Information Security e-Learning - from Practice to Theory

Jorma Kajava*, Rauno Varonen**
* University of Oulu, Department of Information Processing Science, Linnanmaa, Oulu
P.O.Box 3000, FIN-90014 UNIVERSITY OF OULU, Finland
Jorma.Kajava@oulu.fi
** University of Oulu, Language Centre, Linnanmaa, Oulu
P.O.Box 7200, FIN-90014 UNIVERSITY OF OULU, Finland
rvaronen@cc.oulu.fi

Abstract

Focusing on security education, this paper describes an e-learning environment that has been constructed to increase information security awareness among employees of a Finnish telecommunications company. The system has already entered the testing phase, and the preliminary results are interesting – and somewhat unexpected: the designers' assumptions about the current knowledge level turned out to be too high. On the other hand, the design principle, based on making the components of the system as simple as possible, seems to have produced a system that delivers both functionality and stability.
Keywords: e-Learning, information security, information security awareness.

Povzetek

E-izobraževanje na področju varnosti podatkov – od prakse do teorije

Članek opisuje okolje za e-izobraževanje, ki smo ga razvili, da bi dosegli večjo ozaveščenost o problematiki varovanja podatkov med zaposlenimi neke finske telekomunikacijske firme. Sistem je že v fazi preizkušanja, prvi rezultati pa so zanimivi, vendar nekoliko nepričakovani: izkazalo se je namreč, da so razvijalci predpostavljali, da je raven znanja višja, kot je v resnici bila. Po drugi strani pa je osnovni pristop, ki temelji na kar se da enostavnih komponentah, pripeljal do sistema, ki je hkrati funkcionalen in stabilen.
Ključne besede: e-izobraževanje, varnost podatkov, ozaveščenost o varnosti podatkov.

1 Introduction

This paper discusses an e-learning based information security project carried out by a small organisation in the telecommunication service sector. Interestingly, the organisation has outsourced all software development work. All 500 employees on the payroll, mostly technically-oriented specialists, have the basic information processing skills required by their jobs, but only a few have a broader experience of the information sciences.

In a small organisation, it is relatively easy to construct a learning environment and test its functionality in practice. To be useful, the environment must be built in close collaboration with the intended users, i.e., the environment and its contents must be based on their opinions and experiences and meet their practical needs. In the present case, an extensive survey was conducted to find out the employees' wishes and needs regarding the environment [13].

Experiences gathered during this project form the basis for its adaptation to the university setting. The arrangement is advantageous, because development work in a small organisation is fairly flexible, and experiences accumulate quickly. Universities, on the other hand, although constituting open learning environments, tend to suffer from a higher degree of bureaucracy, which may affect the design or implementation of the learning environment. Thus, a trial system tested in practice is an essential resource for planners and constructors [6].

The topic area, information security, was selected as it is rapidly becoming a key issue for businesses, institutes of education and society at large. Traditionally, the highlight has been on the technical aspects of information security, but during the past few years, human and organisational aspects have assumed an increasingly prominent role in discussions on security [1, 2, 3, 4, 19, 20, 21].

E-learning based information security education strives to raise the awareness level of all employees. The aim is to equip them with the necessary skills and knowledge to meet the challenges that they may have to face in their everyday work [12].

The ultimate purpose of this paper is exploring the use of an electronic learning environment to enhance information security awareness.

2 Methods and techniques used

This study was carried out in the target organisation in 2002. The immediate goal was to investigate the information security knowledge of the employees by means of questionnaires and interviews. The results were then used to create an educational programme to correct the perceived weaknesses. As teaching material, the programme utilised various organisational guidelines complemented by educational materials compiled at the University of Oulu.

In addition to the actual learning environment and its contents, the organisation has also implemented an automatic online assignment sheet for tracking and monitoring learning. This form was designed to automate the learning process such that anyone who possessed the necessary skills and knowledge, could take the test and – on successful completion – be automatically exempted from having to go through the learning material. The system automatically handles registration and also updates registry files, when students pass the test. In essence, the environment enables company employees to study at their own pace. What it still lacks is a rewarding system for employees who receive a good grade [14].

