International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 5, Number 4 (August 2016), pp.195-201

http://www.meacse.org/ijcar

Assessing Staff Acceptance and Compliance with Information Security

Talal Alotaibi[1,2] and Steven Furnell[2,3]

[1] Cyber Security Department, Information Technology, Public Security MOI, Kingdom of Saudi Arabia
[2] Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK
[3] Centre for Research in Information and Cyber Security, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

Abstract

Despite the fact that management and decision makers have spent a great deal of money on protecting their data from any possible attack, several have occurred. Moreover, security specialists often establish a well-designed security policy. This research investigates the field of assessing staff acceptance and compliance with information security. Thus, significant factors influencing compliance are investigated and prioritised by this research. The study is conducted in a particular governmental organisation in Saudi Arabia. The study sample is 111 respondents. In terms of the survey result, information security is influenced positively by factors relating to certainty of control (94%), awareness programs (93%), sanctions (93%) and reward (78%). However, the factor relating to trust between employees affects negatively by 45% on information security.

Keywords: Information security, technology, security policy, awareness, sanction, reward.

Introduction

Protecting information from malicious external attack is not enough; organisations should also pay attention to internal attacks. Therefore, the human factor should be considered as the backbone of information security, and raising employees' knowledge, skills and awareness regarding information security should minimise obvious information threats.
Staff compliance with information security is influenced and affected by various significant elements, including but not limited to sanctions, rewards, certainty of control, trust between employees and awareness programs. Therefore, this research investigates and prioritises the factors that have an obvious influence on employees' compliance with information security, and may help organisations to learn more about their employees' compliance as a result.

Background and related works

Although installing new technology devices, such as Intrusion Prevention and Detection Systems and firewalls, is significant in terms of information security, the human factor also plays a crucial role in the success or failure of security systems. In particular, the way that people behave can have significant impacts upon the resulting security of their organisations. For example, employees may use their flash memory devices in the work's computers and Internet cafés. As a consequence, the malware could move between the computers and become inadvertently introduced into the workplace. Decision makers in organisations aim to enhance the awareness of end users dealing with the technology to get the best compliance with information security policy and to avoid user misuse [1].

Using robust hardware is not enough to attain successful information security. Furnell and Thomson [2] state that when employees do not care about information security, this will increase the number of information security threats. However, using well developed, formally documented security policy is one way of ensuring successful information security. Therefore, most organisations now apply security policy [3].Acceptance of security policy reflects how successful the security policy is. All staff within organisations need to understand the security policy and threats to ensure that they accept and comply with this policy. Thus, organisations concentrate on increasing employees' security policy and threats awareness. The Information Security Breaches Survey 2015 [3] suggests that both large organisations and small businesses make sure staff are aware of security threats.

Firstly, prior studies have shown that using rewards is highly subjective; while they might be effective with one person, they might not be with another [4]. A number of studies have proven that despite the fact that rewards are a factor in influencing employees to perform their tasks effectively they do not have a significant effect on employees' acceptance of information security protocols [4]. Secondly, a number of studies have found that sanctions have a positive influence on information security compliance[5]. However, other studies suggest that sanctions do not have a significant influence on information security compliance [6]. Thirdly, it can be argued that rewards and punishments should be more efficient motivators when employees know that there is certainty of control. The timing of a reward or punishment plays a crucial role in its efficacy. For instance, employees are more careful about their behaviour when they are aware that the reward or punishment will be imposed immediately. Therefore, acceptance of and compliance with the policy might be enhanced when the employees know that the organisation is monitoring them, that it will not accept any misuse of policies and that a punishment will be imposed immediately [6]. Fourthly, trust is a significant aspect of human life. In organisations, levels of trust tend to increase among employees over time. Sometimes trust can negatively affect information security compliance [7]. Finally, Furnell and Thomson [2] argue that the greatest threats to information security occur when employees do not care about information. A large number of studies have found a strong relationship between awareness programs and information security compliance. This relationship has a positive effect on information security compliance [8].

Methodology

Although identifying the most significant factors is difficult, this work has concentrated on five factors: rewards, sanctions, certainty of control, trust between employees and awareness programs. There are a number of reasons for this. Firstly, there is a lack of research dealing with this field in Saudi Arabia. Secondly, there is no clear view regarding the significant factors that have obvious influence.

Therefore, this study objective to investigate and prioritise the factors that influenced the human factor, which are rewards, sanctions, certainty of control, trust between employees and awareness programs, and employees' compliance with information security policy.

