Proceedings of the Ninth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2015)

Understanding User Knowledge of Computer Security and Risk: A Comparative Study

C. Thurlby, C. Langensiepen, J. Haggerty and R. Ranson

School of Science and Technology, Nottingham Trent University, Clifton Campus, Clifton Lane, Nottingham, NG11 8NS, United Kingdom
e-mail: criag.thurlby@ntu.ac.uk

Abstract

Academic institutions have to cope with thousands of new students every year, with a wide range of knowledge of computer security. This can potentially lead to many breaches, with resultant impact on availability and cost to fix. In this paper we report on a survey of a group of new first year undergraduate students. Their replies show that 18 year olds use computers very heavily, but their understanding of what computer security means can range from the sophisticated to the worrying. In addition, their emphasis is often on their personal security and privacy within social media rather than any impact on the machines they use at university. We discuss their responses in detail and make some recommendations regarding further analysis.

Keywords

Risk, Computer Security, Security Education

1. Introduction

The Verizon 2015 breach investigations report states that 61 educational institutions who replied to the survey suffered 165 security incidents with 80% of threats coming from external actors. The results demonstrate that all organisations and institutions are vulnerable to malicious attacks and should not ignore strengthening their network and employees.

The purpose of this study is to gain an understanding of how individual students perceive risk by analysing their level of knowledge when related to computer use to better understand how knowledgeable the individual is when introduced into an institution's environment. This forms part of a larger study into behavioural profiling of university students and will eventually be combined with various network data to enable a fuller picture of user network behaviour. It is important to gain both security knowledge and attitude from the students to better understand why certain breaches are more prevalent than others and how this could potentially contribute to problems for the IT department within the University. The questionnaire will build the foundation to better understand the student and ultimately educate the student by grouping these findings into appropriate classifications of security training.

To start with a clean slate, the respondents of the survey conducted were first year undergraduate students attending their university inductions. This selection of

students were chosen because of their limited knowledge of the university's IT systems which ensured the capture of a more neutral and balanced set of results. This selection also assumes that they have a more casual approach to the way they work; another reason why they were chosen.

This paper is organized as follows. Section 2 discusses related work. Section 3 presents the methodology used for the comparative survey. Section 4 presents the results of the survey. Finally, we make our conclusions and discuss further work.

2. Related Work

Security education needs to address the organisation as well as the individual within it. Tsohou et al (2013) comments on how security awareness research has mostly focused on the individual or organisation level with limited studies examining both. The inclusion of institutional IT changes would deliver a more relevant training plan to the end user due to having exposure to changes of the organisation's infrastructure.

Within any organisation employees demonstrate different behaviours and attitudes to their roles and Parsons et al (2014) suggest the production of an empirically validated instrument (HAIS-Q). This tool could be used to measure employee knowledge, attitude, and behaviour to provide management with a benchmark. The need to combine both the understanding and benchmarking of all employee attitudes and behaviours is an important factor to enable the profiling of an employee knowledge base. This would provide direct education that complements the employee knowledge. Szilagyi et al (1990) state that the group, made up of individuals, develops unique characteristics beyond those of the person and his personal contributions. Groups need to be examined independently and not just as the individuals that comprise them.

The study by Bulgurcu et al (2010) suggests that employees who use the information and technology resources of their organisations assume certain roles and are responsible for safeguarding those resources. Within an educational environment consisting of employees and students both parties need to be educated to enable responsibility for the resources that are used. Siponen et al (1990) suggests trying to understand the different ways people respond to different methods and actions used to increase information security awareness.

It is important that all users within an institution are engaged when an Information Security induction is performed to avoid a malicious attack on the organisation or the user. Shropshire et al (2015) state that the greatest threat to information security lies not behind the security perimeter, but rather with the careless or malicious actions of internal users. Tampoe et al (1993) suggest that it would be wrong to assume that users were all interested in the same motivators or that their preferences met the generalized model.

Within the educational context, knowledge-sharing plays a pivotal part of an employee's education and Tagliaventi et al (2006) defines networks of practice that are sets of individuals who share common values and ways of doing things; that is, practices and knowledge sharing through subject matter. The ability to search for a common motivator between students would be of great benefit by forming grouping of individuals from the analysis of common subject areas, thus enabling the sharing of knowledge long after an information security induction has occurred.

For the implementation of a successful information security awareness programme it is imperative that the employees' education is effective and informs all of the employees. Thomson et al (1998) states that the technical development of the computer and associated disciplines has played a large part in the profile and involvement of the user with Harris et al (1999) suggesting that successful end-user computing is therefore dependant on the behaviour of individual end users.

