HAL open science

Demographic Factors in Cyber Security: An Empirical Study

Shweta Mittal, P. Vigneswara Ilavarasan

To cite this version:

Shweta Mittal, P. Vigneswara Ilavarasan. Demographic Factors in Cyber Security: An Empirical Study. 18th Conference on e-Business, e-Services and e-Society (I3E), Sep 2019, Trondheim, Norway. pp.667-676, 10.1007/978-3-030-29374-1_54 . hal-02510112

HAL Id: hal-02510112

https://inria.hal.science/hal-02510112v1

Submitted on 17 Mar 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Demographic factors in cyber security: An empirical study

Shweta Mittal[1*]and P Vigneswara Ilavarasan[1]

[1]Department of management studies, Indian Institute of Technology, Delhi
f12shwetam@iima.ac.in, vignes@iitd.ac.in

Abstract. Despite high quality information systems security in place, organizations are vulnerable to cyber-attacks due to lapses in the human behavior. The present paper explores the importance of human factors in cyber security using an online survey data. It uses the work of Parson, Calic, Pattenson, Butavicius, McCormac&Zwaans (2017) in measuring the human aspects of cyber security (leaving printouts, links from known source, website access, information in website, password complexity, links from known source, plugging USB in public places) and their linkages with the demographic factors (age, work experience, academic discipline, qualification, and place). ANOVA was used on a sample size of 165. It was found that demographic profile of employees and students significantly differ in their perception towards the cyber security. The paper has suggestions for information security awareness training programmes to handle the inadequacies.

Keywords: Demographics, ANOVA, Human Aspects of Information Security Questionnaire, cyber security

1. Introduction

Humans can cause risk to cyber security, as any technical security solution or operation can fail due to the human error. Information security threats cannot be stopped, evaded, noticed or eradicated by completely relying on technological solutions [14,15,36]. Behavior of computer users' can pose danger to an organization's computer system. Human behaviors can probably put the organization at danger by unintentionally or intentionally revealing the passwords to others, providing sensitive information by clicking on embedded web site links, or putting unknown media into work computers. Research has found that human is the weakest link in safe guarding the organization's information security system [13]. Computer users' immature and unintentional behaviors are the reason behind information security breaches[24, 28, 39]. The data of the current research states that 95 percent of security breaches incidents are due to human errors. A technological system doesn't guarantee a secure environment for information [30]. It needs to be collaborated with mature human behaviors. [35] enquired about information security and cyber security, though they are related but can be compared. Information security consists of availability, integrity, and confidentiality. Cyber security also comprises of humans in their personal capacity and society at large. In organizations, security on both the fronts can be established by collaboration of technology and human behaviors [37].

Information security breaches can cost heavily to organizations and can also affect their reputation [29]. Many studies suggest that employees' information security awareness plays an important role to attenuate the risk associated with their behavior in organizations [1, 3]. Organizations invest heavily in technological aspects of information security and tools but still security breaches incidents continue due to the lack of attention to employees in organizations [16].

Cyber security is of paramount importance to individuals and organizations to safeguard important and sensitive information about the clients. The researchers have found that different human characteristics lead to low security practices and are more prone to be a part of cybercrimes, still the work is limited in this area [11]. The research hassuggested that information security awareness (ISA) is important inlowering the risks linked with information security breaches [3, 31]. Humans are consistently being called as "the first line defense" against the information security threats [12, 26]. We have used the Human Aspects of Information Security Questionnaire (HAIS-Q) developed by [23] to understand the different aspects of cyber security factors with respect to demographics.

Through a survey of 165 respondents comprising ofstudents, working professionals at India, Bangladesh and other places, we make the following contributions.

- We used the HAIS- Q questionnaire and found that knowledge, attitude and behavior (KAB) model didn't hold well in our population.
- We deducted the constructs like password sensitivity, password complexity, links from known source, links from unknown source, and etc. with the reliability 0.60 and above.

We expand on the work of [23] by using ANOVAto delineate the linkage between demographic factors and cyber security.

The paper consists of seven sections. The first section introduced the paper. The section twoshares the theoretical background of the research. The section three discusses the importance of demographics. The section four presents the methodology. The fifth section covers the analysis and findings of the study. The sixth section discusses the findings. The final section concludes the paper with suggestions for future work.

