Strengthening the Human Firewall

G.C.Tjhai and S.M.Furnell

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

Employees' complacency, ignorance and unawareness of security are amongst the biggest obstacles to maintaining IT security within an organisation. Indeed, technical security controls alone are not enough to provide a real protection if there is no human participation acquired in this stage. As a consequence, it is desirable for many organizations develop an effective security awareness programme; by which user awareness could be enhanced. The objectives of this paper are to explore the extent of security awareness problems and to ideally specify and develop methods by which security culture could be cultivated (through training and awareness initiatives)

Keywords

Security awareness, User behaviour, Security culture, Training, Education

1. Introduction

Corporate security breaches are no longer new issues, and are now a reality to be faced by many modern organisations. With the numerous security incidents being reported in recent times, the need to secure and protect corporate sensitive information and networks is of greater importance than ever before.

The human element is always thought to be the key as well as the weakest link of security chain. Firmly focusing on human factor in security practices is the first step to achieve a successful corporate security culture. Unfortunately, the human-related security issue is not a straightforward problem to deal with. There is a need to make all employees and end users aware of the need for security, and to educate or train them to do their part in securing the enterprise. An organisational security awareness programme is aimed to make all the employees understand and appreciate not only the value of the company's information assets, but also the consequences if the assets are compromised. A good security programme should be able to change the employees' behaviours or activities into more secure habits, by convincing them why being more security conscious is important.

This paper attempts to benchmark the level of security awareness and culture within two organizations, enabling views to be formed on the effectiveness of the methods in use.

2. Background

As discussed previously, end-user security behaviour is one of the underlying issues of information security practices. Identifying significant factors of corporate security culture would be of value since they could have strong influences on user security behaviours. Besides, it is worth remembering that improper security habits are the major determinant of the level of security incidents experienced, and a good security programme is required to improve user security behaviours across the organisation (Leach, 2003).

Since user security behaviour is the main factor that could determine the level of security incidents, analysing or investigating staff behaviours are considerably crucial to perceive the state of security awareness within an organisation. Having a further investigation on end user security behaviours in a systematic view point of different kind of security behaviours are deemed to have an important role in influencing and enhancing the effectiveness of information system security (Stanton et al. 2005).

Security awareness is another important security component that needs to contribute into security culture. The neglect of information security practices is a result of having no full security culture and policy implementation within the organisation. Therefore, in order to ensure the proper organisational behaviours, information security obedience is the best solution. Information security obedience highlights the combination of corporate governance, culture and information security (Thomson & von Solms 2005), and in order to achieve it effective security awareness training and programmes are of prime importance (especially focusing upon specific groupings of employees within the organisations, such as top management, IT personal and end users).

So, in order to enable a more understanding about the level of security awareness and the extent of security problem faced by organisations, the results of an IT security awareness survey is presented below.

3. IT security awareness survey

The survey was mounted online for around 20 days, during the end of July until the middle of August 2006. Since the survey was targeted at corporate employees only, it had finally been promoted to two organisations within two different industry sectors; namely telecommunication and local government. A total of 134 responses (24 from telecommunication and 110 from local government) were received during the survey period, providing a suitable basis for the subsequent analysis. The sections that follow outline the areas covered by the questionnaire, and the associated results.

3.1 Respondents backgrounds

In this section, twelve questions were presented and basically aimed to gather information about respondents' backgrounds and to assess their basic understanding of current security issues.

3.1.1 Telecommunication sector

From this respondent group, the survey findings resulted in an unequal split between male and female; with approximately twice as many male respondents. From an age perspective, there was a significant focus within the 25-34 category, suggesting that most opinions came from respondents who would have grown up with information technology. It is also worth noticing that more than three quarters of respondents were high educated people, with half of them holding IT-related qualifications.

In respect of employees' security threat awareness, nearly all respondents were threat-aware in general, especially in relation to more common security issue such as viruses and spam, as illustrated in Figure 1. However, the survey result revealed that half of the respondents holding IT-related qualifications were not aware of the existence of social engineering attacks.

