Empirical Study on the Influence of Security Control Management and Social Factors in Deterring Information Security Misbehaviour

Hanifah Abdul Hamid¹*, Nuradli Ridzwan Shah Mohd Dali²

¹Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia
²Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia.

Abstract. Complying with the security rules and standard is important to safeguard valuable information in the organisation. Failure to prevent security breaches costs the organisation huge losses and bad reputation. Technical solutions are abundant but nonetheless still unsuccessful to deter information security incidents. The root cause of incompliance is humans as they are the weakest link of security chain. This paper examines the information security control management particularly on information security awareness, training and education, risk analysis and management, information security policies and procedures as well as physical security monitoring, and cognitive factors which give impact towards the employees’ information security compliant behaviour in the organization. Based on convenient sampling, a survey was conducted to employees of public and private sectors in Malaysia who are the Software as a Service (SaaS) cloud users. Data was collected online and was analysed using PLS-SEM. Result shows that information security control management and cognitive factors have high significant impact in deterring information security misbehaviour in the context of cloud users.

1. Introduction

The emerging of cloud computing has uplifted the information technology to the more advanced level. Cloud environment offers 3 service models i.e.: Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [49].

IaaS is the lowest level of cloud adoption in the organisation. The service provider only offers the network, storage, servers and virtualisation, when an organisation decides to adopt IaaS. However, with PaaS, the IS department of the organisation can fully focus on applications and data since every other service will be managed by selected vendors or providers. The real cloud adoption is with SaaS since all services is taken care of by the providers. The organisation can instead fully pay its attention to the core of their business to achieve competitive advantage. In the SaaS cloud environment, everything is served in and around the cloud to which people are not required to bring their own storage devices, since data can be saved in the clouds.

Nevertheless, study shows that security is a major hindrance of cloud adoption [1], [2]. Even though scientists have come up with an abundant of technical solutions to solve information security problems,
security incidents still happen all the time. Of all the causes, human is the main vulnerability [52] and is the weakest link of security breaches [3] inside or outside of the organisation, since any human errors, intentionally or accidentally, can compromise the security protection. The people’s characteristics, shared values and norms shape their security behaviour in cloud computing environment thus affecting the safety of the information. A security breaches study reported that the employees and former staff are the main culprits of security incidents, however, current and former service providers, consultants and contractors also contributed to an increase of 18% and 15% respectively [52].

Nevertheless, security breaches by the current employees are mostly accidental due to loss of mobile devices or being victims of social engineering. Study shows that Malaysia contributes to the highest organised crime (35%) in the cyber world, a cybercrime organised to obtain financial gain [52]. Private and confidential data and information leakage due to theft by insiders has cost exposure of health patients or bank clients’ information in exchange of monetary incentives. Security compromise causes greater financial and non-financial impacts. The cost of security breaches continues to increase over time [55]. It has been reported that the average cost of security breaches in the UK has gone up substantially from £600,000 in 2014 to £1.46 million in 2015 due to business disruption, lost sales, recovery of assets, and fines and compensation. [52]. The financial costs of security breaches have consistently risen over time as recently reported in [59].

Non-financial impact due to security breaches may include reputational damage, the pirating of products, diversion of research and development information, impacts to innovation, stolen product designs or prototypes, theft of business and manufacturing processes, as well as loss of sensitive information such as corporate strategy [60]. Larger organisations suffer more attacks compared to smaller firms, but the financial losses are varied for the fact that larger organisations often have security measures in place that could better detect security incidents. However, the cases mostly went unreported due to strategic reasons and fear of reputational damage.

A lot of researches done previously highlighted on the technical solutions to overcome security incidents in cloud environment [56]. However, it is evident that technical solutions are meant for preventing security breaches but are not sufficient in deterring security incidents [57].