2. Theoretical Background

In today's scenario, dangers associated with information security pose major challenges for most of the organizations, as these dangers have dire consequences, including corporate liability, loss of credibility, and monetary damage [7]. In organizations ensuring information security has become an utmost managerial priority as well as responsibility [5, 21, 27]. Research on the human perspective of information security have focused on the employee behaviors and have found the factors that lead to risk the information security. The employees can risk the information security because of

their ignorance, mistakes, and deliberate acts [10, 19, 20]. Organizations are organizing technological systems to safeguard their information and technological resources, but still they depend on their employees. Employees who are consistently using information and technology resources take certain roles and responsibilities in protecting those resources, so we are interested in what demographic factors are responsible for ensuring these roles and responsibilities.

Thus, we can understand how much the demography differences of employees understand the need and impact of information security. If the demography differences of employees are not reflecting information security behavior, then the organizations need to tailor the training programs to influence or cultivate positive attitude towards cyber security.

3. Demographics and Hypotheses

Demographics include number of characteristics in a human population. We have focused on the following demographic characteristic: age, place, qualification, academic discipline, work experience and sector working presently. These represent demographic characteristics which we analyzed howcyber security varies according to the differences in age, place, qualification, academic discipline, work experience and sector working presently. [9]found liberal arts students to be more susceptible to attacks than other majors. [22] however, suggested demographics were not conclusive in predicting attack susceptibility. There are few researches showing how demographics influence cyber security behaviors. [38] found that younger people were significantly more likely to engage in the poor security practice of password sharing. [34] found that age is an important demographic predictor in organizations. To this, the prior research states that increasing age has lower attitudes towards its usage [18], and acceptance behavior [8]. The reasoning for this could be that older people have less computer experience, less open to change, and relatively are not good in managing computer related documents. Further, older employees are more inclined to social activities than in knowledge acquisition [6]. This could be another reason for older employees being insensitive towards leaving the printouts. Individuals with lesser job tenure are more inclined towards learning new things [33, 32, 25]. This rationale could be the probable reason that employees with lesser experience are more susceptible to clicking the links from known source, may be thinking that there could be some new knowledge or information. Research clearly shows that education level (EL) is directly associated to knowledge skills, and has positive effect related to behavior [2, 17]. Thus, through this reasoning we can say that PhD qualified people have an intention to share or contribute new learning enters the information in website, forgetting that it could be detrimental to organization's security. Further, different places and academic discipline have different information security issues.
The following research questions were investigated:

1. Is there a difference in 'Leaving print outs' across different age groups?

2. Does the links from known source vary according to the work experience?
3. Isthere difference in 'Website accesses across different academic disciplines?
4. Does the cyber security (information in website) vary according to the qualification?
5. Is there a difference in password complexity across different places?
6. Is there a difference in clicking links from unknown sources across different places?
7. Is there a difference in plugging USB in public places across different places?

4. Research Methodology

This research expanded the work done by the [23] on human aspects of information security (HAIS). This research will help in comprehending different aspects of cyber security with respect to demographic differences. We used Parson & team's HAISquestionnaire. In order to examine the questions, Analysis of Variance (ANOVA) was used to test the differences across different groups.

4.1 Data Collection

Thedata were collected from the employees and students of India, Bangladesh and other countries. We used the electronic version of the questionnaire and sent the link to the participants. This helped the respondent to answer the questions at any time and place, and this way we accelerated the process of data collection. With the aid of Google, we received 200 questionnaires electronically. Thirty-five questionnaires were not considered because of their incongruent responses. Finally, we received 165 questionnaires for data analysis.

4.2 Sample

The sample of 165 consisted of working (78.3%) and non-working (19.3%) professionals from India (70.5%), Bangladesh (26%) and other countries (3%). A total of 81% of respondents were Male. The mean age was 29.41 years, with an average experience of 5.74 years. The sample was composed of arts and commerce (8.4%), management and social science (55.4%), science (4.2%) and engineering (29.5%) backgrounds. It comprised of undergraduate (30.7%), post graduate (59.0%) and PhD (9.6%).

5. Measures

We used the HAIS- Q questionnaire and extracted eighteen constructs with the reliability 0.60 and above. The deducted constructs with reliability are given in Table 1.

