Security Culture in the Context of National Culture

J.Thomas and S.M.Furnell

Centre for Security, Communications and Network Research,
Plymouth University, Plymouth, UK
e-mail: info@cscan.org

Abstract

On a general level, it becomes clear that different countries have different perceptions with respect security and privacy concerns. For example, while many countries may have legislation in place to cover issues such as computer crime and misuse, or data protection, others may lack concern on such issues. Security may be a primary concern for citizens of countries having a reliable technological infrastructure; on the other hand priority may shift from security to infrastructure development for citizens belonging to developing countries. The above factors highlight the technical influences; in addition a range of societal values may also influence attitudes. As the internet is known to cross all borders and jurisdiction, protecting information and maintaining a sense of security is truly a challenge faced by many countries, especially their government authorities.

Keywords

Security, nationality, culture.

1 Introduction to security culture

Security culture is a new dimension in the area of information security. Up until now the concept of security culture has not been defined. Recent research papers relate security culture to improvement of adherence to the security policies (Security Governance.net, 2010). With the global nature of internet and the number of online transactions being performed on a daily basis, security implementation becomes a challenge. The nature of required security varies from individual to individual and organization to organization. Supporting activities in such a way that information security becomes a natural aspect in all the daily activities of internet users should be the primary objective of promoting a security culture. Security culture helps in building the necessary trust between the different components of the organisation and its reliability on the internet. Information security culture is therefore considered as an integral part of organisational culture (Schlienger, 2003).

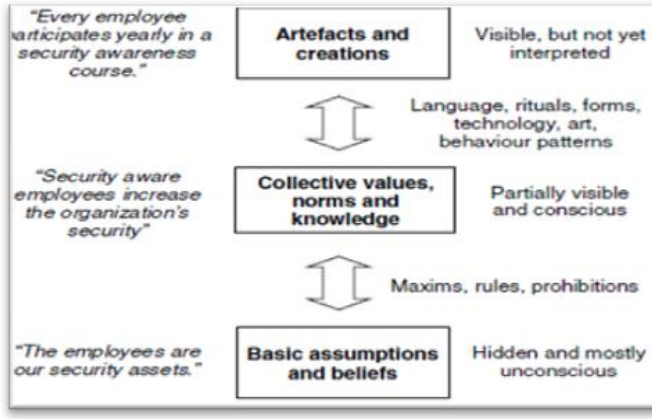

Figure 1: Three levels of security culture (Source: Schlienger, 2003)

2 The Security culture model

The main substances of an organizational culture are basic assumptions and beliefs. The assumptions are based on the nature of the people, their behavioural traits and the relationships they share. The organizational culture is expressed in terms of collective values, norms and knowledge of the organizations. These norms and values affect the behaviour of the people. Norms and values are expressed in form of artefacts and creations which include handbooks, rituals and anecdotes (Schlienger, 2003). It is noteworthy that ultimately it is the organizational culture which largely contributes to the corporate success. As mentioned earlier organizational culture grows with time and it is shaped by the behaviour of dominant organizational members such as the founders and top-level management. Fig.1 illustrates the three layers of security culture and their interactions.

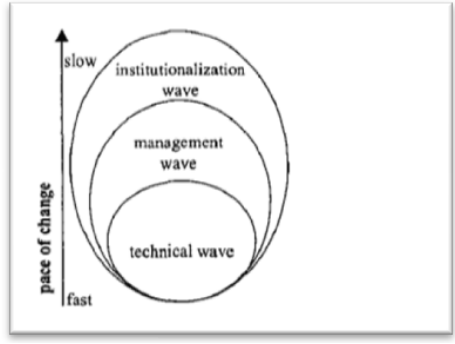

Figure 2: Institutionalization wave, management wave and technical wave (Helokunnas, 2003)

In addition to the above organizational considerations it is important to understand the implications of security culture in a global value net. Resources such as information, knowledge and time are also huge contributors of information security

culture. Concepts of value, value creation and value nets are the popularly discussed matters in industrial marketing and management literature (Helokunnas, 2003). Value is measured as a trade-off between benefits and sacrifices. In a typical scenario value is defined in terms of financial benefits, but considering a wider perspective non-monetary assets like intellectual capital, market position and social aspects may be includes as well. In general terms value net could be understood as a network of organizations or actors interconnected with either a direct or indirect exchange relationship (Helokunnas, 2003). Modern day value net and business environments require organizations to connect themselves to telecommunication networks and exchange information. Fig. 2 shows the three waves of information security: the technical wave, management wave and institutionalization wave which are responsible for shaping a healthy security culture.