Research tends to progress from theory to practice. Having become familiar with information security from various perspectives including the user and end-user perspectives, we decided to go the other way – from practice to theory. Our starting point was that, within information security, relevant knowledge usually resides within the organisation in question. What an outsider, such as a consultant, can contribute is a model or a general framework for exploring, enhancing and utilising this knowledge. On this view, pertinent information that is possessed by company employees is collected and analysed by an outside consultant who introduces a theoretical framework for analysis and may also assist in the utilisation of the results of such analysis.

The practice to theory approach is also supported by the fact that all information security events comprise a variety of aspects, some of which are strongly in relief, while others can best be described as weak signals. Even these can be taken into account thanks to the increased computing power of modern computers, which allows the unique features of each information security incident to be analysed in detail.

This study investigated the information security knowledge of different employee groups using a semi-structured theme interview. At the same time, we were able to establish which areas of information security knowledge needed improvement. This information formed the foundation for the design of the e-learning programme.

However, before delving into these issues, let us first discuss information security awareness in general.

3 Information security awareness

On the basis of a series of practical studies, we have come to the conclusion that there are several stages in how people respond to awareness. It seems that there are three stages of awareness that should be taken into account. We maintain that these stages constitute an implication relation, where – within practically every organisation – there are people at every stage, and the success of IT security awareness correlates with progress toward the next stage. The stages of IT security awareness are [7, 8, 9, 12, 22, 23]:

(ii) drawing people's attention to security issues,
(iii) winning user acceptance,
(iv) getting users to learn and internalise the necessary information security activities.

The first stage includes drawing people's attention to information security-related issues and trying to catch their interest. The second stage involves user acceptance; having attracted the end-users' attention, it is important to get them to accept the organisational IT security policy. Finally, at the third stage, the end-users should have internalised the instructions they have received during their security-related education and should take corrective measures in accordance with the security policy. In this paper, the term 'awareness' includes all the aspects mentioned above.

IT security awareness should be comprehensive, well-organised and systematically executed from the start. In addition, the efficiency of all actions should be measured to ensure the on-going development of the organisational IT security awareness programme. As for our own IT security awareness programme in the university environment, we have come to the realisation that a wide range of tools and methods are necessary to implement security awareness for different people in different environments and at different stages of awareness. Security education is needed to

convince every user of the importance of following guidelines and to make them aware of the consequences of intentional violations of information security. Education is also needed to ensure that the achieved level of awareness (as defined above) will be maintained. Various awareness raising methods, such as campaigning and the so-called Hammer theory, are needed to provide incentives for end-users and to refresh the importance of these factors in the minds of people. And finally, awareness, comprising education and training, should ensure that people internalise security guidelines and abide by them in their daily work.

The awareness programme of any industrial organisation should follow the framework developed in Reference [7, 8]:

(i) Identify programme scope, goals and objectives.
(ii) Identify training staff.
(iii) Identify target audiences.
(iv) Motivate management and employees.
(v) Administer the programme.
(vi) Maintain the programme.
(vii) Evaluate the programme.

The awareness programme should be targeted for at least four different groups. These are: top management, IS management, end-users and IT/IS specialists. Of course, there is no exact formal classification for these groups and, as a result, the end-user group, for example, remains relatively vague.

The IT security awareness programme should be implemented at all levels of the organisation, starting from the top management, who should be made aware of the need to establish and maintain an organisational security policy [7]. Then comes the creation of a security model including IT security policies, the allocation of responsibilities, etc. IT security awareness programmes are essential in keeping users in the "security team" and in ensuring the overall success of the organisation's security strategy. All evidence shows that to function satisfactorily, a security programme must find support in all parts of the organisation. Moreover, the top management has to accept the security policy whole–heartedly and allocate resources and appropriate financial support accordingly. As stated earlier, the effectiveness of the measures taken during an awareness programme should be evaluated as objectively as possible. The problem is that most organisations do not provide feedback or measure the success of their IT security awareness programme. The security management should react to feedback and consider necessary improvements. Feedback should be based on organisational and end–user viewpoints and on the established results of particular security measures [8].

4 Security learning

Understanding information security issues from the technical point of view is an advantage that employees of the case company have [10, 15]. Nevertheless, since they do not have a wider perspective on other aspects of security, such as organisational or end-user related issues, they need information security training [11]. The problem is that, being small, the company does not have the resources to allow its personnel to take time off from work to participate in security training [16]. This paper seeks to answer the question of what technical tools the company could use in this situation.