Even though researchers on information security compliance culture have been doing studies for more than a decade, a study shows that information security culture (ISC) research is lacking in generating and testing theory (Karlsson et al., 2015) that could enhance the body of knowledge of information security compliance. The existing ISC research was focusing more on the theoretical and conceptual work rather than field studies [30]. [50] argued that majority of researched topics of ISC focused on the relations of organisational culture and information security as well as on the framework on cultivating ISC but only a small number of studies have been carried out in these areas such [29][53]. The adoption of organisational culture models in ISC studies is not sufficient for revealing the critical influencing factors of ISC which creates the social gap.

For the past three years fraud and intrusion have become the highest security incidents reported in Malaysia [51]. Cybersecurity professionals agree that security depends on people more than technical control and countermeasures [54]. The socio-organisational factors are the main contributors of security failure and if not addressed properly, can slow down the progress of cloud adoption in the organisations.

Hence this study will approach the information security compliant behaviour (ISCB) from the socio-organisational perspective. Previous studies discussed the factors inculcating security culture in the organisation [5][6][7] but there is no first-hand evidence that could prove the claim. The aim of this paper is to empirically examine the driving factors of security compliant behaviour in the organisation. Specifically, this paper, as part of the whole ISCB research, will seek to answer this question: How significant are the social and information security control management factors in deterring security misbehaviour?
2. Relevant Theories
From the social or organisational perspective, it was observed that past security behaviour researches adapted behavioural theories (e.g.: Social Cognitive Theory (SCT), Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT) or Organisational Culture Theories (e.g.: Hofstede’s Organisational Culture Theory, Detert Organisational Culture, Schein Organisational Culture), depending on the target of research, whether the individual or the organisation. Out of these organisational culture models, most of ISC scholars used Schein’s Organisational Model [58] compared to other organisational models. However, [4] argued that the uses of this model did not provide strong theoretical foundations.

The adoption of various theories from social sciences field indicates that research in security behaviour is still in its infancy [50] and needs further exploration before it comes to maturity.

Adapting Social Cognitive Theory (SCT), as well as extended deterrent theory (DT) as our framework, this study will examine the impact of security control management (SCM), personal values (PV), environment (ENV) and employees’ behaviour (BHV) towards information security compliance behaviour (ISCB). SCT is a three dimensional complementary model that is used to determine human behaviour which consists of cognitive or personal factors, environmental factors and behavioural factors [8]. The theory founder [8] further accentuates that “expectations, beliefs, self-perceptions, goals and intentions give shape and direction to behaviour. What people think, believe, and feel, affects how they behave [8], [9]. He nevertheless argued that behaviour cannot easily change the environment much like it is influenced by the environment unless the behaviour first change itself.

The DT of punishment can be traced to the early works of classical philosophers such as Thomas Hobbes (1588–1678), Cesare Beccaria (1738–1794), and Jeremy Bentham (1748–1832) [10]. Rooted from school of criminology, DT advocates that individual choose to commit crime when the benefits of the action outweigh the costs [11]. Deterrence has been indicated significant in decreasing negative practices and has likewise been observed to be a viable instrument in administration [12]. In Information System (IS) research, DT has been extended by integrating some security control as a measure to deter security breaches [13].

3. Hypotheses Development

3.1. SCM and Security Behaviour

To ensure successful information security in the organisation, the SCM is vital. Past scholars have highlighted on the important roles of SCM in making sure that employees act according to the standards and procedure, and rules and regulations [14], [15].

Security awareness [16]–[18], as well as security training and education [16], [17], [19], [20] are among the most basic factor needed in inculcating information security culture in the organization which must be given much attention by the top management. Employees must be aware that their behaviour must always in accordance to the rules and regulations to avoid security breaches that may occur accidently or intentionally. However, in today’s technology advancement where threats are rising almost from any angle, security awareness is still lagged behind [21]. The lack of security awareness causes security incompliance in the cloud environment, which makes outsourcing arrangement of IT services becomes more complex [22]. Without proper security education, training and awareness (SETA) programmes, people do not know if they have committed security breaches. It was found out that SETA programmes has positive influence on managing and detering security behaviour [15].