Hypotheses. Based on background and related works section, staff compliance with information security might be affected by significant factors. A large number of studies have been carried out in this particular field. Although staff compliance with information security is influenced by five factors: rewards, sanctions, certainty of control, trust between employees and awareness programmes, there is no fixed view amongst researchers regarding how significant the factors are in terms of influencing compliance. Therefore, this work assumes five hypotheses. Each hypothesis indicates one factor.

- H1: There will be a significant relationship between information security compliance and the imposition of sanctions.
- H2: Rewards will have an effect on employees' information security compliance.
- H3: There will be a significant association between certainty of control and employees' information security compliance.
- H4: There will be a negative relationship between the trust between employees and their information security compliance.

- H5: Awareness programs will have a strong positive effect on information security compliance.

Proposed Research Model. The proposed research model is based on previous studies in section 2. Figure 1 shows the proposed research model that describes the relationship between information security compliance and the five factors that influence employees' compliance.

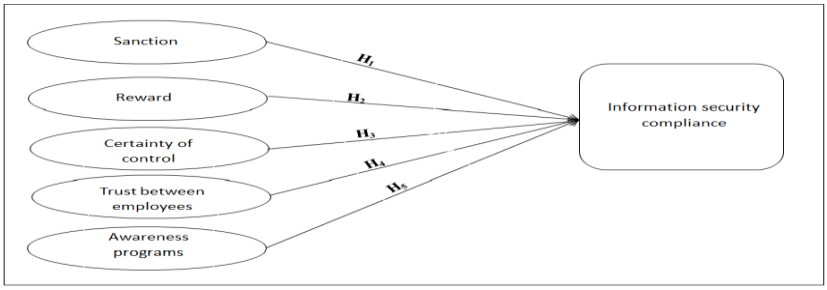

Figure 1: Proposed Research Model

This research work has chosen five factorsto evaluate and prioritise. The reason for this is the dearth of studies carried out in Saudi Arabia. Therefore, this study will be applied in a specific governmental organisation in Saudi Arabia.

Analysis

There were 111 participants. The survey consisted of two main parts. The first part was comprised of six questions used to elicit demographic information. The responses to these questions helped the analyst to classify the participants into sub-groups according to age, gender and educational level. Furthermore, they related to the employees' previous knowledge, skills and programs undertaken on information security compliance, thereby helping the analyst to assess compliance with IS. The second part included seven statements designed to evaluate and assess information influencing security compliance according to five significant factors, as discussed in the literature review. This was accomplished by evaluating employees' attitudes concerning the following areas:

- In life, trust can lead people to share secret values. What is the impact of trust between employees on information security compliance?
- Rewards represent an extremely significant variable and encourage humans to respond to/obey instructions. What is the impact of reward on information security compliance?
- Sanctions drive people to obey instructions. What is the impact of sanctions on complying with information security?
- The way in which an organisation applies any rule, including rewards/sanctions, will affect employees accordingly. Does the quick response of applying a reward/sanction (certainty of control) have an obvious influence on information security compliance?
- What is the impact of awareness programs on information security compliance?

Demographic Analysis. The results indicated that employees aged 18-30 are more likely to be non-compliant with information security rather than employees aged 41-50 as the ratio was almost 7% versus 0%. The reason for this might be that older employees are more likely to have been on a number of security programs.

Approximately 7% of the participants were women, while 93% were men. The most likely reason for this difference is that there are far less females in Public Security due to cultural reasons in this organisation. Reward did not have an obvious influence on compliance, whereas sanctions and certainty of control had a significant effect on females. Also, female compliance was not influenced by the trust between employees factor. On the other hand, 73% of the males had received information security training and were

significantly influenced by these. However, the trust between employees factor negatively influenced males by about 50%.

Lack of education would not be expected to reduce compliance as the findings illustrate that 100% of the employees who were less educated than diploma were complying with information security. However, education increases the possibility of compliance because educated employees are more likely to understand information security and know more about the threats that might be caused by non-compliance.

If an employee has been in an organisation for a long time, they might be more compliant because they are more familiar with the organisation's environment and rules. The findings showed that respondents who had been in the organisation for over 10 years were more compliant than others who had been there for less than five years, with a difference of approximately 8%. Employees who work in IT departments are more likely to comply with information security because working in an IT environment they will of course be more aware of the problems that might be caused by non-compliance. This can be seen in the findings, which revealed that employees who worked in IT departments were 5% more compliant than other employees. About a quarter of non-IT employees had not taken part in training programs, which might make them less likely to comply. This was supported by the findings, which showed that about 4% of the respondents who worked in non-IT departments and had not taken part in training programs did not comply with information security.