One solution is to resort to e-learning and construct an online learning environment. Many e-learning environments are realized by long distance networks, via the Internet, but our solution was to build an intranet-based environment, within the company network. Most e-learning solutions consist of very sophisticated and complicated systems, filled with content that is more entertainment than work-oriented, but we proposed a solution that is both simple and practical.

In the long run, the project reported here aims to develop a five-level solution consisting of different guidelines custom-tailored for different groups. At the first stage of this research, the focus is on guidelines that apply to all user groups. First, a questionnaire on currently prevalent practices is sent to every group. Then, having analyzed the results, the most important guidelines are collected for organisational use using the e-learning environment. It is important that these guidelines are easy to understand and follow - and it would not hurt if they were presented in a humorous way [18].

In addition, it is vital that the information security education programme is automated and computer-supported as well as transportable to different environments, including those based on older systems. As a result, the e-learning environment can be transported to other organisations working in the same field. Moreover, as the basic guidelines pose no problems for employees with a deeper knowledge of the sub-

ject, they must have the option of going directly to the test part, without having to trudge through the entire programme.

5 Requirements for the learning environment

The starting point for this project was the fact the organisation under study is a profit-seeking commercial enterprise. Aiming at improving the security level of this organisation, the project also offers it a competitive edge through the provision of more secure telecommunication services. Technical solutions, although constituting the foundation of security, are insufficient and must be incorporated into a wider approach.

In a drive to promote information security across the organisation, the company initiated the e-learning project reported here. It seeks to find new, cost-effective, ways of offering security education to company employees. A guiding principle is this undertaking is that the education offered must be meaningful and immediately relevant to the employees.

In carrying out their everyday tasks, people tend to place a high value on usability, sometimes at the expense of security. Sadly enough, the significance of information security is often realized only after some mishap occurs.

Another balancing act is frequently observed in the context of e-learning [13]. Striving toward a more exciting and entertaining approach, educators sometimes lose sight of their original purpose, and become entertainers rather than educators. From the organisational viewpoint, the crucial question is which is more beneficial for the functionality of the organisation: a learning environment that is highly enjoyable or a learning environment that is highly usable and functional [5]?

The organisation under study here has posed a number of requirements for its new e-learning programme. For a start, it has to run on all computer platforms used within the company. In terms of structure, it has to be sufficiently simple to be reliable in all environments [16, 17].

6 Presentation and learning

Creating a multimedia e-learning environment requires not only technical and content-related expertise, but also a pedagogical advisor. Chief among the tasks of this advisor is to devise ways of presenting learning materials in a manner that enables learners to assimilate new knowledge into their previous knowledge structures - and thereby understand what they have learned. Another function of the pedagogical advisor is to take account of different learning strategies and styles to maximise individual learning results. If no such advisor is available, and the design of learning materials if left to technical experts, for example, the various multimedia elements may have more entertainment than educational value [18].

All learners have their own learning strategies. Part of each individual's learning strategy is their learning style, which is an essential element of the learning process. We all have our own strengths, which we rely on when processing information. Some people are characterised as holistic, while others are best described as analytic learners. The difference lies in the way they tend approach a task; holistic learners immediately strive for the big picture, whereas analytically-oriented learners favour a piecemeal approach.

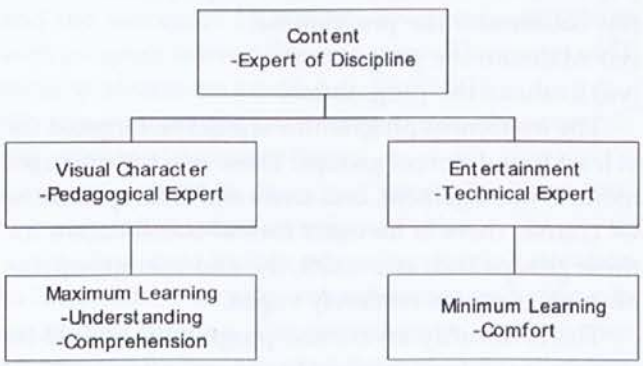

Figure 1. **e-learning and multimedia.**

Also our senses play an important part in the learning process. We receive and process information on the basis of our vision, hearing, tactile or kinetic sense. As a result, we have preferences as to how we want learning materials to be presented to us, how we want to see, hear, feel or experience the materials. Schools depend heavily on vision and hearing, at the expense of pupils who learn better by doing things, for instance. Some learners remember things as images, others as stories. A third group consists of learners who like to try things out through trial and error. Kinetically-oriented persons may memorise a telephone number or a melody, for example, as a sequence of finger movements, and learn certain things best while jogging or biking. Some people prefer to discuss things with other people, others teach themselves by

talking aloud. Most people have one or more preferred senses for receiving and processing information [16].