In addition, the organisations that have proper information security policies and procedures (SPP) are better at guiding employees to good security behaviour. Research shows that complying with
organisation security policy can shape and mitigate the risk of employees misbehaviour [23]. However, employees must be aware of the information security policies in place in order to have an effective deterrence factor [15]. It is also a critical factor to consider setting up ethical conduct policy [24] in building up security culture in the organisation. It is argued that previous research in ISCB did not give attention on ethical conduct due to different organisations have different kinds of values and culture [17].

Another security control is risk analysis assessment and management (RAM). The organization will be able to identify areas that are highly critical for information security and to improve the security effectiveness. Information is secured with the three triads of information system – confidentiality, integrity and availability. However, in nowadays computing, cloud computing for instance, has exposed information to more security risks and challenges issues. Information is at risks of the existence of vulnerability and threats. It is claimed that organizations which have security RAM in place are being more aware of their losses due to security breaches [17].

The fourth factor for SCM is physical security monitoring (PSM) which is essential to control the security behaviour of employees in the organisation [13]. While technical threats are easier to detect and rectify, the human threats are proven to be difficult to identify. Thus, the uses of PSM activities are said to be effective in controlling the behaviour of the employees with regards to the safety of information.

3.2. PV, ENV, BHV and Security Behaviour

Past research examined how PV have been a significant driving factor in complying with security regulations. This includes their attitude [25], [26], security knowledge [18], [27], [28], religious and ethical beliefs [29], [30] as well as level of trust [29], [31]. Humans act according to their habitual conducts. When human do things repeatedly over and over again, these actions become a habit and are stored in the subconscious minds.

Depending on the individual preference towards an object (person, event, thing, time, activity), attitude can be expressed positively or negatively. Attitude has been proven to have a positive effect on employee security compliance behaviour [25] and self-efficiency in attitude help cultivates ISCB [16].

The ENV plays an important role is shaping a positive behaviour of a person. This can be either internal or external environment that influence from within and outside organisation. As an individual, people tend to adapt themselves to the particular situation for the fact that they are unable to change the environment alone. In this situation, the government plays an important role to ensure the information security is at the highest priority.

The Personnel Data Protection Act 2010 was enacted by the Malaysian Government for this reasons. It was suggested that the enforcement of the act will help shaping the behaviour of the people with regards to information security [32]. The influence of regulation with regards to information security culture should be empirically tested [5]. Another ENV element is social norms. Individuals’ behaviour are very much shaped by their ENV such as peer influence. The colleagues and immediate supervisor, other departments’ behaviour, the mechanism for rewarding good behaviour and punishing bad behaviour are constructing factors which influence the security behaviour of the employees in the organisation [12], [16]. It is argued that among others, ENV factors that influence the security behaviour of people are still yet to be explored [33], [34], [3].

BHV is the conduct of a person towards a particular situation which is based upon the ENV as well as the personality traits one owns. The BHV elements which includes skills, practice and self-efficacy (SESE) of employees are formed gradually in such a long span of time and cannot be obtained overnight. ISCB research found out that security conscious behaviour has a significant impact towards the safety of information in the organisation [14], [28], [34]. Practitioners and researchers alike recognise the positive influence insiders’ behaviour can have on information systems security [48]. Good security
behaviour will result in security compliance thus reduce security breaches. In long term this good behaviour will become norms which exhibit security culture of the organisation.

The skills to measure risks and recognise threats are crucial for information safekeeping. Those who possess lower skills in recognizing and detecting threats are more vulnerable to the attacks. Good security practice will likely reduce security incidents as users take all the precaution steps to comply with security policies and procedures. Experience in information security context means one’s familiarity with the skills or knowledge in the field of information security, which were acquired over a period of time through actual exercise and apparently has enhanced better ability or grasp in behaving according to the security rules and regulations [35]. Using social bond theory [36], [23] found out in their study that the experience and involvement of employees have significant effect on their attitude towards complying with security policy. Self-efficacy is a person’s certainty of his or her ability to perform required behaviours to achieve certain accomplishments [37].

Self-efficacy is a form of self-evaluation that can be the most influential apparatus of human agents in motivating and regulating human behaviour. Many studies in information technology and information systems adoption in various domains claimed that self-efficacy is an influencing factor for users to adopt such technology and systems. Self-efficacy has been found to have a significant relationship towards information security behaviour of the employees [12], [25], [38], [39].