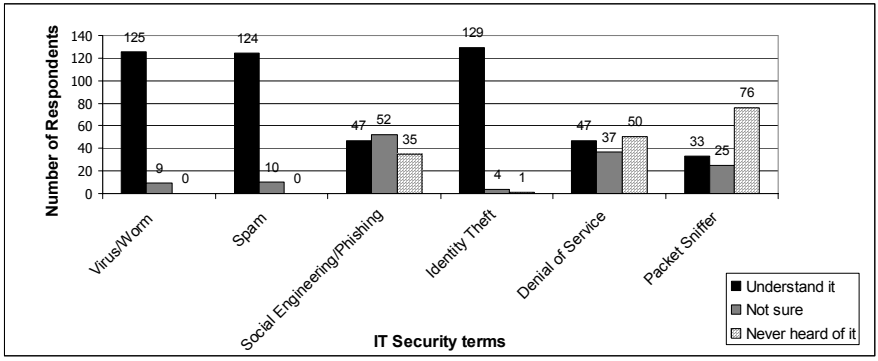

Figure 1: Level of understanding of IT security terms (from both respondent groups)

With regard to respondents' awareness of security initiatives, only one eighth of participants claimed to have security awareness programme in their organisation, while 66% showed that they were not made alert of any security programme in their organisations. Moreover, quite a significant number (one fifth of respondents) had declared to have no any security programme or related training being implemented by their organisations. In terms of their frequency in joining security awareness programme, it is surprisingly enough that from three respondents claiming to have a security awareness programme, none of them had attended a regular security programme, as shown in Figure 2. Two of them never joined any security programme implemented, while another one had had a security education once in an induction day. As such, this result gives a clear illustration that even where a security programme has been implemented in an organisation, it may not been widely adopted by those that may need it.

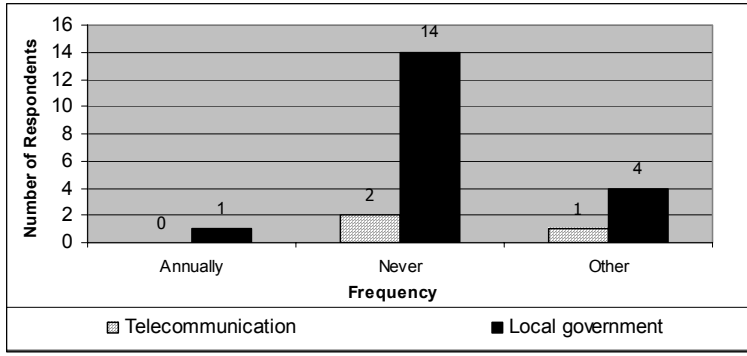

Figure 2: Respondents joining security awareness programme/training

3.1.2 Local government

As to the respondents' educational background, the majority were holding a middle level of education. Similar to what had been found in telecommunication sector, almost all respondents (more than 92%) were reported to have a good understanding and awareness of viruses, spam and identity theft. On the other hand, social engineering was still not a common term for the majority of employees, as illustrated in Figure 1. Only 30% of them had a good perception of social engineering attack.

From 110 respondents received from this respondent group, only 17% (19 people) had declared to have security programme or related training in their organisation. Conversely, a significant proportion (57%) reported having no idea of any security programme in their organisation, while 26% definitively claimed not to one. Worse still, from the 19 people who claimed to have a security programme, only one of them had participated in it (annually). A total of 18 people never attended any regular security programme or only received security education once in the induction day or via security messages, as shown in Figure 2.

3.2 Respondents security attitudes and decision making

In order to focus more upon users' understanding and perception of security issues, the survey presented 6 questions aiming to investigate users' security attitudes and their decision making in their current employment.

3.2.1 Telecommunication sector

Questions were designed to evaluate the effectiveness of password policy enforcement within the organisation. From this sample group, only approximately 8% of respondents (2 out of 24 people) had firmly adhered to the password policy by applying all strong password characteristics in their password selection. In terms of their frequency in changing passwords, almost 42% of respondents hardly ever changed them unless the system prompted them to do so.

The survey results also point out the most common security mistakes made by respondents in this sample group. The highest proportions of respondents, accounting for 42%, were inclined to leave their computers unattended without logging off in an open office. In term of respondents' understanding of corporate system security, the

findings show that almost 88% of respondents (21 persons) believed that personal data is not a good choice of information for password selection. However, 18 out of 21 people who declared to disagree with the usage of private data in password selection were still using that information as their password choice. Surprisingly, two thirds of respondents considered that the IT department has the sole responsibility for securing corporate IT systems. The role of IT administrator in controlling and managing corporate IT system has been misinterpreted by the majority of employees

3.2.2 Local government

From this local government sector, only 3% of respondents had firmly conformed to the password policy by applying all strong password characteristics in their password choice. Through this questionnaire, it is clear that several characteristics of strong password have been widely applied by many corporate employees, for example the usage of 8 characters, combination of letters, symbols and numbers and so on. Significantly, almost 38% of staff did not use private data as their password choice. With respect to their password changing habits, more than half of employees in this respondent group never changed their password unless the system had forced them to do so.