User behaviour dictates the attitude towards end-user computing within the organisation with Pahnila et al (2007) suggesting that attitude, normative beliefs and habits have significant effect on intention to comply with IS security policies and Dhillon et al (2001) indicating that informal controls, perhaps the most cost-effective type of controls, essentially centre around increasing awareness of employees.

In the next section, we present the methodology of a survey of undergraduate students to discover the attitudes towards risk and understanding of computer security.

3. Survey Methodology

To deliver a varied set of results, a questionnaire containing 14 questions targeted a mixed cohort of 97 students who would be attending a range of courses, e.g. Computing, Social Sciences, Psychology and Education. All participants completed a questionnaire that related to their own and observed perception of risk when using computers. The survey sets out to answer what risk means to the individual student, their knowledge of computer related risk and their daily exposure to computer usage.

The survey received 97 responses of mixed gender and all were first year undergraduate students with a varied set of subject knowledge. This research criteria was intentionally chosen to enable a more balanced set of results. The 14 questions were graded by a point scale system of 1 to 3.

When grading the answers for all questions within this paper, an independent examination will be carried out to prevent any preconceptions of the individual's knowledge and academic course. Not all questions contained in the questionnaire have been included for this paper; only the questions that relate to risk and computer usage were chosen to deliver a more directed set of results for the benefit of this paper.

4. Survey Results

The following subsections present and discuss the participants' answers that focus on Computer Security and Risk. The questionnaire required the student to answer 14 questions related to their use of computers and perception of computer risk.

The first question selected for study is: "Briefly explain what you are studying at university". Although not directly related to the question of risk it is of vital importance that an understanding of an individual student's background when related to the use of computers.

A total of 38% of the students who answered the questionnaire were studying an academic subject that did not directly involve the use of computers as their core study area. These subjects included: Psychology, Forensic Science, Education, Criminology and Surveying. The remaining 59% represented those students who have a direct interaction with an academic computing subject area that included subjects: Computer Science, Software Engineering and Computer Systems. Further study of the results demonstrated that the 38% of students from non-computing subjects was more weighted with female participants compared to the 68% that held more male responses.

What part have computers played in your life up to now?

This question provided an insight into the individual student's personal experience of computer use.

Played a little part in my life	3%
Played a general part in my life	30%
Played a big part in my life	63%

Table 1: Personal Experience of Computer Use

Analysis of table 1 shows a higher percentage of students where computers have played a major part in their everyday life compared to only 3% who have limited interaction. For the non-computing group, the following comments were recorded:

"very big part. Socially (Facebook, Twitter, tumblr), for entertainment (YouTube, Netflix)"

"major part, use computer everyday, so do my children"

"a significant part, for both social and educational purposes".

The first question represented 38% of students who were studying a non- computing subject and involved modules that were less computer-intensive. However from the examination of table 1, the results present the opposite when taking into account that

30% of individuals have a general daily interaction with computers and 63% have a lot of interaction from the combined groups.

From the observation for non-computing students, 38% agreed that computers played a major part with a recurring answer that related to the use of social media and 13% having a general usage commenting on the usage of social media and delivering an overall total of 51%.

The result for the computing group showed 68% were of high usage and 51% were of general usage. Responses were:

"I have been using computers since I was 4, for gaming, learning and literally everything"

"a massive part, I use them everyday they are my passion, I love them and enjoy using them".

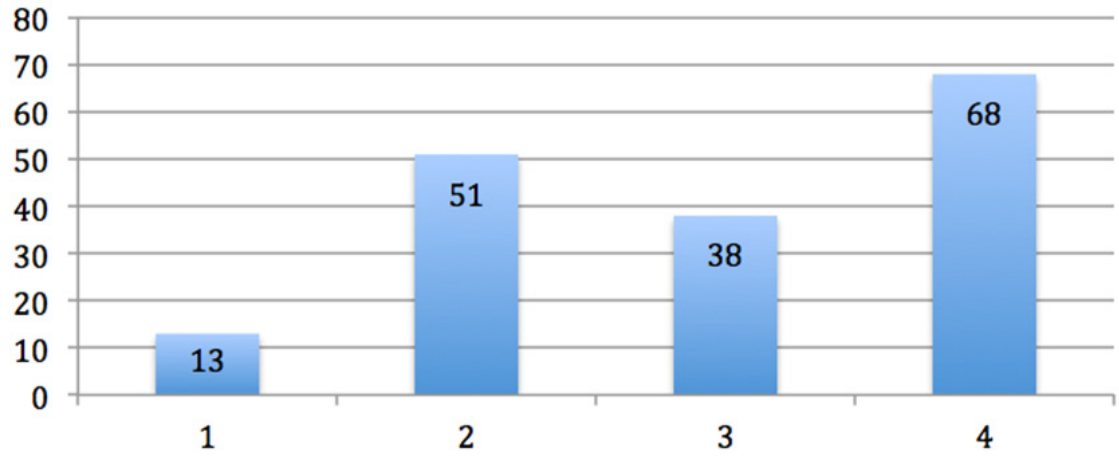

Figure 1: Computer Usage Amongst the Participants

The study of these results shows that all students with a non-computing background have more exposure to computers than was first assumed. From the analysis of the computing group's results, a combined total of only 23% of students with high and general use mentioned social media and a combined total of 75% of the responses for high and general referring to computer related activities.