Learning styles based solely on one way of learning are very uncommon, as most people have their own learning strategies based on their strengths, habits and preferences. Consequently, a learning environment catering a large target group must be designed to accommodate a range of approaches and styles.

7 Significance of automated learning environment to the system

The purpose of the e-learning project was to construct a learning environment that does not require any additional hardware or software. In addition, the environment must be accessible from all workstations within the organisation [17].

For best possible functionality, the adopted solution seeks to minimise the effects of features that exist solely to increase the entertainment value of the environment. A major concern was the fact that an increased degree of automation inevitably leads to larger program code which, in turn, poses a threat to the stability and functionality of the entire system.

These two basic requirements, accessibility and full functionality from all workstations, relate to the levels of programming languages. It is a well-established truth that the lower the level of the used language, the faster the code and the smaller the memory requirement. Such code is also more secure. Nevertheless, implementing any system involves a compromise between automation and reliability, but the old adage "small is beautiful" is well worth bearing in mind.

8 Essential results

When we set out to design the e-learning environment, it was assumed that the basic information security guidelines of the organisation would be well-known by all employees. Therefore, it was a quite a revelation when the first tests in January 2004 indicated that some of the supposedly simple questions proved very hard to answer satisfactorily.

It was also revealed by the theme interviews that a great number of employees had no clear understanding of what information security is. All employee groups tended to describe it in terms of individual or isolated components. Moreover, about half of the interviewees could not explain in what ways information security issues would be relevant to their work. This shows that security education should start by breaking down the definition of information security and analysing how it affects everyday work.

Feedback relating to the use of the e-learning system was mainly concerned with its technical implementation. Typical comments include "it is slow" and "it takes a long time to start". Generally, the learners either wanted the multimedia components to load quicker or they wanted more functionality, including muting or resolution changes on the fly.

The actual content matter of the programme was not commented on. What little feedback was received indicated that the intended practical approach was appreciated and that the learning topics were experienced as having a practical value. This relative lack of feedback may be explained by the fact that the learners did not have any expectations as to the content matter, since they were unfamiliar with the subject. Also, the design of content may have been better than the technical implementation. In general, the e-learning system was described as an interesting novelty and a number of learners indicated an interest to participate in similar training on other topics as well. With an average of 5 - 6 hours, many learners stated that they had used less time than expected on the tasks [6].

Measuring information security awareness is a difficult undertaking. One way of approaching it is to observe employees while they are working to establish the degree to which they follow the given guidelines. However, this study investigated the topic through an interview conducted among the learners. These interviews started by exploring how the learners understood the concept of information security which, after all, constitutes the foundation of information security awareness. The latter term refers to how well employees and members of society understand various information security threats and the related responsibilities. The results show that a high level of awareness has been achieved when all personnel understand the meaning of information security in its full extent and apply this knowledge in their work [6]. In addition, personnel must also be able to identify and manage a range of information security threats. Finally, they must also know what to do to avert these threats.

This bring us to the critical question: is it possible to achieve this goal using an online learning environment?

Answering that question involves separating two different kinds of responsibility. Technical issues and software concerns should be tackled by hardware and software manufacturers, while issues relating to users and organisations are the province of education and are best dealt with by universities. It then follows that universities have the responsibility to define the structure and content of information security studies. In a very broad sense, this involves taking responsibility for ensuring the wellbeing of future society, which is highly dependent or communication and computers.

9 Conclusions

This paper discussed an e-learning environment for information security education, designed and constructed by a small Finnish telecommunications company. The experiences gathered so far indicate that the implementation of an extensive learning system of this kind must be based on simple solutions that minimise system load.

