture in an organization is of utmost importance in the global and local context.

References

Alavi, R., Islam, S., and Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. Infrastructure and Computer Security, 24, 205-227.

Alhogail, R. and Mirza, A. (2014). Information Security Culture: A Definition and a Literature Review. IEEE World Congress on Computer Applications and Information Systems, Tunisia pp. 1-8.

Aurigemma, S. and Mattson, T. (2014). Do it OR ELSE! Exploring the Effectiveness of Deterrence on Employee Compliance with Information Security Policies. *Deterrence Effectiveness on Employee Information Security Policy Compliance,* 1, pp. 1-12.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance. An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 34(3), 523-548.

Chen, Y., Ramamurthy, R. and Wen, K. W. (2012). Organizations' Information Security Policy Compliance. Stick or Carrot Approach. *Journal of Management Information Systems*, 29(3), 157–188.

Choi, M. (2016). Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing. *Sustainability,* 6, 1-21.

Dewasiri, N.J., Weerakoon Banda, Y.K. and Azeez, A.A. (2018). Mixed Methods in Finance Research: The Rationale and Research Designs. *International Journal of Qualitative Methods*, 17, 1-13.

Dojkovski, S., Lichtenstein, S., and Warren, M. (2006). Challenges in fostering an information security culture in Australian small and medium sized enterprises, in ECIW2006: proceedings of the 5th European conference on Information Warfare and Security, Academic Conferences Limited, Reading, England, 31-40.

Dul, J. (2011). Human factors in business: Creating people-centric systems, *RSM Insights*, 1, 04-07.

Eloff, J. and Da Veiga, A. (2002). Information Security Culture. *Security in the information Society.* In Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives, 203-214.

ENISA, (2017). *Cyber Security Culture in organizations*, European Union Agency for Network. Greece. 1-82.

Farahmand, F., Atallah, M. and Konsynski, B. (2008). Incentives and Perceptions of Information Security Risks. *Engineering Management,* 60(2), 238-246.

Feldman, R. S. (1999). *Essentials of Understanding Psychology.* 5th edi. McGraw-Hill Higher Education, Boston.

Glaspie, H. and Karwowski, W. (2018). *Human Factors in Information Security Culture: A Literature Review.* In proceedings of Advances in Intelligent Systems and Computing, 269-280.

Guo, K. H. (2013). Revisiting the Human Factor in Organizational Information Security Management. *ISACA Journal*, 6, 32-41.

Hafizah, N.H., Ismail, Z. and Maarop, N. (2015). Information Security Culture. A systematic Literature Review, Proceedings of the 5th International Conference on Computing and Informatics, 456-463.

Hull, M. (2015). Factors Affecting Secure Computer Behaviour, *Curve,* 05, 1-128.

Hulugalle, R. (2018). Lanka Business Online. Available at: http://www.lankabusinessonline.com/virtusa-worth-us1-5bn-projects-year-end-march-2019-revenue-of-us1-25bn/ [Accessed on 19. 08. 2018].

Humaidi, N. and Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, 5(4), 311-318.

Pereira, P.A.D.F. (2017). Creating and Defining a Culture of Security. Creating and Defining a Culture of Security: The Human Factor. *ISACA Journal*, 6, 1-5.

Kelly, S.T. (2017). Instilling a Culture of Security Starts with Information Governance. *ISACA Journal*, 5, 1-5.

Karwowski, W. and Glaspie, H. (2018). Human Factors in Information Security Culture: A Literature Review in Advances In Intelligent Systems and Computing. Proceedings of the International Conference on Applied Human Factors and Ergonomics, 269-280.

Kavoos Mohannak, A. S. K. N. (2010). Information Security Culture:A behaviour compliance conceptual framework, In Boyd, C & Susilo, W (Eds.) Information Security 2010: AISC '10 Proceedings of the Eighth Australasian Conference on Information Security, Australian Computer Society, Australia, 51-60.

Kayworth, T. and Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive*, 9(3), 163-175.

Lim, J. S., Ahmad, A., Chang, S. and Maynard, S. (2010). Embedding Information Security Culture: Emerging concerns and Challenges. PACIS 2010 Proceedings. 43, 463-474.

Maylahn, P. (2018). K-12 IT Leadership Survey Report, *Leading Education Innovation*, 1, 1-37

McLeod, S. (2019). Likert Scale Definition: Examples and Analysis. [Online] Available at: https://www.simplypsychology.org/likert-scale.html [Accessed 21 08 2018].

Metalidou, E., Marinagic, C, Trivellasc, P., Eberhagen, N., Skourlasd, C. and Giannakopoulosa, G. (2015). The Human Factor of Information Security: Unintentional Damage. *Procedia - Social and Behavioral Sciences*, 147, 424-428.

Morgan, S. (2018). Cybersecurity Market Report. [Online] Available at: https://cybersecurityventures.com/cybersecurity-market-report/ [Accessed 20 08 2018].

Nasrin, B. and Habibi, A. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. *Journal of Basic and Applied Scientific Research*, 2, 9331-9347.

Nilashini, W.T.A. and Sajeevanie, T.L. (2018). Relationship between Organizational Work life factors and Executive Employees Performance in Selected IT organizations in Sri Lanka. *Sri Lankan Journal of Human Resource Management*, 8(1), 60-76.

Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. Command, Control, Communications and Intelligence Division, 1-54.

Prince, B. (2015). Employees Not Following Policy is the Biggest Threat to Endpoint Security, IT Pros Say. [Online] Available at: https://www.securityweek.com/employees-not-following-policy-biggest-threat-endpoint-security-it-pros-say [Accessed 19 08 2018].

Rantapelkonen, J. and Salminen, M. (2013). *The Fog of Cyber Defense*, National Defense University, Helsinki.

Sahito, F. (2013). *The Human Factor of Cyber Crime and Cyber Security*, Eleven International Publishing, Netherlands.

Sekaran, U. and Bougie, R. (2013). *Research Methods for Business*. 6th edi, Wiley India Pvt. Ltd, New Delhi.

Verizon Enterprise, (2018). Data Breach Investigation Report, [Online] Available at: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf [Accessed 19 08 2018].

Veseli, I. (2011). *Measuring the Effectiveness of Information Security Awareness Program*. Gjøvik University College, Norway.