Information security studying by means of extracurricular research projects

Gevorg MARGAROV [a,1]

[a] *State Engineering University of Armenia, Department of Computer Systems and Informatics, Yerevan, Armenia*

Abstract. This article is devoted to problems of information security studying by means of extracurricular research projects on base of the university. The expediency of a choice of information security as a subject of extracurricular studying is proved. Aspects of information security awareness are considered and their influence on educational process is discussed. The technology of studying by means of extracurricular research projects is briefly described.

Keywords. Extracurricular research project, information security, aspects of awareness, studying technology

Introduction

The world economy and the life are moving from a predominantly industrial society to a new set of rules - the information society. Digital technologies make accessing, processing, storing and transmitting information increasingly cheaper and easier. The sheer scale of information available creates huge opportunities for its exploitation through the development of new products and services. Transforming digital information into economic and social value is the basis of the new economy, creating new industries, changing others and profoundly affecting citizens' lives. Enterprises in all sectors are starting to transform their business into e-business - requiring from the consumer of more and more wide use of information and communication technologies in a daily life.

In these conditions a secure information infrastructure is, after widespread availability of broadband access, the second enabler of a broader access to information technology for all. Acquaintance to means of information security is required to each user of electronic means of information interchange, therefore information security in the future becomes "the third literacy" along with "the second literacy" - possession of a computer and information technologies.

Taking into account above stated in State Engineering University of Armenia the pilot program of high school and baccalaureate level university students training of information security by means of extracurricular research projects is developed and prepares for realization.

---

[1] Corresponding Author: Gevorg Margarov, State Engineering University of Armenia, Department of Computer Systems and Informatics, 105 Teryan str., Yerevan, Armenia; E-mail: dunmar@arminco.com

1. Why the wide awareness of information security is so important?

The relevance of information security awareness is widely agreed upon among information security researchers. The concept of information security awareness is taken in the literature to mean that users should he made aware of security objectives (and further committed to them). Although information security awareness is commonly recognized, there are only a few scientific studies that consider it in any depth. Perhaps this situation can be traced back to the non-technical nature of security awareness and related areas. The concept of awareness may have been not considered in greater depth because it falls outside the scope of the traditional engineering and computer sciences [1].

Even though researchers interested in information security have recognized the significance of the awareness factor at the organizational level, it is curious that they have failed to see its other aspects. The information society has a powerful need to extend this organizational viewpoint, however. We are based on a belief that the concept of information security awareness, in addition to the organizational viewpoint, should also constitute an integral part of the general knowledge of citizens in the information society In other words, anyone who regards information in any form as an important asset should be aware of the possible threats related to it.

For different reasons, a lot of people see issues and aspects connected with information technology (IT) through rose-colored spectacles, often blindly ignoring potential complications. For example, it seems that many companies, individuals and educational institutions think that it is important to increase technical IT skills, to use IT for almost every conceivable purpose and to advance the computerization of society in general. And often the main limits they see for such development are financial restrictions or lack of technical knowledge which should therefore be increased. Moreover, catch phrases such as "information revolution" or the names of particular programs (such as MS Word) have strong positive metaphorical associations, redolent of paradise. In addition, IT is already embedded in our everyday lives to the extent that we often fail to notice it (let alone realize the encapsulated security flaws). As a result, even occasional IT users should be aware of basic security issues. Organizational informational security awareness is not sufficient to satisfy the concerns of security - additional aspects are needed.

The main contribution and objective of the theoretical training during extracurricular research projects is to outline the various aspects of information security awareness and to explore certain key issues around these aspects. Additionally the categories (or target groups) in each aspect are distinguished. In other words, the scope of the theoretical training is limited to setting up information security aspects in terms of form and target groups by proposing a framework for awareness perspectives in order to raise certain issues and produce practical examples in the hope of inspiring further research and practical activities around the topic at a stage of performance of research projects. Conceptual analysis is used as the research approach and in order to justify the aspects and categories in the light of this conceptual analysis, a number of practical examples are provided.

2. Aspects of information security awareness

As mentioned earlier, the aspects of security awareness are based on the belief that awareness is an issue that everyone using any form of IT services, either directly or indirectly particularly in an Internet environment, should bear in mind. It is possible that a wider knowledge of these awareness aspects may have negative consequences if it is used to commit abuses (this may be true of all kinds of knowledge, of course), and this may be one reason why information is not shared equally among the parties mentioned below. In an attempt to formalize an essentially informal issue with various aspects into an understandable pattern, the aspects of awareness may be classified as follows:

- The organizational aspect.
- The general public aspect.
- The socio-political aspect
- The computer ethical aspect
- The institutional education aspect.

Because of the informal nature of information security awareness, there may not be any exact and dear borders between these aspects. Within the organizational aspect, for instance, we have to take into account issues that belong to the general public aspect.