Hence, we posit the hypotheses below as shown in the following diagram:

H1: Security education, training and awareness programmes have a positive impact towards SCM.
H2: The security policy and procedure have positive impact towards security control management.
H3: The physical security monitoring has a positive impact towards security control management.
H4: The security risk analysis and management have positive impact security control management.
H5: Security control management has positive impact towards personal values.
H6: Security control management has positive impact towards the environment.
H7: Security control management has a positive impact towards ISCB.
H8: Personal values have positive impact towards behaviour.
H9: Personal values have positive impact towards information security compliant behaviour.
H10: Environment has positive impact towards behaviour.
H11: Environment has a positive impact towards personal values.
H12: Environment has positive impact towards information security compliant behaviour.
H13: Self Efficacy have positive impact towards behaviour.
H14: Practice has positive impact towards behaviour.
H15: behaviour has positive impact towards information security compliant behaviour.
4. Methodology
The survey instruments were adapted from the work of [18], [27], [40], [41] for cognitive factors using reflective measurement. The security control management instruments were adapted from [15] using formative measurement. All items were measured on a 5 points Likert-scale from 1- strongly disagree to 5- strongly agree. A pilot study was conducted to test the reliability of the questions hence producing the result as in article [47]. The survey was conducted online to professionals in the organisations in Malaysia from October to December 2016 to 1000 potential respondents at various organisations from public and private sectors. Google doc was used as the platform of the survey. Potential respondents were contacted through Facebook, and email messages to which the link of the survey was attached to the messages. Convenience sampling was used as the sampling method. Respondents were informed about the purpose of the study and given option to quit answering at any time.

Screening questions were asked to identify the correct respondents. Respondents were asked about the usage of mobile devices such as laptops or smartphones for their job-related tasks. Respondents were also questioned about their exposure to cloud applications such as cloud storage, social media networks as well as email applications. Altogether, there were 410 people responded to the questions. Screening the missing data, 396 data was useful for empirical analysis. Partial Least Square (PLS) was used to analyse the ICSB model.

5. Findings
Descriptive analysis was conducted to identify the background of the respondents. Female respondents outnumbered male respondents by 26% where 251 female respondents participated in this study compared to male (145). There were two big majority age groups, each at the range of 31-40 (39.4%) and 41-50 (33.6%), followed by 21-30 (23.5%), 61-70 (2.5%), 20 and below (0.8%) and 51-60 (0.5%). With regards to education background, two majority groups are from degree (41%) and master’s degree holder (35.4%), followed by PhD (11.9%), diploma (8.4%) as well as high school level (3.3%). Their working experiences vary, from below 5 and years (33.7%), 5 to 7 years of experience (23%), 11 to 15 years (16.9%), 16 to 20 years (16.9%) and only 15% have experience more than 25 years. Around 46.2% of the respondents are from the public sector, 43.7% from the private sector and the rests are from NGO.
Respondents were also asked with regards to their exposure to the SaaS applications as part of screening valid respondents. Majority of the respondents were exposed to the usage of SaaS applications such as email and social media. The result of their SaaS exposure is summarized as below:

Table 1: Users SaaS Exposure

|                     | Exposure       | Frequency | Percent |
|---------------------|----------------|-----------|---------|
| Email               | Very limited   | 4         | 5.3     |
|                     | Some experience| 10        | 13.2    |
|                     | Quite a lot    | 41        | 53.9    |
|                     | Extensive      | 21        | 27.6    |
| Cloud Storage       | None           | 2         | 2.6     |
|                     | Very limited   | 13        | 17.1    |
|                     | Some experience| 25        | 32.9    |
|                     | Quite a lot    | 27        | 35.5    |
|                     | Extensive      | 9         | 11.8    |
| Mobile Apps         | None           | 2         | 2.6     |
|                     | Very limited   | 8         | 10.5    |
|                     | Some experience| 20        | 26.3    |
|                     | Quite a lot    | 39        | 51.3    |
|                     | Extensive      | 7         | 9.2     |
| SSO Portal          | None           | 1         | 1.3     |
|                     | Very limited   | 8         | 10.5    |
|                     | Some experience| 20        | 26.3    |
|                     | Quite a lot    | 38        | 50.0    |
|                     | Extensive      | 9         | 11.8    |
| Social Media        | Very limited   | 7         | 9.2     |
|                     | Some experience| 7         | 9.2     |
|                     | Quite a lot    | 39        | 51.3    |
|                     | Extensive      | 23        | 30.3    |
| E-Services          | Very limited   | 4         | 5.3     |
|                     | Some experience| 15        | 19.7    |
|                     | Quite a lot    | 30        | 39.5    |
|                     | Extensive      | 25        | 32.9    |
|                     | Very limited   | 2         | 2.6     |

The PLS evaluation of measurement model analysis of formative exogenous latent variables takes 3 steps as suggested by [42] such as examining the convergent validity, the presence of collinearity among indicators, and the significance and relevance of outer weights. Prior to that, the content validity has been achieved by referring the scales to the subject-matter experts and industrial professionals through a pilot study, as well as through conducting an EFA analysis.

The convergent validity can be examined by looking at the value of path coefficient which must be above 0.80 or at least 0.64 [42]. The analysis shows the value of path coefficient for each exogenous construct is above 0.80, which indicates that the formative scales exhibits a sufficient convergent validity of the scales. To examine collinearity issues, the variance inflation factor (VIF) values was referred. Analysis shows that some of the indicators have VIF values above the threshold 5.0 hence, the
The bootstrapping procedure was further conducted to examine the significance and relevance of the indicators. For this analysis, the outer weight and outer loading values must be significant respectively.

The result of formative measurement assessment shows that PSM 35, PSM 36 and PSM 37, RAM 26, SETA 24, SPP 15, SPP 16, SPP 17 and SPP 18 were dismissed from the scale because the VIF are above the threshold value of 5.0. The outer weight and outer loading were further examined to all indicators and those items were found to be insignificant and hence resulting items dismissal. The final formative constructs (PSM, RAM, SETA, SPP) were having convergent validity.

Next is the measurement of reflective scales for exogenous latent variable of SESE and PRCTC as well as endogenous latent variables of BHV, ENV, SCM and ISCB. The reflective measurement specifically analyse for the reliability and validity, convergent validity as well as discriminant validity. The composite reliability values for reflective endogenous latent variable are above 0.70 demonstrate that all reflective constructs have high levels of internal consistency reliability according to [43]. Convergent validity assessment builds on the AVE value as the evaluation criterion. The AVE values of BHV (0.823), ENV (0.55), PV (0.702), ISCB (0.806) and SCM (0.887) are well above the minimum requirement level of 0.5, as suggested by [42]. Thus the measure of the reflective constructs has high levels of convergent validity.

Finally, the discriminant validity assessment was conducted using the Fornell-Larcker criterion and the result revealed that there were no discriminant validity problem. The PLS structural model analysis involves five steps of assessment as suggested by [42] which includes assessment for collinearity, significance and relevance, level of $R^2$, the effect size $f^2$, as well as predictive relevance $Q^2$ and effect size $q^2$. The result of structural collinearity assessment shows that VIF tolerance value for all sets of predictors are below the threshold 5.0 which indicates no collinearity problem in the structural model. The bootstrapping procedure was conducted to assess the significant of path coefficients. Table 2 exhibits the results of path coefficients of ISCB model. The result clearly shows that all paths are significant at least at 5%, except for H1, H5, H12 and H14 which are not significant.