3 What to analyse in security culture?

In order to understand the implications of security culture on information security, it is important to analyse and understand the factors influencing security culture. Unfortunately there is no standard method or toolset to identify the existence of a security culture or its diversity. Therefore a considerable amount of research is still required in this domain. Due to the complexity and no pre-defined methodology for research, lot of challenges are faced by the experts and researchers. Security culture can be analysed by considering two things

(i) By measuring the collective norms, values and awareness

(ii)Measure the cultural indicators and try to derive the cultures (Schlienger, 2003)

The first aspect seems to be very promising but it has some problems associated with its practical implications. Values are mostly defined by theoretical constructs. Therefore values become increasingly vague and comparisons between individuals on this basis get difficult. Values are difficult to be stated as most of the times they are revealed unconsciously. On the other hand values attributed to negative social sanctions are hidden consciously.

The limitations of the first approach, brings us to the second which deals with analysis of cultural indicators. Qualitative research methods are one good approach to analyse cultural indicators and influences. Security culture encompasses social, cultural and ethical aspects which would be instrumental in understanding and improving related behaviour. In addition, it would be worth noting that security culture does not include basic human norms and beliefs (Schlienger, 2003). However, having this approach of qualitative research could be successful as human behaviour is ultimately driven by cultural, social and ethical aspects. Moreover, human factors influenced by the above three aspects also play an important role in ensuring that policies and procedures are followed appropriately.

4 How to analyse security culture?

For the analysis of the data the above two methods are not effective as they do not propose empirical analysis. So it would be advisable to use a approach which uses empirical outcomes with statistical analysis. So for achieving the above objective, two methods are used

(i) For gathering observable indicators, analysis of documents and other resources were carried out.
(ii) Similarly for measurement of norms, values and beliefs narrative focus group sessions were conducted.

Focus groups are an effective method for gathering information for qualitative research. To analyse security culture a series of five focus groups composed of 3-6 participants were conducted. The sessions composed of participants belonging to different countries with participants belonging to the name nationality in each session. The participants were recruited from the university campus and it was also ensured that there was a balance between students pursuing computer related courses and those pursuing other non-related courses. However there arises a concern with regards to the extent to which the participants actually represent their general national population. The sessions addressed security concerns, measures and other aspects which were to be considered by users while using the internet. These concerns and issues have been illustrated in the following sections. Furthermore the sessions were video recorded for analysis of issues and drawing conclusions.

Achieving good information security awareness in the general population of Internet users is of the fundamental nature if they are to remain secure and electronic business is to flourish. Comparing the home and work environments, it is clear the latter provides more prospects for such awareness programs to take place. However, it is normal human tendency that the practised followed at work need not be followed at home. Some aspects of a nation's security culture have evolved as a logical response to security threats, and are adopted by the users. Some users learn about practises and policies as part of a natural socialisation process that is not controlled, and that leads to behaviours and attitudes in use that may or may not be approved by the organisation's managers.

Currently the term "information security culture" is often drawn near models describing organizational culture. However, considering only the organizational culture **is** not sufficient for understanding the influencing factors behind information security culture. Each individual working for an organization or accessing the internet at home is influenced by several ethical, national and organizational cultures. These cultures have an effect on the way the individual infer the meaning and importance of information security. .

In some countries confidentiality of information is often emphasised upon while integrity and availability of information is buried. However, confidentiality, integrity and availability need to strike a balance. Development of information security culture is needed to ensure and balance the confidentiality, integrity and availability of information and knowledge at institutional level and also the home user level.

4.1 Misconceptions

Security culture is vastly affected by the misconceptions that most of the internet users possess. Firstly many users believe that the internet is absolutely secure and that its foundations are not susceptible to attacks. Reality is, 13 of the top-level DNS are vulnerable to flooding, basically targeting the root servers. Secondly government lapses could also be responsible for occurrence of security incidents which may be due to inefficiency, mis-management or ignorance. Users are also under the impression that only large organizations are targeted, but in reality hackers target home users as well. This also means that users have a false sense of security and assume that only intended users can see their systems (which is not the case, the moment a system is connected to the internet, it becomes a potential target). Users also lack awareness with regards to security tools and solely rely on one security mechanism such as firewalls or anti-virus software. As per the survey conducted most of the users were satisfied with the firewall technology, but also felt that it required some improvement. This mis-conception also goes beyond this, where users think their security is someone else's responsibility.