Two very different characteristics of information security awareness have to be considered. The first relates to the division between descriptive and prescriptive, as modified and simplified from the theory of universal prescriptivism [2]. The term prescriptive denotes here (only) intrinsic, action-guiding commitment to the objectives of awareness (e.g. security guide-lines), while descriptive, albeit including some level of knowledge of information security, may not include such an action-guiding commitment to objectives. Other aspects of information security awareness are classified as descriptive, as commitment to certain security norms may not be necessary.

As a second characteristic, it seems to be that security awareness may be difficult to internalize properly in the sense that it may often be regarded in the same way as a matter of health; nothing is done as long as nothing goes wrong. And when things do go wrong, people are suddenly very keen on the issue. The problem is that when something undesirable happens, it often requires a huge effort to recover from the situation, if recovery is possible at all any longer.

2.1 The organizational aspect

There seems to be common agreement that security awareness (like education) plays a significant role in the overall security level of any organization. Without an adequate level of awareness, many security techniques are liable to be misused or misinterpreted by their users, the possible result being that even an adequate security mechanism may become inadequate. Several approaches to increasing user commitment to organizational security guidelines have been presented [3], but most of these fail to pay enough attention to behavioral theories, and the empirical studies based on behavioral theories are especially urgently needed. Moreover, measurements of the adequacy of awareness approaches (e.g. whether the motivation of end-users towards security missions or end-user guidelines has increased) are far and few between and this is still an open issue which can be a subject of studying within the framework of extracurricular research projects.

The categories of the organizational aspect of awareness refer to different target groups for security awareness at an organizational level. Examples of these categories may

3

include the following: top management, IT/IS (Information security) management, IS staff, computing/IS professionals, end-users of various kinds (e.g., casual end-users, parametric end-users, sophisticated end-users and stand-alone users) and third parties. From the organizational point of view, these target groups need different kinds of information on security.

With respect to the top management category, awareness is most closely related to the gap between top management and information security concerns. In this respect, the main objectives of awareness are A) getting the commitment of the top management; B) reaching an exact understanding and consensus within the top management as to what components of the organization require protection (along with the nature of that protection).

The other possible categories starting from IT/IS management and going on to normal end-users are largely about sealing the gap between information security and the various target groups of the awareness programs (such as those mentioned). Necessary information concerning information security issues must be shared, and this information must be clarified to all the target groups to enable them to reach a state of commitment (the ideal state from an information security point of view).

Finally; the third party category of the organizational aspect of awareness consists of factors by which the company ensures that third parties are aware of the required information security level.

2.2 The general public aspect

The general public aspect can be divided into two target groups: IT/computer/IS professionals and other end-users. The professional skills of IT/computer professionals should include certain knowledge related to security. Consequently, professional qualifications should be established that harmonize and develop these skills alongside others. Furthermore, the professional associations should co-operate with educational institutions to manage this procedure and to determine the content of the relevant knowledge and skills.

The main objective in terms of the other target group of the general public aspect is to increase public awareness of relevant security issues. The main idea of this aspect is based on the argument that there are some central information security issues that every citizen using IT should be aware of. Although the Internet is one of the main causes behind this concern, there are many other information security threats not related to it, such as cash and smart cards (as used by ATM machines, mobile phones, etc).

There are many common practices that, if not carried out carefully, could constitute a secularity threat. Perhaps the most common ones include the failure to observe adequate password procedures and careless use of the Common Gateway Interface (CGI) or Application Programmer Interface (API). These practices, if neglected or undertaken carelessly offer an easy way for third parties to violate the system and the users (account holders) informational privacy and assets.

In addition to the possible problem areas, Internet users, (organizations and individuals alike) should also consider carefully what information they put on their homepage, plan file (which is accessible via a finger command), voice mail, e-mail, speak mail, etc. Many people may not yet be aware of the insecurity of the Internet (as the TCP/IP protocol family

4

is insecure without the use of additional cryptographic techniques and may send "classified" information by it (e.g. credit card numbers).

2.3 The socio-political aspect

The socio-political aspect involves increasing people's information security awareness with respect to the socio-political nature of IT. This aspect includes the following categories (target groups): lawyers, public relations people, politicians and the government. Information security awareness is an important concern within the socio-political aspect and an important factor in terms of the overall well-being of society. Many countries are developing electronic services for official communications and trading. Failures to see the importance of security issues related to such solutions may lead to serious complications in terms of the well-being of the society in question.

Laws are another case in point. As we know, legislation is often said to be lagging behind current technological development. Nevertheless, in order to be successful, it should reflect the moral view of society in question. For that reason, politicians should be aware of information security issues in high-level and ethical principles, because, at least in democratic societies, they are directly or indirectly responsible for making legislative decisions. Hence, along with lawyers, they should understand information security issues at a high-level. If the moral perspective of IT is neglected, a moral/legislative gap may emerge, implying conceptualist laws (laws for which the moral background has not been explored), which may be detrimental to human well-being. Many juridical experts on IT legislation are convinced that the Internet will force the introduction of some form of global legislation, mid various pressure groups such as the EU and the UN are already starting to push in this direction. One weakness, however; may be that too few people in these circles have an adequate knowledge of security issues, for many of these issues require thorough contemplation with the help of ethical theories and facts (including security issues).