Table 1. Reliability of the constructs

Focus Area	Sub Area	Reliability
Password Sensitivity	It's acceptable to use my social media passwords on my work accounts.	0.71
	It's safe to use the same password for social media and work accounts.	
	I use different password for my social media and work accounts.	
Password Complexity	A mixture of letters, numbers and symbols is necessary for work passwords.	0.60
	I use a combination of letters, numbers and symbols in my work passwords.	
Attachments from un-known source	I am allowed to open email attachments from unknown senders.	0.64
	It's risky to open an email attachment from an unknown sender.	
	I don't open email attachments if the sender is unknown to me.	
Links from known sources	I am allowed to click on any links in emails from people I know.	0.62
	It is always safe to click on links in emails from people I know.	
Links from unknown source	Nothing bad can happen if I click on a link in an email from an unknown sender.	0.64
	If an email from an unknown sender looks interesting, I click on a link within it.	
Download file	I am allowed to download any files onto my work computer if they help me to do job.	0.75
	I download any files onto my work computer that will help me get the job done.	
Website Access	While I am at work, I shouldn't access certain websites.	0.61
	Just because I can access a website at work, doesn't mean that it's safe.	
Information in website	I am allowed to enter any information on any website if it helps me do my job.	0.72
	If it helps me to do my work it doesn't matter what information I put on a website.	
Social Media Privacy	I must periodically review the privacy settings on my social media accounts.	0.62
	It's good idea to regularly review my social media privacy set-tings.	
	I don't regularly review my social media privacy settings.	
Work infor-mation on social media	I can post what I want about my work on social media.	0.68
	It's risky to post certain information about my work on social media.	
Laptop Care	When working in a café, it's safe to leave laptop unattended for a minute.	0.79
	When working In a public place, I leave my laptop unattended .	
Public Wi-Fi and Sensi-tive files	I am allowed to send sensitive work files via a public Wi-fi net-work.	0.64
	It's risky to send sensitive work files using a public Wi-fi net-work.	
	I send sensitive work files using public Wi-fi network.	
Strangers	When working on a sensitive document, I must ensure that strangers can't see my laptop.	0.85

and Sensitive file	It's risky to access sensitive work files on a laptop if strangers can see my screen.	
	I check that strangers can't see my laptop screen if I'm working on a sensitive document.	
Disposing the sensitive printouts	Sensitive printouts can be disposed of in the same way as non-sensitive ones.	0.75
	Disposing of sensitive print-outs by putting them in the rubbish bin is safe.	
	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.	
Plugging USB in public places	If I found a USB stick in a public place I shouldn't plug into my work computer.	0.76
	If I find a USB stick in a public place nothing bad can happen if I plug it into my work computer.	
	I wouldn't plug a USB stick found in a public place into my work computer.	
Leaving printouts	I am allowed to leave print-outs containing sensitive information on my desk overnight.	0.66
	It's risky to leave print-outs that contain sensitive information on my desk overnight.	
Reporting of suspicious acts	If I see someone acting suspiciously in my workplace, I should report it.	0.72
	If I ignore someone acting suspiciously in my workplace nothing bad can happen.	
	If I saw someone acting suspiciously in my workplace, I would do something about it.	
Security behavior of colleagues	Nothing bad can happen if I ignore poor security behavior by a colleague.	0.80
	If I notice my colleague ignoring security rules, I wouldn't take any action.	

5.1 Data Analysis and Results

Cyber Security: Leaving Printouts

A one-way ANOVA was conducted to understand the perception of respondents towards leaving printouts, in accordance to their age. Leaving printouts perceptions varied according to the age at $p < .05$ for the four conditions [$F(3,157) = 2.89$, $p=.037$]. Post hoc comparisons using the Turkey B test indicated that the mean score for the age range (>25 and <=27) (M=4.52) and (<=25) (M=4.16) was significantly different than the age range (> 32 and <=50) (M=3.94).

Cyber Security: Links from known source

We found that Links from known source vary according to the experience of employees in organization by conducting one-wayANOVA at the $p < .05$ for the four conditions [$F(3,159) = 3.727$, $p=.013$]. Post hoc comparisons taking the Turkey B test

indicated that the mean score for the work experience (<=2) (M=2.97) was significantly different than the work experience (2 and <=3) (M= 3.56) and (>8 and <=28) (M=3.57).

Cyber Security: Website Access

Again, by applying ANOVA we found website access perception was different for the academic discipline at $p < .05$ for the four conditions [F (3,156) = 4.19, p=.001]. The mean score of the academic discipline Arts and Commerce (M=3.32) was significantly different from Management and Social Science (4.06), Science (4.32) and Engineering (4.57) by using Turkey B test of Post hoc comparisons.