Factors That Influence In Information Security Compliance. This section of the survey aimed to assess employees' compliance with information security. Five factors were evaluated and prioritised according to the responses. The survey showed that about 78% of the respondents intended to comply all the time with information security, whereas 18% intended to comply sometimes. Only approximately 4% of the respondents did not intend to comply. It was observed that compliance is correlated with the number of years in the organisation. This is perhaps because long-term employees are more comfortable and familiar with the organisation and its rules. The results of the survey show that only 5% of the respondents who had been in the organisation for less than one year complied with security, whilst 25% of those who have been there for 1-5 years were compliant, 30% of those who had been there for 6-10 were compliant and 41% of those who had been there for more than 10 years were compliant. In terms of reward factor, the results showed that the male respondents were more likely to be influenced by this factor than the females by 16%. This might be because in Saudi Arabian culture the man takes responsibility for spending money on his family, even on his wife.In order to sanction factor, the results show that most employees are positively affected by sanctions. This factor is more effective than rewards, but if organisations use both rewards and sanctions, compliance should increase based on previous statistics. According to the findings, sanctions are more effective if they are related to receiving information security training. Respondents who had taken part in information security training were more influenced by sanctions than respondents who did not receive information security training, specifically by 48%.

Regarding to certainty of control factor, the findings indicates that a high percentage of the employees were influenced positively by certainty of control when they felt the organisation they worked in effectively monitored misuse because employees expect to receive a sanction or reward due to their behaviour immediately. Thus, a combination of the previous three factors is a significant requirement in gaining compliance with information security. It is can be observed that this factor is more likely to influence employees who have been in the organisation for less than 5 years than others who have been in the organisation over 6 years because the former employees might be less familiar with their organisation and need this factor to encourage them. From the results, 100% of the respondents who had been in the organisation for less than 5 years were influenced by this factor, whereas 91% of the employees who had been in the organisation for over 6 years were influenced by it.

In terms of trust between employees factor, approximately 6% of the respondents commented that sharing a password with a colleague is wrong but sometimes special circumstance force employees to do that. The results indicate that trust in colleagues has an obvious negative influence on compliance because more than a third of employees are willing to break information security policy. This high number indicates that employees in this field need to take part in more awareness programs because they are confused about trust boundaries and breaking security policy. From the results, the respondents who received training about

information security were less influenced than those who did not receive training, specifically by 4%.Moreover, employees working in an IT department are less likely to be influenced by this factor as those employees are more aware of information security and the security threats caused by humans. The findings illustrated that the respondents who worked in IT departments were negatively influenced by this factor by 46%, whereas those who worked in non-IT departments were negatively influenced by 50%.

Only about half of the employees would not be comfortable sharing secret information with their manager, whilst conversely the rest are willing to share secret information. This indicates that trust between employees is a factor that negatively affects compliance. Therefore, the solution to overcoming this factor is to increase awareness programs as there is an obvious lack of understanding amongst employees about the threat caused by trust. In terms of trust awareness programs factor, the results show that most of the employees would be positively influenced by awareness programs. Moreover, this factor was mentioned many times in the respondents' comments because they thought that awareness programs were the first line of defence against attacks on security, increasing compliance and even dealing with the trust between employees factor.

Discussion of results

A number of studies have found that although reward is a factor in influencing employees to achieve their tasks effectively, it does not have a effect on employees' acceptance of information security [4]. On the other hand, rewards can be used effectively to prevent violations, while sanctions are not so efficacious in preventing them [6].In this work, the results of the survey showed that a large number of employees agreed that rewards positively influence information security compliance.

From the sanctions factor perspective, a number of studies claim that sanctions have a positive influence on information security compliance [5]. Meanwhile, other studies suggest that sanctions do not have an obvious effect on information security compliance [6]. In this work, the findings indicated that sanctions are a key factor that increases compliance with information security.

According to Chen et al., compliance with information security would be enhanced positively if employees were aware that organisations were monitoring them effectively and a punishment would be imposed immediately [6]. The results of this work showed that a high percentage of employees believed that effective monitoring of misuse would increase the likelihood of compliance.

