INFORMATION SECURITY IN E-LEARNING: THE MATTER OF QUALITY

MARJAN MILOŠEVIĆ
University of Kragujevac, Faculty of Technical Sciences in Čačak, marjan.milosevic@ftn.kg.ac.rs
DANIJELA MILOŠEVIĆ
University of Kragujevac, Faculty of Technical Sciences in Čačak, danijela.milosevic@ftn.kg.ac.rs

Abstract: *Paper deals with analysis of security aspects of e-learning and its relation to quality in e-learning on Serbian example. It is shown that no special attention is paid to security in e-learning, but also that end-users indicated need for stronger security culture. Extracts from quality assurance schemes are used as proper guidelines for quality enhancement and, combined with user feedback, are put into cornerstones of a model that is supposed to assist in quality enhancement.*

Keywords: *e-learning, security, quality assurance*

1. INTRODUCTION

Rapid development of information and communication technologies is followed by market shift that requires need for lifelong learning. Natural result of these tendencies is increased interest for on-line learning, as an affordable option that provides possibilities for using advanced contents in learning/teaching. In this context, many pure online courses and study programs are being established. Also online learning has quickly found its place within traditional in-class learning in form of so called blended learning, which means combination of traditional and online process.

With expansion of online learning, issue of quality is yielded. Having a huge amount of courses offered on market puts a reasonable doubt about whether its quality is acceptable for wide range of participants and tailors their individual needs. Although initiatives on quality assurance (QA) in e-learning are running for some years now, they are still restricted to some interested universities [1]. Also, as stated in ENQA report the eLearning quality is rarely included as a regular or integral part of national quality reviews, so the quality assurance of eLearning remains yet to be developed [2]. Therefore the whole matter of quality management is mostly left at the institution's behalf.

Moving a substantial or even complete learning/teaching process online means that many learning records, resources and personal information are saved electronically and accessible via Internet. That further implies the increased risk of jeopardizing data caused by unwanted exposure of private information, altering learning records and learning results or even stopping the whole system by cutting access to learning platform and tools. The concise list is given in [3].

Despite popularity of new learning forms, there is little importance devoted to data security in practice, such as remarked in [4]. However this topic is in variable extent included in popular quality assurance schemas that consider e-learning at infrastructure level.

On the other hand, users also recognize that elements of security tightly related to their performances in e-learning and have their own attitudes and requirements in this field.

In the following chapters first of all the preview of online learning security practice in Serbia is given. Then the student's attitudes towards security are presented and the QA schemas and their parts dealing with security are addressed. Finally, a model that utilizes all presented factors will be proposed as a proactive quality enhancement component.

2. CASE STUDY: SECURITY AND ONLINE LEARNING IN SERBIA

In order to get more information, two surveys were piloted.

The first survey considered usage of security mechanisms in e-learning platforms. All registered publicly available Moodle systems were checked in order to get basic information whether they use rudimentary mechanisms for protection.

Second was conducted among students using on-line component in blended learning form at the Faculty of Technical Sciences in Čačak. A short survey was companioned with an open question, in order to get additional feedback from users.

E-learning practice in Serbia: security features

Moodle stands as the most popular LMS, according to [5] On Moodle.org, the official Moodle web site, there is a country list of all registered Moodle installations [6]. There are a minor number of sites omitted from the list as their founders did not want to publish their address.

A small survey was made among available sites in Serbia in order to check whether the basic security mechanisms were implemented: usage of SSL, password policy, captcha usage and existence of site usage policy.

These measures are well supported within Moodle platform.

- SSL utilizes public encryption algorithm that prevents eavesdropping of information transferred between client and platform.
- Password policy means preventing users to form too simple password, which could be easily guessed. Default Moodle policy requires at least 8 character, with nonalphanumeric signs, numbers and minimal number of upper and lower case symbols.
- Captcha is used as way to prevent automatic filling of forms. In Moodle captcha is valuable if the self-registration is turned on.
- Site usage policy is set of information a new user should comply with in order to use the system. An important part of policy is security-related.

The survey was limited by its scope and validity, since there was no full access to platforms. However, some clear points could be drawn out of it.

After omitting sites at free domains and empty ones, 89 sites remained:

- Only three sites used SSL, but with self-made certificates, therefore not recognized by browsers and generally considered as not-trusted, since not provided by certified authority.

After removing sites without selfregistration, there was 52 sites left.

- Even 21 did not use any password policy.
- Only five sites used captcha anti-bot check, meening an automatic registration could be easily processed, further giving opportunity to spam with deliberate content.

Not a single installation has had site usage policy available.

Student Survey

Users' feedback is crucial for quality enhancement. The same stands for quality in e-learning, as stated in [7]. Survey was initiated in April 2012 at Faculty of technical sciences in Čačak and remains opened in order to continuously monitor users' opinions and standings. Its goal was to bring details about students' security culture and to get suggestions regarding security and the learning platform.