It became clear during this study that, to be successful, e-learning requires that the designers and tutors are familiar with the learners' needs and learning styles. Diverse ways of presenting the learning materials makes it easier for individuals with different learning styles to take in the information. What renders the entire task more challenging is that the content matter of information security is often fairly abstract, highlighting the importance of careful design and presentation. The education offered must provide a range of possibilities for interaction, because the chosen medium, online teaching, markedly lessens personal contact among teachers and learners. Other important aspect include the provision of support to the learners and ways of creating an inspiring atmosphere conducive to learning. Feedback provided by the teacher is an integral part of learning, and its role is even more important in online teaching, where studies are usually conducted in (relative) isolation from other learners. Time must also be allocated to electronic communication between the participants. And finally, attention must also be given to developing the proficiency of the teachers and promoting their interaction.

An interesting – and quite unexpected – finding was that the planners' assumptions about the level of security knowledge among company employees was fairly low. In the information age, every citizen should have a basic understanding of information security, otherwise they will be weak links in the chain, vulnerabilities that can be exploited. Increasing the level of security knowledge necessitates the implementation of various kinds of information security awareness programmes, an example of which is provided by the e-learning environment described here.

Acknowledgements

The authors wish to extend their thanks to Mrs Tiina Ramet, Mr Ilari Heikkinen and Mr Erkki Tuormaa, who have been responsible for the practical design and implementation of the e-learning system.

References

[1] BS7799-1:fi. Standard. – Information Security Management. Part 1: Code of practice for information security management systems. Finnish standards association SFS, 15. February (1999).

[2] BS7799-2:fi. Standard. – Information Security Management. Part 2: Specifications for information security management systems. Finnish standards association SFS, 15. February (1999).

[3] A Code of Practice for Information Security Management, Department of Trade and Industry. DISC PD003. British Standard Institution, London, UK. (1993).

[4] Computer Security Handbook, The Practitioners Bible Computer Security Institute. Mac/Donnel Printers, USA. (1984).

[5] Epelboin, Y. : E-learning: putting documents On the web – Do and Don't. Workshop in the 8th Conference of European University Information Systems (EUNIS 2002). European University Information Systems (EUNIS) and University of Porto, Faculty of Engineering. June 19 - 22. Porto, Portugal. (2002).

[6] Heikkinen, I., Ramet, T., "e-Learning as a part of information security education development from organisational point of view". Oulu University. Oulu. May (2004) (in Finnish).

[7] ISO-IEC-27, Guidelines for the Management of IT Security (GMITS): Part 1 – Concepts and models for IT Security. (1994).

[8] ISO/IEC JTC1/SC27, Guidelines for the Management of IT Security (GMITS). (1995).

[9] Kajava, J. & Siponen, M., "Effectively Implemented Information Security Awareness - An Example from University Environment". In Jan HP Eloff and Rossouw von Solms, editors: *Information Security - from Small Systems to Management of Secure Infrastructures.* Proceedings of WG 11.2 and WG 11.1 of TC11 (IFIP TC-11 Sec'97, 13th International Information Security Conference). IFIP, 13 - 16th May, Copenhagen, Denmark. (1997).

[10] Kajava, J., "IT Security Infrastructure – Opportunity or Threat for Future Society?" Politics & Internet. 2nd International Congress on Electronic Media & Citizenship in Information Society. The Finnish National Fund for Research and Development (SITRA) on the initiative of the Committee for the Future of the Finnish Parliament. 6-9 January, Espoo, Finland. (1999).

[11] Kajava, J., Varonen, R., "Information Security Education: From the End-User Perspective to Public Administration Applications". In *Verwaltungs-informatik 2000: Verwaltungsinformatik in Theorie, Anwendung und Hochschulausbildung* /3. Internationale Fachtagungen "Verwaltungsinformatik" der Gesellschaft für Informatik (FTVI HBS 2000). Herausgegeben von Hans-Jürgen Lüttich und Claus Rautenstrauch. Otto-von-Guericke-Universität Magdeburg. 11 – 13th October. Halberstadt, Germany. - **mdv** Mitteldeutscher Verlag GmbH Halle (Saale), Germany. (2000).