Nearly 28% of respondents admitted to sharing their password with other colleagues and to writing it down as a way to remember. Interestingly, leaving the computer unattended without logging off is again the most frequent mistake made by corporate employees, with 46% (51 people) being likely to do this.

A large number of respondents (84%) agreed that personal data is a bad choice for password selection. Despite this, however, 56 out of 93 persons used the personal data as their password. The usage of private data as password is undoubtedly more usable and practical for the users, but this choice could definitely render the system vulnerable to the attack since personal data is easier for hackers to guess. Significantly, the majority of respondents from this respondent group again believed that IT administrator is the only one who is responsible for securing the corporate IT system.

3.3 The influential factors of employees' security behaviours

After focusing on the employees' perception of organisational security awareness and their security habits, the next aspect of the questionnaire was directed to evaluating the factors that could possibly affect the way employees behave in their organisations.

3.3.1 Telecommunication sector

The survey finding has shown a clear point that the vast majority of respondents (92%) installing antivirus software were influenced by their awareness of security threats. Approximately 70% and 50% claimed to be affected by other two factors, namely policy enforcement and usability respectively. Significantly, less than 9% of participants asserted that installing security software could be strongly influenced by the environment surrounding them.

As to good security practice in taking back-up of data, around 83% of respondents in the telecommunication company claimed that having an experience of losing data could serve as a good motivation to take a back-up of their data. Very surprisingly, only 15% of them declared that the environment could effectively influence them to follow this security practice.

3.3.2 Local government

Interestingly, similarly to the findings from telecommunication sector, 77% of respondents who installed the security software were influenced by their security awareness. Quite a significant number of employees (67% and 47% of participants) installed antivirus software as a response to policy enforcement and usability factors. Interestingly enough, only a small number of them claimed that installing anti virus software could be deeply influenced by the environment or people surrounding them. For example, few thought that looking at other colleagues firmly following security practice (e.g. installing security software to protect their work PC) could strongly motivate them to do the same thing.

With regard to the second security practice, 71% of respondents were more likely to take back-up of their data because of their experiences in losing data and their awareness of the importance of having back-up data. Significantly enough, 62% of them asserted that policy enforcement was one of the strongest influential factor motivating them to adhere to this security practice, whilst two fifths of employees were affected by the usability issue. Only 15% of employees took back up of data because of their environment, such as the motivation from other colleagues.

3.4 Preferable security learning methods

The final question was focused on the evaluation of several familiar security learning methods. In this study, the respondents were asked to rate their preferences for each of the security learning techniques available.

3.4.1 Telecommunication sector

In general, the most popular learning methods reported among the employees in this respondent group was via presentation or face to-face training, with 83% of respondents rating it as an excellent learning method. Significantly, web-based awareness courses and inspection/audits were also well-liked among employees in this group; around 42% of employees viewing these methods as beneficial. Very interestingly, poster/screen savers, trinket/gifts and regular bulletins were rated as the least popular or helpful learning methods. Through this finding, it is clear that more educational methods (such as presentation sessions) are much more favourable than methods that are only intended to remind the users about security issues.

3.4.2 Local government

The findings here were slightly different to what had been found in the telecommunication company. Significantly, four learning methods were most welcomed by this respondent group; namely presentation or face-to-face training, web-based awareness courses, regular bulletins, and inspection or audits. Roughly 85% of respondents said that a presentation or web-based course was the best method used to enhance security awareness or deliver security materials.

Significantly, web-based awareness course and regular bulletins were also considered to be other beneficial methods used in security awareness programme, accounted for 60% respectively. Unlike the result found in telecommunication sector, regular bulletin is deemed to be a favourable method.

4. Discussion

Since the objective of conducting the IT security awareness survey was to investigate the security culture within the organisations, it is clear that the findings have revealed some interesting facts about the level of employee awareness within those respondent groups.

With regard to the employees' understanding about IT security terms, the majority of employees knew the common threats such as virus and spam. However, the findings show that the lack of understanding about more uncommon security threats, such social engineering, could become one of the major challenges faced by organisations. Social engineering, which is also linked to the threat of phishing, is one of the most malicious attacks targeted on human element instead of technology. The lack of understanding from employees renders corporate system vulnerable to the attack. Due to this issue, the level of security awareness should be enhanced for people at every level in the organisation, regardless of their status. The employees ought to be educated well about corporate security issues, the potential risks, as well as their responsibility or participation in protecting company's assets.