Study of the results has showed that the non-computing group may still be susceptible to a malicious attack in the guise of a phishing attack due to their regular usage of social media applications for communication compared to the computing group whose answers are directed to the use of computing in relation to programming, gaming, 3D modelling and the building of computers. Also of interest is the split between genders where the majority of female students mentioned the use of social media compared to the more technical side from the computing group. Also of note is the amount of exposure both groups have and the definite separation of

how computers are used in the conventional way with the first group having large amounts of exposure from the use of social media.

What does computer security mean to you?

This was asked to form an understanding of the individual student's perception of Computer Security in relation to their everyday life. This was a 3-point scale ranging from 'a little knowledge' to 'a lot' with all answers being examined independently.

Have little knowledge	22%
Have a general knowledge	46%
Have a lot of knowledge	32%

Table 2: Perception of Computer Security

The study of table 2 shows 22% of individuals had a limited knowledge of computer security with 46% having a general understanding and 32% demonstrating a lot of knowledge. Dividing the results into their relevant groups, 21% of the non-computing individuals showed a lack of knowledge, 51% had a general knowledge and 22% a lot of knowledge. The 46% of students commented:

"I take my computer security very seriously as I bank online and purchase products regularly"

"after getting a few (like 50) viruses on my laptop. It is the most important thing when downloading items online"

"making sure that all my private information is safe and secure. Also that by having security ensures I don't get any viruses".

The computing group who claimed a general knowledge delivered similar comments:

"not getting viruses and your information being private"

"staying safe when using computers, like dodging viruses and keeping data secure and safe".

Those who claimed more knowledge showed this in their answers – for example:

"Privacy, knowing that I am the only one who can access/view/modify my work. Security, preventing unauthorised access which could lead to a breach of privacy"

"To ensure a computer or system is secure from both malicious and accidental attacks, whether it be physical or cyber-based".

The responses for the more knowledge group demonstrated an understanding of threats that occur both internally and externally and dominated by the computing group compared with the non-computing group's responses that presented a more

insular view on computer security with concerns relating to their personal computers and private work. The comparison between the two groups demonstrate a definite split between the perception of computer security with a more secure rounded approach coming from the computing group due to the inclusion of external threats. The study of the non- computing comments demonstrated a high response related to the protection from viruses, demonstrating knowledge of personal protection but no responses related to external threats. This is by no means a negative aspect as both groups showed a good grasp of computer security. Again analysing both of the groups' responses to determine which group could be more vulnerable to a malicious attack, the non-computing group, based on responses, would be the most at risk due to the insular nature of their responses.

What risk have you taken when using computers and would you take the same risk now?

From the results of the previous questions the assumption is that the non-computing group will focus more on the internal experience compared to the computing group who will understand both internal and external risk. A 3-point scale was used from 'no risk' to 'high risk' and all answers being examined independently.

No Risk	27%
General level of Risk	30%
High level of risk	41%

Table 3: Participants risk appetite

From the study of the table findings there is a fairly even spread of students who take no risk to students that are classed as taking a general risk with only 3% difference. The separation of results into the two respective groups showed a shared percentage for all three scales for non-computing at 33% with answers to for medium risk consisting of:

"posting pictures online and details of holidays, and no I wouldn't"

"used to use the same password which was very obvious. And I would never take that risk again"

Comments for the high risk group stating that:

"I have used computers when they still had a virus. I wouldn't do it again as I ended up loosing all my photos"

"downloaded fake updates that put viruses on my PC. No don't download much now."

The results of the 32% of the computing group answers for medium risk consisted of:

"using computers in public without protecting my passwords or data. No I wouldn't do it again"

"Downloading from untrusted websites, and no."

Non-computing students concentrated on the downloading of files or leaving their accounts logged on which is in total contrast to the computing groups focus, directed at using open networks, having their personal data stored on shared computers and accessing untrusted websites which demonstrates the understanding of what an external threat is.

For the Computing students answers for high risk, 54% fell into this category and responses to the question consisted of:

"downloaded unsafe software, torrenting"

"Sourcing unsafe software. No I would not take that risk again" "downloading software from dodgy websites. Most likely not."