4.2 Concerns

With the existence of a wide range of vulnerabilities, it is important to understand the potential concerns of internet users. Viruses and malicious code was still a popular concern among most users, in spite of having updated anti-virus software installed. It was even pointed out that most of the malicious codes propagated through emails. Spam was another concern, as users reported to have been receiving mails which had nothing to do with them. However, not many users faced incidents related to hacking, this may be attributed to the fact that those users have given out some user credentials at undesired locations. Having experienced these incidents, users are not sure as to whom to report such incidents. Anti-virus software vendors were a popular choice for reporting malicious activities such as worms, viruses and Trojans. As the law in most countries (especially developing countries) are just evolving, even government officials could not be relied for dealing with such incidents.

4.3 Awareness of security measures

Having mentioned the concerns, users were known to consider some precautionary measures to deal with it. Majority of the users agreed on the reliability of anti-virus software and firewalls to achieve some basic level of protection. Maintaining updates and installing them was also one key point mentioned in each of the survey sessions. Passwords were regarded to be effective in maintaining system level security.

4.3.1 Security measures

A majority of the participants agreed on the reliability of antivirus software's and firewalls to achieve a basic level of protection. The other issues could be taken care of with some basic user education and promoting awareness. For instance, the way different banks over the world dealt with phishing was known to be different. In developing countries banks were not liable for any financial losses incurred in a phishing incident. While in developed countries banks offered some amount of

compensation to the victim. Similarly there was a point raised about the efficiency of judicial systems. Participants also expected government authorities to raise awareness and have effective measures to counteract security incidents.

4.3.2 Security updates

Having all the required security tools installed, updating them was one major point highlighted in each of the sessions. Most of the population considered updating anti-virus software and Operating System related components to be vital. The remaining population considered updating every piece of software and applications being used on a daily basis. The participants believed that most of the security issues and possible vulnerabilities could be addressed by installing updates. There was a considerable amount of awareness with regards to virus updates. This clearly visible when comments about implications of anti-virus software updates was put across. Almost everyone knew what the updates did with respect to updating latest virus definitions.

The next question with regards to updates, was that, how often was it recommended to install an update? The response to this issue was alarmingly positive, in the sense that most of them installed the updated the component as and when the updates where available. Latest application design techniques do not need the systems to be rebooted immediately as and when the update was installed. So most of the population either prefer to use automatic updates or delay to the time of their convenience. However there was some concern regarding the source of the update, and only a handful of the population actually bothered to check the source of the updates. Updates were acceptable, as there seemed to be no usability issues while installing them. The only concern was that, installing updates could introduce some compatibility issues with other applications. In a nut shell, security tools such as anti-virus software, spyware and firewalls where considered to be a primary necessity to have some level of security while connecting to the internet. Updating these components was the next level of security.

4.3.3 Passwords

Most of the above mentioned tools worked with minimum interaction with the user. To protect physical access to a system and information stored in it, passwords were widely accepted as a effective security mechanism. However, there was a need to analyse the participant's idea of a strong password. Almost all the participants had a similar idea of a strong password, i.e. its composition included multi-case characters, numbers and special characters. The size range of a strong password was perceived to be around 8-16 characters in length. However, it was noticed that forgetting long passwords was a common problem. This induced the undesirable act of writing them down. In spite of having long password, none of the participants recommended using the 'remember me' check box below the password input area. Some of them felt that this would mean storing the password on some location on the system and make it available for access. Another issue pointed out was that of changing passwords. Most of the participants never actually changed their passwords. They were concerned that changing passwords too frequently would lead them to forget them. As users are known to have accounts with different systems, it was pointed out that

the passwords to each of those systems were different and only accounts that didn't contain sensitive information were known to have same passwords. To conclude, the awareness possessed by users regarding passwords was pretty much similar in nature.