From the survey results, it is also clear that the level of training given to the employees is variable within the organisations. Significantly, the survey finding has suggested that the level of security education or training given to the employees is deemed to be considerably low within both respondent groups. The low level of actual take-up suggests that the programmes have merely been thought to be an add-on activity, and that the value of security awareness has not been widely communicated to people in the organisation. For that reason, the lack of understanding about the importance of security awareness undoubtedly becomes a major obstacle in developing or building the ideal security culture.

Another significant point that could be drawn from the survey findings is that security is often traded-off against usability by employees. For example, even though more than three-quarters of respondents disagreed with the usage of personal data as password choice, 65% of the total group still used it in their password selection. This negative correlation is likely to have occurred as a result of the security and usability trade-off. Although, users believe that personal data is very sensitive information and easily guessed, they will yet apply this information as their password selection since it is easy to remember. This finding reveals the similar result as what had been discussed in prior research (Besnard & Arief 2003). In terms of their password-changing habits, the findings have shown that there is a lack of tendency or attentiveness from quite large number employees to change their password frequently. Commonly, instead of being seen as a security measure, a password is deemed to be a mere tool used to gain access to a system. As a result, the employees'

awareness of password security should be improved to some extent as an attempt to maximise the level of organisational system security.

Importantly, the survey findings also provide a clear picture that user security behaviours and attitudes are potentially influenced by environmental factors, usability issues, enforcement and self-persuasion (Leach 2003; Thomson & von Solms 1998). Through this result, it is clear that employees could adopt good security practices if they have the understanding of what behaviours are expected of them; for example what they are being told (enforcement), what they see being practiced by others around them (environment/social learning) and the experiences they had from the decision they made in the past (experience of failure).

Another critical component that needs to be seriously considered during the development of effective security programme is the technique used to deliver or promote the security culture. A good security programme should be able to attract the audiences to actively respond to the security initiative/material promoted. Here, several examples of effective security programme techniques are web-based awareness courses, presentation or face-to-face training, inspection and audit, handbooks, reference materials, and so on.

5. Conclusions

Overall, the survey has revealed some interesting facts about security awareness in organisations. Even if awareness programmes exist, there is still lack of understanding from the employees about the importance of corporate security awareness. Due to this issue, raising security awareness is becoming one critical practice for all companies; which then need to be tailored to minimise user-related faults and maximise the efficiency of security practices and procedures from the users' perception. Since only two industry sectors had been evaluated in this research, the study has not provided an enough basis for an extensive investigation of security culture across wide range of organisations.

After evaluating and developing an ideal security measure to increase the level of security awareness throughout the organisations, which is more focused on the measures at the strategic level, the future work now should be shifted to investigate the method used to measure the effectiveness of security programme. This is supporting by the fact that there is a lot less available in the literature on how to measure the effectiveness of security programme rather than how to deliver it. Since the security awareness programme is a dynamic process, it needs to be continually measured and managed to keep pace with changes in the organisation's risk profile.

6. References

Besnard, D. and Arief, B. (2003), 'Computer security impaired by legitimate users', Computers and Security (23). available online: http://www.sciencedirect.com, date visited: 6 August 2006.

Leach, J. (2003), 'Improving User Security Behaviour', Computers and Security 22(8). Available online: http://www.citeulike.org/article/56424,date visited: 21 January 2006.

Stanton, J. M., Stam, K. R., Mastrangelo, P. and Jolton, J. (2005), 'Analysis of end user security behaviours', Computers and Security 24(2). available online: http://www.elsevier.com/wps/find/journaldescription.cws home/ 405877/description#description, date visited: 20 January 2006.

Thomson, M. and von Solms, R. (1998), 'Information Security Awareness: educating your users effectively', Information Management and Computer Security 6(4). available online: http: //www.emeraldinsight.com/Insight/ViewContentServlet?Filename= Published/EmeraldFullTextArticle/Articles/0460060404.html, date visited: 25 January 2006.

Thomson, K.-L. and von Solms, R. (2005), 'Information security obedience: a definition', Computers and Security 24(1). available online: http://www.informatik.uni-trier.de/_ley/db/journals/compsec/compsec24.html, date visited: 22 January 2006.