| Hypotheses | Path | Path Coefficient | T Values | Sig. Level | P Values | Remarks |
|------------|------|------------------|----------|------------|----------|---------|
| H1         | SETA -> SCM | -0.009 | 0.112 | NS | 0.911 | Rejected |
| H2         | SPP -> SCM | 0.405 | 4.174 | *** | 0 | Supported |
| H3         | PSM -> SCM | 0.345 | 4.892 | *** | 0 | Supported |
| H4         | RAM -> SCM | 0.183 | 2.285 | ** | 0.023 | Supported |
| H5         | SCM -> PV | 0.048 | 0.93 | NS | 0.353 | Rejected |
| H6         | SCM -> ENV | 0.349 | 5.464 | *** | 0 | Supported |
| H7         | SCM -> ISCB | 0.257 | 4.084 | *** | 0 | Supported |
| H8         | PV -> BHV | 0.185 | 3.472 | *** | 0.001 | Supported |
| H9         | PV -> ISCB | 0.206 | 3.518 | *** | 0 | Supported |
| H10        | ENV -> BHV | 0.106 | 2.385 | ** | 0.017 | Supported |
| H11        | ENV -> PV | 0.449 | 7.277 | *** | 0 | Supported |
| H12        | ENV -> ISCB | 0.075 | 1.109 | NS | 0.268 | Rejected |
| H13        | SESE -> BHV | 0.608 | 12.951 | *** | 0 | Supported |
| H14        | PRCTC -> BHV | 0.047 | 1.433 | NS | 0.152 | Rejected |
| H15        | BHV -> ISCB | 0.348 | 6.123 | *** | 0 | Supported |
6. Discussion dan Conclusion

Driving by the aim of the study, we examined the influencing factors of information security compliant behaviour of SaaS cloud users. All results for information security control management factors are consistent with [15] and [44] except for SETA programmes. Contradict to SETA programmes, the security policy and procedure (SPP), the risk analysis and management (RAM), together with physical security monitoring (PSM) have significant impact to the security control management of information security. A clear information security policy and procedures is vital for it becomes a guidance of what can or cannot be done legally and ethically.

In addition, the results also suggest that the management should emphasize on the PSM more intensively for the fact that this is an effective deterrent factor to prevent information security breaches, which is consistent with [13] result. This perhaps includes the access management system as well as constant monitoring through computer surveillance to inculcate good information security behaviour.

Furthermore, the RAM is a proactive solution, which is crucial not only for correcting information security incidents but also for preventing potential security issues. Organisations which have RAM in place are taking advance step ahead in deterring security breaches to ensure that information is safely protected as well as to avoid substantial losses due to security compromise. Nevertheless, it is quite a surprise that SETA programme is found to be insignificant towards driving good information security behaviour of the users, which is contradict to [13] and [14]. SETA programme has been found to be a salient factor to shape good security behavior of the users as reported in studies [15] and [46]. The contradicting result is most probably due to insufficient security awareness training and education being conducted at the public and private sectors in Malaysia.

Despite SETA is being insignificant to SCM, SCM has significant impact towards the security environment but not to the personal values of employees. Nevertheless, the environment significantly influences the personal values of employees, indicating that the environment is the mediator of the SCM and personal values. The skills, experience and self-efficacy have significant impact to the behaviour of the employees and this is consistent with the results of [25], [39]. Self-efficacy has been proven to be a substantial factor in many security behaviour research to which users believe that their abilities in complying with security regulations as well as utilizing security measures are important in keeping good security behaviour [45]. Without these, employees are unable to distinguish between the good and bad security conduct. Overall, the security control management, the personal values and the behaviour of the employees play a significant role in establishing ISCB.

Similar to other researches which utilised purposive research samplings, the result of this study is not generalizable to all contexts and settings. Whilst much care and effort have been taken prior to conducting this study in terms of making certain the validity of the questions through a pilot study, the researcher has no ability to control the responses given by the respondents as their answers are subject to their own perceptions and judgements. This ISB study was carried out in the context of SaaS cloud environment users, for which the technical issues of SaaS are totally borne by the service providers, hence the suitability of this model for PaaS or IaaS applications remains unknown. In future research, if this model is to be used for PaaS and IaaS context, the technological factors might be taken into consideration.

This study contributes to the knowledge of ISCB through the extension of the SCT and extended DT theories in the context of SaaS cloud users, as well as the development of integrated of an ISCB model. The findings from this study could be enhanced from a different perspective by using a case study method to provide an in depth explanation of the phenomenon. A case study is suggested to be conducted at the public organisation to assess the security compliance behaviour using this model both for external validation as well as for understanding the actual phenomena of information security.

