Demographic Profile and Intention to Comply with Security Policy in Financial Institutions in Malaysia

Ahmad Iqbal Hakim Suhaimi* and Anitawati Lokman

Universiti Teknologi MARA, Shah Alam, Selangor; aiqbal@tmsk.uitm.edu.my, anita@tmsk.uitm.edu.my

Abstract

Objectives: The aim of this research is to assess demographic profiles in security compliance intention on financial institutions in Malaysia. Methods/Statistical Analysis: Based on the correlation, the research attempts to identify areas that should be focused to improve employees’ intention to comply with policies in financial institutions. The research uses quantitative approach, and administers survey to one hundred respondents of a selected financial institution in Malaysia. Findings: The result shows there is no significant relationship in demographic profiles and security compliance intention in financial institution. Application/Improvements: In considering, financial institutions should emphasize their focus on policy making, employees training, and awareness program to improve the security policy compliance intention within the institutions.

Keywords: Demographics Profile, Information Security Policy, Security Compliance, User Behaviour

1. Introduction

A major challenge for the corporate organization is ensuring their employees comply with security policies. Information system security compliance is a process of discovering and preventing security problems which aims at minimizing the risks associated with information assets and misbehaviour among employees. Employees play an important role in the information security performance based on their awareness level and behaviour.

Demographic background has been seen as one of the factors that influence user behaviour. Several studies have been conducted to assess the relationship between demographic background or characteristic and behaviour in the context of security awareness. Information system security is more about controlling human behaviour. End users are not consistent in their behavioural intentions to comply with recommendations to protect their information assets. Some employees have intention not to comply with information system security due to either ignorance, reluctance, avoidance or sometimes altering organization’s monitoring equipment or software.

On the other hand, to secure client and financial data, it is imperative for financial institutions to deal with this information security compliance since the emerging of unified communication could significantly compromise the policies. Although such policies are implemented in the institutions, but to what extent employees comply with the policies and how their demographic background influences their security compliance are not clear. Employees have a profile that is unique to each one of them. Their age, gender, designation, education or years working is among factors that might have significant impact on information system security compliance.

Thus, the research aims to assess demographic profile and security compliance intention in Malaysian financial institution. The research objective is to determine correlations between employees’ profile based on their age, gender, years working, education and designation, and security compliance intention. This research sets its focus to employees of a target group from a selected financial institution in Malaysia which consists of employees from different department, job designation and scope of task, education, gender, age and year of service.

Policy is a crucial direction-giving document. It is a document that indicates board management’s commitment to and support of information security, as well as defining the role information security has to play in reaching and supporting the organizations’ goals. It creates a solid platform to implement secure practices.

*Author for correspondence
in an organization. However, having defined the policy does not ensure that all users will necessarily obey it. As a matter of fact, employees are far greater threat to information security than outsiders. Although organizations have a well-established security policy, they still encounter issues and challenges regarding security policy compliance because of human behaviour.

It is crucial to study the behaviour of people when implementing effective security solutions. The behaviour of people is often shaped based on the culture they assimilate into. The causes of sixty-six percent (66%) of computer attacks that occurred in Greece (a country as a case study) originate from employees' actions within the organizations. The success of information security is highly dependent on the employees' understanding which will directly influence their behaviour. According to, behaviour exhibited by employees is related to information security problems in an organization. The study indicated that an astounding eighty percent (80%) of large-scale security issues occur due to inefficient behaviour by employees.

Information system security compliance is also important to avoid intentional users' actions and the consequences that occur afterwards. Humans are seen as the 'weakest link' in the information security chain. The implementation of effective information system security compliance would help employees to understand the importance to comply with information system security compliance and assists the employees while completing their daily business operation.

Although a number of studies have studied policy compliance intention, the studies addressed policy compliance intention in general and do not consider differences in business goal of particular institution. A research model was proposed to assess the impact of security culture and the Employee-organization relationship on security compliance, as shown in Figure 1. Research Model Framework, with three variables; security variable, organization behaviour variable and control variable. All variables have critical factors, i.e. top management commitment, security communication, computer monitoring, job satisfaction, perceived organizational support and security compliance intention. Their control variable is age, gender and industry.

2. Methodology

The research conducted quantitative inquiry using open-ended and close-ended questionnaires as instrument used in a survey administration. The questionnaire was organized and grouped into two sections. Section 1 consists of five structured questions to extract demographic information from the participants: a) Age, b) Gender, c) Years working, d) Education, and e) Job title. Meanwhile, Section 2 consists of questions on security compliance intention. Online questionnaire survey was broadcasted via email.