4.3.4 Online transactions

Security is a primary concern while conducting financial transactions over the internet. When asked about the comfort level while conducting online transactions and shopping online, a wide range of answers were obtained from the participants. The population of people belonging to developing countries felt that, though online transactions provided some amount of convenience, they were known to be insecure. While those from the developed countries thought that it was convenient and did not encounter problems while conducting them. Noteworthy was the fact that, though they were aware of the risks associated with such transactions, they only preferred using sites and forums they were well acquainted with. When asked about identifying secure websites, most of them pointed out the padlock symbol next to the URL as a prime necessity to actually perform a transaction on that particular site. A very few users also recommended using site advisors to determine if the site was a legitimate one or dubious. The sample of population who used the internet for shopping and other financial activities, also highlighted the aspect of using it only for transactions incurring a very small monetary value (they preferred shopping for large value items face-to-face).

4.4 Concerns with online transactions:

With the advent of e-banking and online shopping, most of the users were sceptical of conducting online transactions. Making purchases worth a small financial value was considered acceptable by most. Users looked for the security of the website and checked for the padlock while confirming any sort of financial transactions, only a handful of them knew what it meant though. However, there were variations in opinions obtained from people belonging to different countries on the same issue. Individuals belonging to developing countries did not possess the necessary risk taking ability. Convenience was one major advantage of online transaction with security as a trade off for most. The main concern was that of reliability of the infrastructure and the credibility of the websites. However people from developed countries showed more comfort and ease while using online shopping websites. This however reflected that concerns with respect to online transactions varied from country to country.

Social engineering attacks are another category of attacks that cause tremendous damage as well. During the survey sessions the following scenario was put across;

"You receive a e-mail reporting a failed attempt to transfer £950 from your bank account and a request to follow a link to your online banking pages to check for dubious transactions. How would u react?"

Half of the participants of the sessions considered confronting the bank though a telephone call or visiting the bank. They stressed on the fact that they would not click

on the link whatsoever. Others pointed out the fact that they would log into their banking website through the actual link. Users were not aware of the fact that banks would not send e-mails pertaining to failure in transactions and direct them to the website and further ask for credentials. The other half mentioned that they would ignore the mail or simply delete it.

Thus it can be concluded that activities involving monetary aspects were considered highly critical and users are aware of the frauds and other scams that take place. This could be attributed to the awareness training programs or other means of educating online banking users.

4.5 Privacy

Privacy was one of the concerns expressed by most participants of the research sessions. A wide range of information was known to be disclosed during initial registrations at various websites and forums. Social networking sites are a very popular platform where users are known to reveal both a lot of unwanted information. When the issue of privacy was addressed, most of the participants instinctively thought about Facebook. All of the participants were known to have a Facebook page. When questioned about the type of information that was required to be protected, a wide range of answers were obtained. In general all the participants thought that personal information and contact details needed to be protected. Date of birth is one such piece of information which was a concern for some while for the others; it was dealt with as a ordinary piece of information disclosed. Contact details such as e-mail address and telephone numbers were the most important piece of information that according to the participants thought needed a high level of protection. A considerable proportion of the population were unaware of the means in which personal and contact information could be misused. Similarly they weren't even aware of the fact that such information could be used for social engineering attacks and other illicit purposes such as black-mailing etc. The condition stays the same for status updates and other preferences that are disclosed over such forums. Interestingly, a few of the participants even felt that medical records had to be protected and maintained confidential. This was mainly because a few of them participants felt that medical history was very personal and incidents of selling medical information had raised some concern. The participants were also aware of incidents related to internet companies selling customer information to other companies.

Social networking sites and other forums are known to disclose a lot of unwanted personal and contact information. Internet users are living under the illusion that privacy is always protected, which is not the case. Considering spam mails yet again, not many people actually know where the mail originated from or when they subscribed for the same. Personal information such as contact information, date of birth and even photographs has been misused over the internet. Yet users disclose such vital information over the internet without understanding the repercussions. Again national background plays a vital role. A particular piece of information considered private in one country may not be regarded the same in another. For instance, date of birth is considered highly confidential in the South-East Asian countries while it is considered just as another piece of information in western

countries. Similarly during the survey, it was found that the responsibility protection of such information rested with website owners and government authorities. While it was not pointed that users too have some level of responsibility with regards to the tremendous amount of personal and unwanted information they disclose on social networking sites.