This study can also be replicated to the private sector as well as other domain such as healthcare and banking sectors as these group have the most classified information of patients and clients.
Acknowledgement
We wish to acknowledge Faculty of Science and Technology, Universiti Sains Islam Malaysia for their assistance in this research.

References
[1] Hamid, H. A., & Yusof, M. M. (2015). State-of-the-art of cloud computing adoption in Malaysia: A review. Jurnal Teknologi, 136.
[2] Abdul Hamid, H., & Yusof, M. M. (2016). Conceptualizing global cloud landscape: A review of adoption issues and challenges. Research Journal of Applied Sciences, 11(6), 333-339.
[3] AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567-575.
[4] Connolly, L., Lang, M., & Tygar, D. (2014, June). Managing Employee security behaviour in organisations: The role of cultural factors and individual values. In IFIP International Information Security Conference (pp. 417-430). Springer, Berlin, Heidelberg.
[5] Wood, R., & Bandura, A. (1989). Social cognitive theory of organizational management. Academy of management Review, 14(3), 361-384.
[6] Bandura, A. (1986). Social foundations of thought and action. Englewood Cliffs, NJ, 1986.
[7] Lieberman, P. E. (2010) Deterrence Theory. Billboard, 1(45), 1–8.
[8] Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.
[9] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.
[10] D’Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. Journal of business ethics, 89(1), 59.
[11] Božić, G. (2012, May). The role of a stress model in the development of information security culture. In 2012 Proceedings of the 35th International Convention MIPRO (pp. 1555-1559). IEEE.
[12] Alnatheer, M. A. (2015, April). Information security culture critical success factors. In 2015 12th International Conference on Information Technology-New Generations (pp. 731-735). IEEE.
[13] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security, 42, 165-176.
[14] Furnell, S., & Moore, L. (2014). Security literacy: the missing link in today's online society?. Computer Fraud & Security, 2014(5), 12-18.
[15] Bachlechner, D., Thalmann, S., & Maier, R. (2014). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. Computers & Security, 40, 38-59.
[16] Alnatheer, M., & Nelson, K. (2009). Proposed framework for understanding information security culture and practices in the Saudi context.
[17] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.
[18] Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. Procedia Economics and Finance, 28, 243-248.
[19] D’Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.
[20] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model
in organizations. *Computers & Security*, 56, 70-82.

[21] PricewaterhouseCoopers International Limited. (2015). Managing Cyber risks in an interconnected world: Key findings from the global state of information security survey 2015.

[22] Da Veiga, A., & Elof, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), 196-207.

[23] Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486.

[24] Connolly, L., Lang, M., & Tygar, J. D. (2015, May). Investigation of employee security behaviour: A grounded theory approach. In *IFIP International Information Security and Privacy Conference* (pp. 283-296). Springer, Cham.

[25] Alfawaz, S., Nelson, K., & Mahannak, K. (2010). QUT digital repository: Information security culture: A behaviour compliance conceptual framework. In *Security, Information Aisc, Conference*.

[26] Al-Hamar, M., Dawson, R., & Guan, L. (2010, June). A culture of trust threatens security and privacy in Qatar. In 2010 10th IEEE International Conference on Computer and Information Technology (pp. 991-995). IEEE.

[27] Leiwo, J., & Heikkuri, S. (1998, January). An analysis of ethics as foundation of information security in distributed systems. In Proceedings of the Thirty-First Hawaii International Conference on System Sciences (Vol. 6, pp. 213-222). IEEE.

[28] Colella, A., Castiglione, A., & De Santis, A. (2014, September). The Role of trust and co-partnership in the societal digital security culture approach. In 2014 International Conference on Intelligent Networking and Collaborative Systems (pp. 350-355). IEEE.

[29] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65-78.

[30] Alnatheer, M. A. (2015, April). Information security culture critical success factors. In 2015 12th International Conference on Information Technology-New Generations (pp. 731-735). IEEE.