Descriptive statistical analysis, and Regression analysis, T-Test and one-way ANOVA were performed to the collected data, and reported in the next section. The descriptive statistical analysis includes the respondents' demographic profiles and their responses on the compliance of information system security. On the other hand, Regression analysis, T-Test and one-way ANOVA were used to demonstrate whether demographic profiles have significant impact on employees' information system security compliance intention in the context of financial institution. The data analysis was performed to determine relationship between demographic profile based on age, gender, year service, education and job title security compliance intention. The hypotheses were analysed to see the result on security compliance intention. 6-point Likert scale was used in the close-ended questionnaires. The online and hardcopy questionnaires were distributed to 100 selected respondents from several departments based on age, gender, year service, education and job title.

Regression analysis was used to discover relationships between independent and dependent variables. T-Test analysis was used to examine relations between categories.

Figure 1. Research Model Framework.
like gender. On the other hand, ANOVA was used to analyse means among groups.

The research hypotheses for this study were as follows:

H1: Age has a significant effect on Security Compliance Intention
H2: Year Working has a significant effect on Security Compliance Intention
H3: Education has a significant effect on Security Compliance Intention
H4: Job Title has a significant effect on Security Compliance Intention
H5: Gender has a significant relationship on Security Compliance Intention

3. Result and Discussion

A total of 100 respondents have participated in the survey. The regression result analysis based on the independent and dependent variables are given.

Table 1. Model Summary shows that the r square is 0.060 which means 6% of the security compliance intention has been explained by educational level, job title, age, gender and year working.

Table 2. ANOVA Result shows the p-value = 0.453, which was greater than p-values > 0.05. This indicated that the implementation of regression analysis is appropriate for this study.

The beta coefficient was yielded from regression analysis which naturally adopted the weighted least square estimator. As in Table 3. Beta Coefficient, there were no significant factor exist. Moreover, the VIF were all below than 5.0, which mean the multicollinearity problem does not exist. It can be concluded that the factors involved in the study are not redundant.

Table 4. Research Hypothesis presents analysis result to the research hypotheses. The analyses showed that there were no significant effect on security compliance intention and the rest of research hypothesis were not supported to security compliance intention.

One-way ANOVA analysed the result based on each categories of independent variable. For instance, there are different type of education level, such as master, bachelor, diploma, high school and others. One-way ANOVA was used to determine the highest effect.

3.1 Age

Table 5. Age - Security compliance shows mean of security compliance intention for each categories of age. The result obtained shows the respondents among ‘31-40’ are having the highest interest on security compliance intention in management. Instead, the respondents among ‘41-50’ are having the lowest interest on security compliance intention in management.

The significant value of the ANOVA table is 0.224, which is greater than 0.05. Hence, the null hypothesis is accepted, which means that the security compliance intention in management has no difference with age.

3.2 Year Working

Table 7. Year Working – Security compliance shows mean of security compliance intention for each categories of
year working. The result obtained shows the respondents among '7 – 8' are having highest interest on security compliance intention. Instead, the respondents among '0' are having lowest interest on security compliance intention in management.

Table 2. ANOVA result

| Model       | Sum of Squares | df | Mean Square | F     | Sig. |
|-------------|----------------|----|-------------|-------|------|
| Regression  | 1.561          | 5  | .312        | .951  | .453 |
| Residual    | 24.287         | 74 | .328        |       |      |
| Total       | 25.848         | 79 |             |       |      |

a. Predictors: (Constant), Edu Level, Job Title, Age, Gender, Year Working
b. Dependent Variable: security compliance

The significant value of the ANOVA table is 0.731, which is greater than 0.05. Hence, the null hypothesis is accepted, which means that the security compliance intention in management has no difference with year working.

3.3 Education

Table 9. Education – Security Compliance and Table 10. Education – Security Compliance (ANOVA) illustrate that education has no significant difference in mean for security compliance intention in management.

3.4 Job Title

Table 11. Job Title - Security Compliance (Descriptive) and Table 12. Job Title – Security Compliance (ANOVA)
Table 6. Age – security compliance

|          | Sum of Squares | df | Mean Square | F   | Sig. |
|----------|----------------|----|-------------|-----|------|
| Between Groups | .986          | 2  | .493        | 1.527 | .224 |
| Within Groups    | 24.862        | 77 | .323        |      |      |
| Total            | 25.848        | 79 |             |      |      |