Cyber Security: Information in website

Information in website varied according to the qualification by using one-way ANOVA at the $p < .05$ for the three conditions [F (2,159) = 4.79, p=.01]. The mean score for the PhD qualified people (M=2.94) was different from Post Graduates (3.72) and Undergraduate (3.72) by Turkey B test.

Cyber Security: Password complexity and Links from known source

Password complexity and links from known source didn't vary according to the place. We used one-way ANOVA to get the results.

Cyber Security: Plugging USB in public places

Plugging USB in public places varied according to their place by applying ANOVA. Plugging USB in public places was significantly different according to the place at the $p < .05$ for the three conditions [F (2,158) = 3.09, p=.048]. The mean score for other Places (M=4.80) significantly varied from Bangladesh (M=4.06) and India (M= 4.31) by using Turkey B test.

6. Discussion and Findings

The results clearly states that there is a need to increase security awareness, and it has been found that security awareness training is the most cost- effective form of security control [4]. Precisely, from the results, we can advocate that the culture of cyber security needs to be cultivated by providing training and workshops by laying emphasis that if cyber security is not kept in mind it could be detrimental to their work. Age differences show different behavior towards cyber security (leaving printouts). The people in the age range of (> 32 and < =50) are prone towards leaving important printouts on their table. It is imperative that organization or colleges orient these people how leaving these important papers could be harmful to the information framework of their respective companies. Employees who have an experience of (< = 2) should be provided with a training that by clicking any links in email could harm their data. These trainings would make them cautious and vigilant towards link in email.

People specifically from Bangladesh should be sensitize through trainings that picking up and plugging in USB drives can unknowingly open their organization to an internal attack of virus. The results also concluded that the students from arts and commerce are more inclined in accessing websites which could be harmful. They require an orientation programme to address towards the safety of their data by avoiding the access to certain websites. Further, the PhD students' needs a training to be aware of entering any information in website could have adverse effects on cyber security framework. These results clearly point that age, work experience, place, academic discipline and qualification differences require tailored training programes to cyber security issues. Building on this, human intervention like putting the important print outs in the file, avoiding certain websites, entering any information in website, picking up and plugging in USB drives, forming simple passwords and clicking any links in emailcould make the cyber security robust in the organization.

7. Conclusion

The organizations should adopt proper information security training, which in turn brings the information security awareness, which is an important parameter for security assurance. This study examined the relationship between cyber security issues (leaving printouts, links from known source, website access, information in website, password complexity, links from known source, plugging USB in public places) with demography differences (age, work experience, academic discipline, qualification, and place) to understand which are the significant relationship between demography and cyber security. It was found that demographic profile of employeesand students significantly differ in their perception towards the cyber security. Our findings have important implication for organization that students and employee's perception towards cyber security varies in accordance to their difference in age, work experience, qualification, education and place. It can help organization identifying cyber security strength and weakness across demography and can assist in developing the tailored information security training programmes for the respective employees and students.

7.1 Future Directions

Building on the present study, future research could examine the human aspect of information security and organization security culture. Future research can also consider the different aspects of personality traits of human beings.

References

1. Abawajy, J.:User preference of cyber security awareness delivery methods. *Behaviour& Information Technology*33(3), 237-248 (2014).