Recent research has proven that sometimes trust between employees might negatively influence information security compliance [7]. In this work, the results indicated that this factor has an obvious negative influence as about a third of employees were willing to break information security policy with their colleagues or managers. There are several reasons for this from the employees' perspective. A large number of employees who were willing to break information security policy believed that trust between employees makes achieving daily task easier and faster. Finally, a large number of studies have proved that there is a strong positive relationship between awareness programs and information security compliance [8]. The findings of the survey in this work showed that a high percentage of employees agreed that awareness programs increase the likelihood of compliance with information security. Furthermore, a reasonable number of employees commented that awareness programs are the solution to issues associated with rewards, sanctions and trust between employees.

Generally, the results confirm support for all five hypotheses, as above. Figure 2 shows the resulting model from conducting the study. The weight of each factor has been calculated individually based on the survey results.

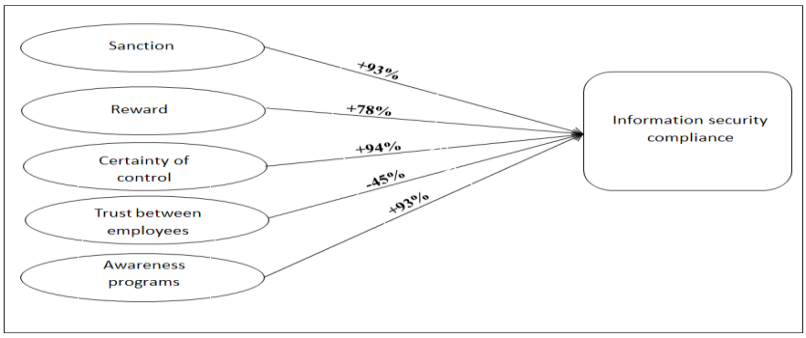

Figure 2: Resulting Model

The findings of the survey provide an opportunity to prioritise the five factors that influence information security compliance. Awareness programs are allocated the first rank because a high percentage, approximately 66%, of employees said that they are the factor that influences information security compliance the most. Moreover, a high percentage of employees, about 93%, chose awareness programs to raise information security compliance and a number of employees commented that awareness programs can help avoid issues associated with others factors. Certainty of control is ranked second. The effective monitoring factor was given 31% by employees in terms of ordering the factors. Furthermore, a high percentage of employees, almost 94%, agreed that effective monitoring of misuse increases information security compliance. Sanctions are ranked third. The findings show that about 20% of employees chose sanctions as an influencing factor. In addition, roughly 93% of employees believed that the presence of a sanction increases compliance with information security. Rewards are ranked fourth. Only 2% of employees put rewards as the first influencing factor. Furthermore, about 78% of employees said that the presence of a reward increases the likelihood of complying with information security policy. Finally, all the previous four factors have a positiveeffect, whereas trust between employees is ranked fifth and has a negative influence as about half of the employees were willing to break information security policy.

Conclusions

The purpose of this research is to help organisations to assess their staff in order to improve information security compliance and to identify the significant factors that influence compliance. Generally, the findings of the survey confirmed the proposed model and all five hypotheses. Regarding prioritising the factors, the winning factor was awareness programs. Certainty of control was ranked second. The findings put the sanctions factor in third place, and the rewards factor was ranked fourth. Finally, trust between employees was ranked fifth. A major limitation of this research work was obtaining a large enough number of participants who were working in the targeted organisation in Saudi Arabia to reveal employees' real attitudes. Furthermore, a number of participants did not complete the questionnaire, which impacted on the overall number.

References

[1] Sommestad, T., Hallberg, J., Lundholm, K. and Bengtsson, J. (2014) 'Variables influencing information security policy compliance; A systematic review of quantitative studies'. Information Management and Computer Security, 22 (1).pp 42-75.

[2] Furnell, S. and Thomson, K. (2009) 'From culture to disobedience: Recognising the varying user acceptance of IT security'. Computer Fraud & Security, 2009 (2).pp 5-10.

[3] ISBS (2015) Information Security Breaches Survey 2015 - Technical report'.: www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf (Accessed: 12 July 2016).

[4] Siponen, M., Pahnila, S. and Mahmood, M. A. (2010) 'Compliance with information security policies: an empirical investigation'. Computer, 43 (2).pp 64-71.

[5] Siponen, M., Mahmood, M. A. and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study'. Information & Management, 51 (2).pp 217-224.
[6] Chen, Y., Ramamurthy, K. and Wen, K.W. (2012) 'Organizations' Information Security Policy Compliance: Stick or Carrot Approach?'. Journal of Management Information Systems, 29 (3).pp 157-188.
[7] Al-Mukahal, H.M. and Alshare, K. (2015) 'An examination of factors that influence the number of information security policy violations in Qatari organizations'. Information & Computer Security, 23 (1).
[8] 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).pp 523-548.