Table 7. Year working – security compliance

|         | N   | Mean  | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | Minimum | Maximum |
|---------|-----|-------|----------------|------------|---------------------------------|---------|---------|
| 0-1     | 5   | 2.0889| .70885         | .31701     | 1.2087                          | 2.9690  | 1.00    |
| 1-2     | 9   | 2.3951| .35185         | .11728     | 2.1246                          | 2.6655  | 1.89    |
| 3-4     | 25  | 2.5085| .63803         | .12513     | 2.2508                          | 2.7663  | 1.00    |
| 5-6     | 13  | 2.4188| .50543         | .14018     | 2.1134                          | 2.7242  | 1.44    |
| 7-8     | 13  | 2.8632| .27649         | .07669     | 2.6962                          | 3.0303  | 2.22    |
| 9-10    | 7   | 2.6984| .67194         | .25397     | 2.0770                          | 3.3199  | 2.00    |
| >16     | 7   | 2.0952| .54970         | .20777     | 1.5868                          | 2.6036  | 1.00    |
| Total   | 79  | 2.4931| .57201         | .06395     | 2.3658                          | 2.6203  | 1.00    |

Table 8. Year working – security compliance (ANOVA)

|          | Sum of Squares | df | Mean Square | F   | Sig. |
|----------|----------------|----|-------------|-----|------|
| Between Groups | 4.166         | 6  | .694        | 2.737 | .060 |
| Within Groups    | 21.682        | 73 | .297        |      |      |
| Total            | 25.848        | 79 |             |      |      |

Table 9. Education – security compliance

|        | N   | Mean  | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | Minimum | Maximum |
|--------|-----|-------|----------------|------------|---------------------------------|---------|---------|
| Master | 4   | 2.6111| .51719         | .25860     | 1.7881                          | 3.4341  | 2.11    |
| Bachelor | 58 | 2.4923| .60612         | .07959     | 2.3330                          | 2.6517  | 1.00    |
| Diploma | 12 | 2.5185| .50438         | .14560     | 2.1981                          | 2.8390  | 2.11    |
| High School | 3 | 2.1852| .16973         | .09799     | 1.7636                          | 2.6068  | 2.00    |
| Other   | 2   | 2.8889| .47140         | .33333     | -1.3465                         | 7.1243  | 2.56    |
| Total   | 79  | 2.5007| .57153         | .06430     | 2.3727                          | 2.6287  | 1.00    |

Table 10. Education – security compliance (ANOVA)

|          | Sum of Squares | df | Mean Square | F   | Sig. |
|----------|----------------|----|-------------|-----|------|
| Between Groups | .657          | 4  | .164        | .489 | .743 |
| Within Groups    | 24.822        | 74 | .335        |      |      |
| Total            | 25.478        | 78 |             |      |      |

Table 11. Job title – security compliance (Descriptive)

|            | N   | Mean  | Std. Deviation | Std. Error | 95% Confidence Interval for Mean | Minimum | Maximum |
|------------|-----|-------|----------------|------------|---------------------------------|---------|---------|
| Dpt./Op. Manager | 5  | 2.4000| .33633         | .23986     | 1.7341                          | 3.0659  | 2.00    |
| IT Manager  | 8   | 2.3750| .32496         | .14899     | 2.1033                          | 2.6467  | 2.00    |
| IT Staff    | 26  | 2.5641| .53048         | .10404     | 2.3498                          | 2.7774  | 1.00    |
| Security Manager | 13 | 2.4444| .78436         | .21754     | 1.9705                          | 2.9184  | 1.00    |
| Security Officer | 13 | 2.5214| .72063         | .19987     | 2.0859                          | 2.9568  | 1.00    |
| Security Staff | 6   | 2.5556| .50185         | .20488     | 2.0289                          | 3.0822  | 2.00    |
| Operation Staff | 8  | 2.5000| .43644         | .15430     | 2.1351                          | 2.8649  | 2.00    |
| Total       | 79  | 2.5007| .57153         | .06430     | 2.3727                          | 2.6287  | 1.00    |

Table 12. Job title – security compliance (ANOVA)

|          | Sum of Squares | df | Mean Square | F   | Sig. |
|----------|----------------|----|-------------|-----|------|
| Between Groups | .346          | 6  | .058        | .165 | .985 |
| Within Groups    | 25.132        | 72 | .349        |      |      |
| Total            | 25.478        | 78 |             |      |      |
illustrate that job title has no significant difference in mean for security compliance intention in management.

3.5 Gender
The means of security compliance intention between male and female. Table 13. Group Statistics indicates that the mean to security compliance intention for male is higher as compared to female.

Based on the above results, it can be concluded that all variables do not have significant effect on security compliance intention. The result of this research indicated that demographic background does not have significant effect on intention to comply with the information security system in an organization. Thus, focus point must be shifted to another angle. Financial institutions should have emphasized their focus and effort on policy making and employees training and awareness program to improve the security policy compliance.