Finally, public relations people are also key players in the security game, because they are in a position to inform people of various information security issues. Information security practitioners should ensure the co-operation of this group in order to be able to influence the general public aspect through them.

2.4 The computer ethical aspect

The objective of the computer ethical aspect is first of all to provide relevant (e.g. technical) information for (computer) ethics scholars, and secondly to learn from and make use of their conclusion. These scholars study, among other things, ethical dilemmas and problems, and there is a strong demand to produce continuously updated issues (e.g. technical facts) that covers the whole area of IT. Information security researchers are likely to be helpful in providing information concerning security issues which computer ethics scholars can use when studying its moral aspects. Co-operation and sharing of information between information security people and computer ethics scholars have so far been ineffective, in spite of the fact that many such issues offer possibilities for synergism (they might share some of the same goals, for example). Computer ethics can perhaps be defined

5

as an approach for finding the best solution to the problem of enabling harmonious human life in the information technology domain.

Although information security is not ethics (nor vice-versa), information security (or security generally) may have a certain special connection with the field of ethics. This does not mean that security activities are more right per se than any other activities, whether scientific or practical (and as a result we should analyze all activities equally from a moral point of view). Instead, this special connection means that security activities, whether in terms of science or practice, are mainly stimulated by a concern to prevent certain activities that are interpreted as abuses. Moreover, demands have been raised by computer ethics scholars to develop (more specific) professional norms, the creation of which may benefit technical facts on information security - even though not purely based on these.

In addition, issues related to computer ethics are intimately connected with legislative issues: behind successful legislation there is a moral aspect. Without a moral consensus, laws tend to be ignored, regardless whether the law is considered important - a lesson that the information age needs to learn. As is known, arguments appealing purely to legislation (e.g. "because this is the law or rule"), are not sufficient per se to qualify peoples actions. Therefore, a one possible mission of this aspect, from an information security point of view, should include the provision of persuasive arguments for legislation. As a result, the computer ethical aspect is important for information security. If people were to regard particular security breaches, misuses or abuses (e.g. distribution of viruses) as immoral, they might avoid them. Security people (or those concerned about security) would likely to be beneficiaries of a strengthening in moral thinking in the area of computing,

2.5 The institutional education aspect

Institutional education refers to a society-driven process of education that is aimed at making individuals proper members of society. In this way society-ideally-will develop and renew its culture in a desirable way (and hopefully in a way that is not based on indoctrination). However, the amount of technical education provided with respect to computers is increasing, and organizations are increasingly using computers and global computer networks such as the Internet. Unfortunately, as a result of this (and without any information security awareness), the sheer number of people who constitute a potential target for criminals and misusers is increasing.

Consequently certain relevant information security concerns should be included in the educational programs, which is seldom the case at present. Many high school and university curriculums seems to be concentrating only on technical skills, while ignoring the relevant social, ethical and security aspects encapsulated in IT.

Moreover, the increasing number of home Internet users and organizational end-users with little knowledge may cause damage through careless use (virus distribution and creation are cases in point). From the point of view of educational institutes, the former ease raises the need for providing relevant computer ethical education. Educational institutes play an important role in this, for in addition to imparting technical knowledge, they also teach ethics and bring up ethical topics for discussion. To summaries, the mission within this aspect is to share relevant information with various educational institutes, bearing in mind the fact that they have different educational needs.

3. Technology of studying by means of extracurricular research projects

On the basis of the considered aspects extracurricular education should be carried out in several target groups which correspond to prospective future specialties of trained. In these conditions the most convenient form of information security studying has to by base on extracurricular research projects, which should include various aspects for each of target groups. Inside of each target group a number of small working subgroups (3-5 students) are formed for performance of separate projects.

Trained carry out several consecutive projects, term of performance each of which is one academic year. On the first year of the studying all subgroups receive research project tasks of survey character with approximately identical complexity. At the end of each academic year the public representation of projects with attraction of representatives of the enterprises interested in the result of projects is made. According to the marks received trained during representation of projects new subgroups, are formed thus that each subgroup entered trained with approximately identical marks. For the next academic year new subgroups receive tasks for the following project. Thus complexity of projects is directly connected to the marks received by students in the subgroup. In other words more talented students who had the maximum marks receive more complex (difficult) project tasks with elements of scientific researches.

The most interesting projects devoted to the decision of real technical and scientific problems are recommended for publication and application in corresponding organizations. Work in small subgroups allows not only to reveal the most talented students, but also to form ability to teem work and aspiration to leadership.

References

[1] M .E. Thompson and R. von Solms, An effective information security awareness program for industry. – Proceedings of WG 11.2 and WG 11.1 of TC11 (IFIP): *Information security - for small systems to Management of Security Infrastructure*. 1997

[2] R. M. Hare, The Language of Morals. Oxford University Press, Oxford, 1952

[3] P. Spurling, Promoting Security awareness and commitment. Information Management and Computer Security, Vol. 3 No. 2, 1995, pp. 20-26