[31] Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: a behaviour compliance conceptual framework. In Proceedings of the Eighth Australasian Conference on Information Security-Volume 105 (pp. 47-55). Australian Computer Society, Inc.

[32] Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol.*, 55, 591-621.

[33] Cialdini, R. B., & Trost, M. R. (1998). Social influence: Social norms, conformity and compliance.

[34] Topa, I., & Karyda, M. (2015, September). Identifying factors that influence employees’ security behavior for enhancing ISP compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 169-179). Springer, Cham.

[35] Munteanu, A. B., & Fotache, D. (2015). Enablers of information security culture. *Procedia Economics and Finance*, 20, 414-422.

[36] Hirschi, T. (2017). On the compatibility of rational choice and social control theories of crime. In *The reasoning criminal* (pp. 105-118). Routledge.

[37] Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191.

[38] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, 49(3-4), 190-198.

[39] Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.

[40] Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees’ adherence to information security policies: An exploratory field study. *Information & management*, 51(2), 217-224.

[41] Thomson, K. L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information
security culture. *Computer fraud & security, 2006*(10), 7-11.

[42] Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security, 29*(4), 476-486.

[43] Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM).* Sage publications.

[44] Nunnally Jr, J. C. (1970). Introduction to psychological measurement. New York, NY, US: McGraw-Hill.

[45] He, W., Yuan, X., & Tian, X. (2014, August). The self-efficacy variable in behavioral information security research. In *2014 Enterprise Systems Conference* (pp. 28-32). IEEE.

[46] Hamid, H. A., & Dali, N. R. S. M. (2019). Curbing Misbehaviour With Information Security Measures: An Empirical Evidence From A Case Study. Al-‘Abqari: Journal of Islamic Social Sciences and Humanities, 17, 28-38.

[47] Hamid, H. A., Yusof, M. M., Dali, N. R. S. M., (2017). Security Compliance Behaviour of SaaS Cloud Users: A Pilot Study. *Journal of Engineering and Applied Sciences, 12*(16), 4150-4155.

[48] Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders’ psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190-209.

[49] Mell, P., & Grance, T. (2012). The nist definition of cloud computing: Recommendations of the national institute of standards and technology, 2011. *NIST Special Publication*, 800-145.

[50] Karlsson, F., Åström, J., & Karlsson, M. (2015). *Information security culture–state-of-the-art review between 2000 and 2013.* *Information & Computer Security, 23*(3), 246-285.

[51] MyCERT (2019), Incident Statistics Online Available: [https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&sid=9028b785-1b09-4218-a9eb-2d5ede57901b](https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&sid=9028b785-1b09-4218-a9eb-2d5ede57901b)

[52] Miller, A., Horne, R. and Potter, C. (2015) 2015 Information Security Breaches Survey. London.

[53] Yuryna Connolly, L., Lang, M., Gathegi, J. and Tygar, D. J., 2017. Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. Information & Computer Security, 25(2), pp.118-136.

[54] Benson, V., McAlaney, J., & Frumkin, L. A. (2019). Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1264-1269). IGI Global.

[55] Corbet, S., & Gurdgiev, C. (2017). Financial Digital Disruptors and Cyber-Security Risks: Paired and Systemic. *Forthcoming in Journal of Terrorism & Cyber Insurance, 1*(2).

[56] Gupta, U., Saluja, M. S., & Tiwari, M. T. (2018). Enhancement of Cloud Security and removal of anti-patterns using multilevel encryption algorithms. *International Journal of Recent Research Aspects, 5*(1), pp. 55–61.

[57] AlSabbagh, B., & Kowalski, S. (2017). Socio-Technical SIEM (ST-SIEM): Towards Bridging the Gap in Security Incident Response. *International Journal of Systems and Society (IJSS), 4*(2), pp. 8-21.

[58] Schein, E. H. (1990) ‘Organizational culture.’, American Psychologist, 45(2), pp. 109–119.

[59] Cyber Security Breaches Survey 2019: Statistical Release. Online Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf)

[60] Wolff, J., & Lehr, W. (2017). Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data.