From the study of these results, it is evident that the majority of the computing group have a good understanding of the risk that they have taken with the majority of answers involving the downloading of software from non-reliable sources and descriptions of methods and sites they have used and visited. Although the risk and consequence of this activity is understood the individuals still decide to carry out the activity. If compared with the non-computing group, the risk, acknowledgement and avoidance have been acknowledged. The study of both groups demonstrates that the non-computing delivers the less risk due to the internal nature of responses that were provided, again the risk is related to the student's personal work and PC. The computing group understands the risk they are taking which could increase the chances of a malicious attack due to their knowledge of external entities.

5. Conclusions and further work

From the study of the questionnaire on risk and computer security, it can be observed that there is a need to adapt the way that computer security education is delivered to users. Tracing through the questions that were asked and answered, there is a definite split on the way that students perceive computer security.

From the analysis of the answers it establishes the way that different interpretations of usage and risk are perceived. The analysis of question 2 "What part have computers played in your life up to now" demonstrates the perception of usage between the two groups of students with one being the usage of social media and the other with usage of computer based software. The author has discovered that the perception of what computer use represents is no longer the traditional view of sitting at a computer producing work; it also associated with the use of social media. Both sets of groups have good exposure to computers but from completely different sides of how IT is used.

The study of question 3 "What does computer security mean to you?" demonstrates the different perceptions that both groups deliver with the non-computing group presenting an internal perception and the computing group presenting the internal and external perception. From the study of this question, it is evident that the first group is more focused on their personal work within the internal environment. The comment of viruses and anti-virus software were mentioned throughout the non-computing group's answers but do the group understand what a virus is or how it is propagated compared to group 2 who included external influences in their responses. In the second phase of research work will be performed to discover how much knowledge of external threats the students truly understand to enable a fuller understanding of student security knowledge.

The initial assumptions until question 4 were that the non-computing students would be the biggest threat from a malicious attack to the institution until the responses from "What risk have you taken when using computers and would you take the same risk now?" The students within group 2 identified the risk and also understood the risk that was being taken which when compared to the responses of the computing group was more reckless in relation to the non-computing group due to the level of knowledge that these students hold.

The results from this questionnaire have highlighted that further work is needed within the field of information security training. From the analysis of four questions, the research has highlighted the levels of knowledge that exists between users and more importantly the groupings of users. Observation of the collected data has highlighted a definite trend when related to knowledge and usage between different groupings of students and the importance of further study in this area. When designing an effective training plan, the classification of groups with the same background and knowledge base could minimize the need to address individual users with targeted training by developing separate computer security groups to ensure full engagement and understanding of the security information that is being delivered.

Also of importance is the student interpretation of risk along with the acceptance of computer risk. The study of the results showed those students who had a greater knowledge of computers were more likely to take the bigger risks that could potentially cause greater issues to the organisation's IT systems. Further studies will be carried out on how confident students are when using computers and if this confidence can influence the student into taking greater risks.

The next stage of the research is to investigate the students' perception of risk further, with more work on the influence of their peers attitudes and actions towards risk, along with the study into their knowledge of external threats and understanding of how this could have an effect on an organisation's IT system. These new questions combined with the present set would enable a fuller student profile to be developed that would assist in developing a relevant security training programme for new students.

6. References

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

Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing about the enemy within. Computers and Security, 20(8), 715–723.

Harris, R. W. (1999). Attitudes towards end-user computing: A structural equation model. Behaviour & Information Technology, 18(2), 109–125.

Pahnila, S., Siponen, M., Mahmood, A., Box, P. O., Oulun, F.-, & Siponen, E. M. (2007). Employees ' Behavior towards IS Security Policy Compliance University of Oulu , Department of Information Processing. October, 1–10.

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 and Security, 42, 165–176.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, 177–191.

Siponen, M. T. (1991). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, (Table I), 31–41.

Szilagyi AD, Wallace MJ. Organizational behavior and performance. 5th ed. Illinois: Scott, Foresman and Company; 1990.

Tagliaventi, M. R. (2006). The role of networks of practice, value sharing, and operational proximity in knowledge flows between professional groups. Human Relations, 59(3), 291–319.

Tampoe, M. (1993). Motivating knowledge workers—The challenge for the 1990s. Long Range Planning, 26(3), 49–55. doi:10.1016/0024-6301(93)90006-2

Thomson , M. E., & Solms , R. Von . (1998). Information security awareness: educating your users effectively. Information Management & Computer Security, 6(4), 167–173.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2013). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38–58.

Verizon Business. (2014).2014 Data Breach Investigations Report. Verizon Business Journal, 2014(1), 1–60.