Likert scale was used for most items. Here follows highlights from summative results based on answers from 163 students. On item 1 "It is all right to tell a colleague own username and password" 23% answered "Agree" or "Fully Agree". 22% answered positively when asked if they would reveal their credentials to the teacher if asked to. Twenty percent did not agree that system should keep logs of all activities. Answers about their profile information disclosure model, ("Who is supposed to be able to see profile data?") are shown in Figure 1.

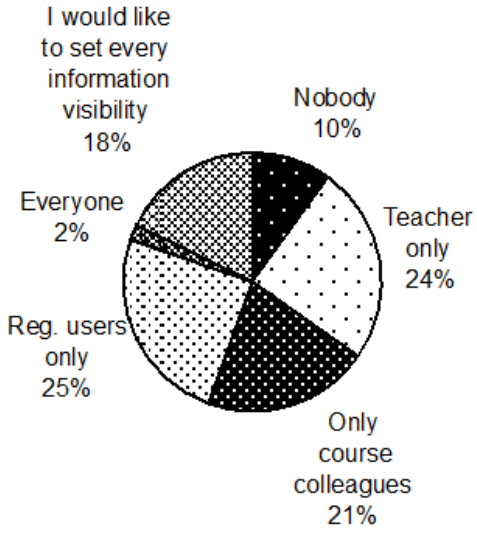

Figure 1: Students' preferences for profile information disclosure model

When asked about the password strength, 18% answered that they used only one strong password for all systems and 2% even said that same, weak password was used for all systems (sites, portals).

In response to statement "I need additional education in area of Internet security", students answered as follows:

- 12% - Fully disagree
- 23% - Disagree
- 26% - Do not have opinion
- 34% - Agree
- 4% - Fully agree.

There are also answers from open questions, which were not compulsory:

- "There should be a document about rules regarding protection of private data."
- "IP trace for every student should be set in order to log details about every access in case of an incident."
- "I think there is no sufficient information about risks brought by Internet. Rules are rarely applied even by advanced user who is aware of them."

Discussion

As previously mentioned, the survey among sites is not higly representative, but its general conclusions should not be neglected and a rough picture can be constructed. Even though all these sites are not formally included as official tools, that does not preclude need for security attention. That means there is a strong motive for improvement.

The given preview shows that even mechanisms fully supported in the LMS itself are often neglected, therefore raising the risk of jeopardizing data.

Presented results from student survey show that students are interested in security, but also that there is uncertainty about specific aspects and their own need to grasp them. Since the security is strongly affected by users and their awareness, it is implicated that students are supposed to be further informed about security and privacy features. It is matter of choice how it would be done: through formal trainings, by using informal guidelines through the very course and so on. Hence, there is an interest to include the user awareness and user feedback component in model that considers quality enhancement in area of security.

3. QUALITY ASSURANCE AND SECURITY IN E-LEARNING

The question of quality in e-learning triggered forming of many agencies specialized in this area. Moreover, different quality schemas were constructed in order to provide a systematic guideline for quality assessment.
Some of them act at institutional level, while there are also schemas applicable at course level, or even learning software in various formats (courseware).

Security is primary matter of infrastructure level, and therefore takes place in schemas that are wider and consider university level, embracing the technology and tools involved.

UNIQUe

UNIQUe is created by the EFQUEL foundation and stands as basis for the certification process at the institutional level. The UNIQUe criteria demand proof of continuous iterative innovation in all aspects of pedagogical design and course provision [8]. In addition, they have been designed to be complimentary to the European Standards and Guidelines for Quality Assurance in Higher Education, thus allowing for quality improvement in E-Learning harmonized with ongoing Bologna reforms.

The UNIQUe process is structured in six very distinct stages and offers a formalized approach in each step:

0 - Inquiry
1 - Application
2 - Eligibility
3 - Self-Assessment
4 - Peer Review
5 - Awarding Body
6 - Continuous Quality Improvement

UNIQUe's quality label can be articulated in three areas: resources, processes and context. Every category further contains criteria that divide in subcriteria. Every subcriteria is formulated as statement. It is then judged for its compliance. For the institution to qualify for the certificate, it ought to pass all subcriteria. The exact grading formula is given in Guidelines.

The matter of security is considered mostly by second area. Further, the appropriate statements are given.

Area 2 (Learning Resources), Criteria 4 (Technology and Equipment)

- 2.4.1. Staff and students have single sign-on access to various applications
- (i.e. using the same password to log into different applications)
- What is the level of integration between the university's various learning management, communications and administrative systems?

2.4.5. Strong, end-to-end encryption, is used to protect all personal data of users in the system.

- What technological measures are employed to protect confidential user data?
- What sort of access rules are applied to the data?
- Who is responsible for overall management of data?

2.4.7. Best practice procedures are implemented for backups. At very least these include mirroring, and asynchronous off-site backup

- Please describe your backup arrangements.
- What sort of procedures are in place for (a) continuity of service, (b) disaster recovery?