Participants reported to have registered at various forums and other websites through which they would like to receive regular updates and posts. Such websites are known to pay tribute to other organizations which target customers to increase their business. This brings us to the fact that companies may at times sell customer information with other companies to generate revenue. Through the survey topics, it was identified that participants were not aware of any such situation and that they trusted such forums to use their information for only legitimate purposes. The participants were not even aware if there were any laws which ensured protection to their personal information.

4.6 Legal aspects

The legal and judicial systems in different countries play an important role in shaping security culture. As per the survey it was concluded that laws in many countries were still evolving, as defining jurisdiction over the internet was a very complex task. In spite of having issues with information protection and privacy, a handful of the participants were aware of the laws pertaining to the same. Participants belonging to the western developed countries were to some extent aware of the laws protecting data (Data Protection Act). They also mentioned that the act was in most cases conflicting with the Freedom of Information Act. As far as developing countries were concerned the laws were non-existent as security issues were not a priority in those countries.

The legal system has a very important role to play in influencing an individual's attitude towards security. Legal and regulatory aspects of the internet make the users more confident while using the internet and addressing issues that they may encounter. However, the participants were not exactly aware of the laws governing the internet in their respective countries. Another important factor that governs a particular country's judicial system is the level of technological advancements achieved by country. As mentioned in the earlier sections, security is one aspect which is dependent primarily on the infrastructure availability within a country. Priorities of a developing country vary significantly from those of a developed country. This brings us to the conclusion that, in developing countries laws and legislation related to technology misuse are just being designed and approved. Countries which have concerns related to privacy have laws implemented to address the same. Data Protection Act is one such instance of law dealing with privacy issues. However Data Protection Act very frequently come into conflict with the Freedom of Information Act. The most challenging aspect of internet law is that, it is difficult to bring justice across the borders, as a particular illicit activity in one country may not be illicit in another.

5 Conclusion

For the purpose of this research, security culture was broken down into themes relating to daily internet usage and awareness with regards to concerns, security measures and legal system. As per the observations made during the survey sessions, every nation has some form of security culture in place. Security culture primarily depends on the technological infrastructure and its usage. For developing countries maintaining availability of the infrastructure is a primary concern, due to which security culture is not so prevalent at the moment. As far as developed nations are concerned, the infrastructure has existed for a while and is improving day by day, securing the infrastructure is the next step, so a more proactive security culture exists as compared to the developing countries. This can also be reflected in the number of users in the developed being comfortable in using the internet to carry out financial transactions and online shopping. However, internet users in developing countries are more concerned and sceptical while using this functionality of the internet. Not having a effective level of security over the has affected the risk taking ability of internet users. A considerable amount of similarity was observed with regards to the security mechanisms adopted, so security perspectives were very similar with this regards. The legal system varies across borders and hence the legislation for laws pertaining the internet are also bound to be different. The significance and sensitivity of the data to be protected also varies when we consider different countries.

Currently the term "information security culture" is often drawn near models describing organizational culture. However, considering only the organizational culture **is** not sufficient for understanding the influencing factors behind information security culture. Each individual working for an organization or accessing the internet at home is influenced by several ethical, national and organizational cultures. These cultures have an effect on the way the individual infer the meaning and importance of information security. .

6 Further Work

The current research work was restricted to the participants from the university campus itself. The research just focused on the various concerns and other factors which would influence the respondent's attitudes towards security. Qualitative methods of analysis were successful in obtaining subjective answers from the participants; however the future research attempts could have a approach using a combination of both qualitative and quantitative research methodologies. As one aspect of this research focused on the analysis of awareness regarding the security measures, the subsequent research attempts could aim at analysing the usability issues of the same. In the future, a concrete methodology to analyse both qualitative and quantitative data would also be instrumental in given better results to the research.

7 References

Helokunnas, T. (2003). Information Security Culture in a Value Net. *IEEE*. 03 (1), p190-194.

Malcolmson, J. (2009). What is Security Culture? Does it differ in content from Organizational Culture?. *Security Technology*. 43 (1), p361-366.

Schlienger, T. (2003). Analyzing Information Security Culture: Increased trust by an Appropriate Information Security Culture. *IEEE*. 88 (3), p1-5.

Security Governance.net (2010). Security culture Available: http://www.securitygovernance.net/clulture/index.htm. Last accessed 17 July 2010