[12] Kajava, J., Varonen, R., "Incorporating Information Security into University Infrastructure". In Ligia Maria Ribeiro, Jose Marques dos Santos (eds): *The Changing Universities: The Challenge of New Technologies.* The 8th Conference of European University Information Systems (EUNIS 2002). Proceedings. European University Information Systems (EUNIS) and University of Porto, Faculty of Engineering. June 19 - 22. Porto, Portugal. (2002).

[13] Kajava, J., Pyy, J., Tuormaa, E., Heikkinen, I., Mukari, J., Ramet, T., "Education material produced by TiKo project". Oulu Telecom Plc. May 16. Oulu, Finland. (in Finnish). (2003).

[14] Kajava, J., Tuormaa, E., Ramet, T., Heikkinen, I., Kuusijarvi, T., Polvi, M., "Automated online assignment sheet for tracking and monitoring e-Learning. EFo program." Oulu Telecom Plc. November 20. Oulu, Finland. (in Finnish). (2003).

[15] Kajava, J., "Information Security Challenges for Users, End-Users and Organizations in the Beginning of the new Millennium" (Abstract in English). *Administrative Studies Journal*. Volume 19, Number 2. Tampere, Finland. (2000).

[16] Kajava, J., Varonen, R., Tuormaa, E. Nykanen, M., "Information Security Training through eLearning - Small Scale Perspective". In Eveline Riedling (ed.): *VIEWDET 2003*. Vienna International Conference on eLearning, eMedicine, eSupport. Vienna University of Technology. Nov. 26. - 28. Vienna, Austria. (2003).

[17] Kajava, J., Varonen, R., "e-Learning as a Tool: Framework for Building an Information Security Awareness Programme for a Local Teleoperator". In Jeanne Schreurs and Rachel Moreau (eds.): Euromedia'2004. Tenth Annual Scientific Conference on Web Technology, New Media, Communications and Telematics Theory, Methods, Tools and Applications. Huize Corswarem. Hasselt, Belgium. April 19 - 21. A Publication of EUROSIS. Ghent, Belgium. (2004).

[18] Neal, L., Perez, R., Miller, D., " eLearning and Fun". CHI'04 SIG. ACM. Vienna, Austria. April 26 - 29. (2004).

[19] "The NIST handbook, An Introduction to Computer Security", NIST special publications. October. USA. (1995).

[20] Parker, Donn B., "Computer Security Management". Prentice Hall, Reston, USA. (1981).

[21] Royal Canadian Mounted Police, Security in the EDP Environment. Security Information Publication, Second Edition. Gendarmere Royale du Canada. Canada. (1981).

[22] Thomson, M.E., von Solms, R., "An Effective Information Security Awareness Program for industry". In Jan HP Eloff and Rossouw von Solms, editors: *Information Security - from Small Systems to Management of Secure Infrastructures.* Proceedings of WG 11.2 and WG 11.1 of TC11 (IFIP TC-11 Sec'97, 13th International Information Security Conference). IFIP, 13 - 16th May, Copenhagen, Denmark. (1997).

[23] Walsh, T., "Measuring the Effectiveness of Computer Security Training". 23th Annual Security Conference and Exhibition. CSI. November 11 - 13. Chicago, Il. (1996).

Jorma Kajava graduated from the University of Oulu in 1976 (M.Sc., Dept. of Technical Physics, Control and Systems Engineering) and completed his Licentiate Degree in 1978 (Faculty of Technology, Wireless Telecommunications, Adaptive Antennas). Since then he has been in the employ of the University of Oulu in various positions, including Lecturer, Head of Laboratory, Acting Associate Professor and Acting Professor. His teaching experience includes not only the University of Oulu, but also the University of Lapland, the Raahe and Oulu Polytechnics as well as other institutes of education. Aside from his involvement in numerous international projects (including the European Commission's Information Society Technologies (IST) Programme), he has found the time to write c. 350 articles, published in a variety of formats such as conference proceedings, journals, research reports, electronic publications, educational support materials and newspaper articles. Among his research interests are computer ethics, information security and e-learning.

Rauno Varonen has worked at the University of Oulu since his graduation in 1985 (M.A, Faculty of Humanities). He did his teacher training in 1985-1986 and completed his Licentiate Degree in 1996. Working as a Lecturer at the university's Language Center, he has a wide teaching experience. His publications include teaching materials and academic papers. One of his interests is e-learning, which he approaches from the practitioner's viewpoint. He is also a distinguished member of the Black Hole.