2. Agarwal, R. & Prasad, J.: Are individual differences germane to the acceptance of new information technologies? *Decision sciences* 30(2)**,** 361-391(1999).
3. Arachchilage, N. A. G., & Love, S.: Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior* 38, 304-312 (2014).
4. Albrechtsen, E., &Hovden, J.: Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security* 29(4), 432-445 (2010).
5. Brancheau, J. C., Janz, B. D., and Wetherbe, J. C.: Key Issues in Information Systems Management: 1994-95 SIM Delphi Results, *MIS Quarterly* 20(2), 225-242 (1996).
6. Carstensen LL, Issacowitz DM, Charles ST.: Taking time seriously: A theory ofsocioemotional selectivity. *American Psychologist 54*, 165–181. (1999).
7. Cavusoglu, H., Cavusoglu, H., &Raghunathan, S.: Economics of ITSecurity Management: Four Improvements to Current Security Practices. *Communications of the Association for Information Systems14*(1), 3(2004).
8. Chung, J. E., Park, N., Wang, H., Fulk, J. & McLaughlin, M.: Age differences in perceptions of online community participation among non-users: An extension of the Technology Acceptance Model. *Computers in Human Behavior*26(6)**,** 1674-1684. (2010).
9. Darwish, A., El Zarka, A., &Aloul, F.: In *2012 International Conference on Computer Systems and Industrial Informatics*, towards understanding phishing victims' profile, pp. 1-5. IEEE. (2012, December).
10. Durgin, M.: Understanding the importance of and implementing internal security measures. *SANS Institute Reading Room (https://www2. sans. org/reading_room/whitepapers/policyissues/1901. php)*. (2007).
11. Egelman, S., & Peer, E.:. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*Scaling the security wall: Developing a security behavior intentions scale, pp. 2873-2882, ACM(2015, April).
12. European Union Agency for Network and Information Security (ENISA). The new users' guide: how to raise information security awareness (EN) (2010).
13. Furnell, S., & Clarke, N.: Power to the people? The evolving recognition of human aspects of security. *computers& security31*(8), 983-988 (2012).
14. Furnell, S. M., Jusoh, A., &Katsabas, D.The challenges of understanding and using security: A survey of end-users. *Computers & Security 25*(1), 27-35 (2006).
15. Herath, T., & Rao, H. R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems 18*(2), 106-125(2009).
16. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security 31*(1), 83-95(2012).
17. Igbaria, M., &Parasuraman, S.: A path analytic study of individual characteristics, computer anxiety and attitudes toward microcomputers. *Journal of Management15*(3), 373-388 (1989).
18. Igbaria, M., Zinatelli, N., Cragg, P. &Cavaye, A. L.: Personal computing acceptance factors in small firms: a structural equation model. *MIS quarterly*,279-305 (1997).
19. Lee, J., & Lee, Y.: A holistic model of computer abuses within organizations. *Information management & computer security10*(2), 57-63(2002).
20. Lee, S. M., Lee, S. G., &Yoo, S.: An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management 41*(6), 707-718(2004).
21. Lohmeyer, D. F., J. McCrory, S. Pogreb.: Managing information security. *McKinsey Quart.* Special Edition, 2, 12-16 (2002).

22. Mohebzada, J. G., El Zarka, A., BHojani, A. H., &Darwish, A.:In *2012 International Conference on Innovations in Information Technology (IIT)*. Phishing in a university community: Two large scale phishing experiments, pp. 249-254. IEEE (2012, March).
23. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., &Zwaans, T. The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51(2017).
24. Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., &Jerram, C.:The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making9*(2), 117-129. (2015).
25. Porter, C. E., &Donthu, N. Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics. *Journal of business research59*(9), 999-1007 (2006).
26. Pricewaterhouse Coopers (PWC). Security awareness: turning your people into your first line of defence.(2010).
27. Ransbotham, S., &Mitra, S.: Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research 20*(1), 121-139 (2009).
28. Schultz, E.: From the Editor-in-Chief: The human factor in security. *Computers and security 24*(6), 425-426(2005).
29. Safa, N. S., & Ismail, M. A.: A customer loyalty formation model in electronic commerce. *Economic Modelling35*, 559-564(2013).
30. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., &Herawan, T.:Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78 (2015).
31. Safa, N. S., Von Solms, R., &Furnell, S.: Information security policy compliance model in organizations. *Computers & Security 56*, 70-82 (2016).
32. Taylor, S. & Todd, P.: Assessing IT usage: The role of prior experience. *MIS quarterly*19**,** 561-570 (1995).
33. Venkatesh, V. & Morris, M. G.: Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS quarterly*, 115-139(2000).
34. Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D.: User acceptance of information technology: Toward a unified view. *MIS quarterly***,** 425-478. (2003).
35. Von Solms, R., & Van Niekerk, J.:From information security to cyber security. *Computers & security*, *38*, 97-102(2013).
36. Vroom, C., & Von Solms, R.:Towards information security behavioural compliance. *Computers & security 23*(3), 191-198(2004).
37. Werlinger, R., Hawkey, K., Botta, D., &Beznosov, K..: Security practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies 67*(7), 584-606(2009).
38. Whitty, M., Doodson, J., Creese, S., & Hodges, D.: Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking 18*(1), 3-7(2015).
39. Wood, C. C., & Banks Jr, W. W.: Human error: an overlooked but significant information security problem. *Computers & Security 12*(1), 51-60(1993).