The objective of any organizational policy is to determine employees' course of action. Most organizations have a challenging issue to ensure all workers comply with their security policies based on several reasons. Poor quality, aside from the lack of context, weak structure, grammatical errors, undefined terminology and loose ends policies are often written in a way that is not easy to read, hence become a hindrance for compliance. Thus, the process of policy making is a very crucial part towards compliance. To encourage compliance, the contents of the policy also should be easy to understand and aligned with business goal. Policy making should be based framework or security management best practices. Policy itself should shape the culture of employees with intention to comply with policy. Thus, financial institutions should emphasize their focus to make policy based on best practices.

Effectiveness of security compliance can be achieved through security awareness training of employees. A continuous information security awareness program should be in place to ensure initial education, and also regular updates and reminders. Due to the fact that the people in the organisations are actually the primary and the most critical line of defence security awareness programme is a ‘must’ for everyone in the organization. As our result has indicated that demographic background has not significant impact on security compliance, the awareness program is seen promising as a proposed solution and need to be conducted to all level of employees regardless of their gender, age, year service, education and job title.

4. Conclusion
The purpose of this study is to assess demographic profiles and how it affects security compliance intention in financial institutions in Malaysia by determining the correlations between employees' profiles based on the employees' age, gender, years working, education and designation, and security compliance intention. A financial institution was selected as a case study the results showed that there is no significant relationship in demographic profiles and security compliance intention in the financial institution. Instead of focusing on demographic background, the researches propose the financial institution should have emphasized their effort on policy making and employees training and awareness program to improve the security policy compliance intention within the institutions.

5. References
1. Chen Y, Ramamurthy KK, Wen K. Organizations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems. 2012; 29(3):157–88.
2. Lebek B, Uffen J, Breitner MH, Hohler B. Employees’ information security awareness and behavior: A literature review. Proceedings of HICSS’13; 2013. p. 2978–87.
3. Schneier B. Beyond fear – thinking sensibly about security in an uncertain world. Copernicus Books; 2003
4. Johnston AC, Warkentin M. Fear appeals and information security behaviors: An empirical study. MIS Quarterly. 2010; 34(3):549–66.
5. Stanton JM, Julian AI. The impact of social cues about an EPM system on performance quality and quantity. Computers in Human Behavior. 2002; 18(1):85–101.
6. Stanton JM, Weiss EM. Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. Computers in Human Behavior. 2000; 16(4):423–40.
7. Karin H, Petrus EjH. Information security procedure - What do international information security standards says? International Journal of Computers and Security. 2002; 21(5):402–9.
8. International Organization for Standardization. ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements; 2005.

9. Von Solms R, Von Solms B. The 10 deadly sins of information security management. International Journal on Computers and Security. 2004; 23:371–6.

10. Von Solms R, Von Solms B. From policies to culture. International Journal on Computers and Security. 2004; 24(3):275–9.

11. Debi A. Information security management: A human challenge. International Journal of Information Security Technical Report. 2008; 13(4):195–201.

12. Lim JS, Chang S, Maynard S, Ahmad A. Exploring the relationship between organizational culture and information security culture. Proceedings of Australian Information Security Management Conference; 2009. p. 12.

13. Koskosas I, Kakoulidis K, Siomos C. Information security: Corporate culture and organizational commitment. International Journal of Humanities and Social Science. 2011; 1(3).

14. Chan M, Woon I, Kankanahalli A. Perceptions of information security at the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy and Security. 2005; 1(3).

15. Pahnila S, Siponen M, Mahmood A. Employees' behavior towards is security policy compliance. Proceedings of HICSS’07; 2007.

16. Greene G, D’Arcy J. Assessing the impact of security culture and the employee-organization relationship on IS security compliance. Proceedings of Proc ASIA’10; 2010.

17. Burcu B, Hasan C, Izak B. Information Security procedure Compliance: An empirical study of rationality-based beliefs and information security awareness. International Journal of MIS Quarterly. 2010; 34(3):523–48.

18. Zoran C, Marija B. Information security management – defining approaches to information security policies in ISMS. Proceedings of SISY’10; 2010. p. 83–5.

19. Mete E, Erdem U, Şaban E. The positive outcomes of information security awareness training in companies - A case study. Information Security Technical Report. 2009; 14(4):223–9.

20. Tipton HF, Krause M. Information security management handbook. Auerbach Publications; 2007.

21. Scholtz T, Byrnes FC, Heiser J. Best practices and common problems for information security programs, Gartner; 2006.