Obviously, the UNIQUe takes in count only the most crucial criteria regarding security. The whole schema tends to define essence, criteria most important, thus reducing details of every element in order to maintain its compact structure and keep it manageable.

eMM – E-learning Maturity Model

The eMM started on foundations of Capability Maturity Model and SPICE (Software Process Improvement and Capability dEtermination) methodologies. It comprises of a very complex set of criteria, which should be tailored to a specific application by choosing the most proper statements.

The eMM model recognizes five main categories, also called process areas [9]. These are shown in Table 1. In eMM institution's capability to provide e-learning is evaluated through five dimensions: Delivery, Planning, Definition, Management and Optimization and every process is converted to practices. These practices are

evaluated on 4-degree scale from "not adequate" to "fully adequate".

Practices/statements dealing with security are given as follows:

Category L4/Dimension Planning:

- Institutional policies define requirements for protecting the privacy of digital information.

Table 1 – eMM process areas

Process category	Brief description
Learning	Processes that directly impact on pedagogical aspects of e-learning
Development	Processes surrounding the creation and maintenance of e-learning resources
Support	Processes surrounding the oversight and management of e-learning
Evaluation	Processes including quality evaluation and control of the e-learning quality through whole
Organization	Processes associated with institutional planning and management

Category D5/Dimension Delivery:

- All user digital information is stored in a validated backup system.

Category D5/ Dimension Planning:

- All elements of the e-learning infrastructure are regularly audited to ensure the validity of backups and disaster recovery procedures.

Category S6/Dimension Planning:

- Access to all student digital information is authenticated and authorized.

Dimension Definition:

- Teaching staff are provided with resources (including training, guidelines and examples) on supporting the use of digital information by students, including intellectual property, plagiarism and assessment aspects.

Category Optimization O4/Dimension Planning:

- E–learning design and (re)development procedures address the integrity and validity of digital information.

Category Optimization O4/Dimension Management:

- Feedback collected regularly from staff regarding problems with student use of technology and media that are not addressed in the provided course descriptions.

The eMM model gives a comprehensive set of criteria. However, these are not mandatory and there is no prescribed set that should be aligned with in order to get some certificate. Therefore, it is up to the institution to select criteria and form a sub model that suits its specific needs. The same recommendation stands for criteria dealing with security.

4. SeLMa - MODEL OF SECURITY IN E-LEARNING TOWARDS THE QUALITY ASSURANCE

Minding the aforementioned elements: quality schemes, users' attitudes and elements of security practice in Serbia; a global model of security in e-learning related to quality assurance may be generated. Its role would be to help in leveraging the elements of security in order to assure the quality of e-learning in general.

Parts of quality assurance schemas and accompanied statements may be used as guidelines for improvements, even if no formal quality assurance process is up to be conducted. It is preferable to include adequate parts into official institution regulative (rule set, recommendations) in order to systematically and officially take care of an emerging education component that online learning presents.

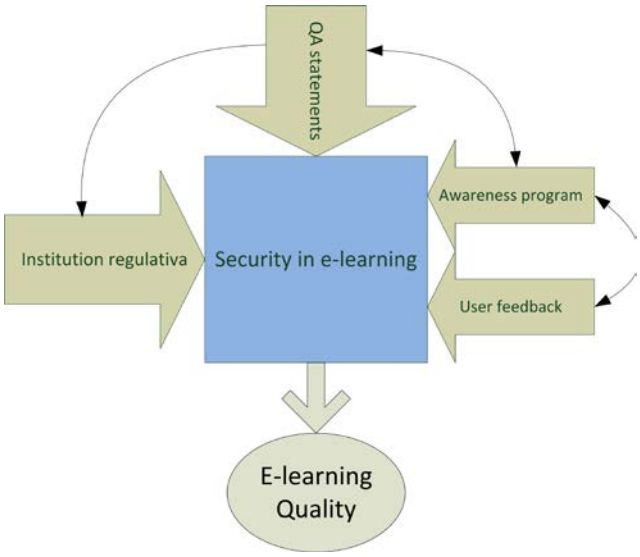

Figure 2: SeLMa model for quality enhancement

Already formed quality criteria regarding security aspects is virtually ready to be applied as guideline with certain accommodations. Security awareness program is included as additional component in order to process the "other side" part of security medal, by leveraging the security culture. Also, there is a user feedback component that is vital in order to keep the quality/security circle by constant improvement.

All elements interact directly or using each other as a proxy.

5. CONCLUSION

Quality in e-learning is a complex matter of various factors. Security is recognized as one of them. Establishing quality in formal view means meeting certain

criteria. As there are many QA approaches, it is up to institution to merge them and make a customized set of criteria, applicable to certain institution. However, meeting the "checklist" is, although a way of assuring quality, not the only way the quality is maintained. It came out that users, as key elements in security, have certain attitudes that yield the need for extension of matter of quality to include them.

All elements placed produce a complete picture of what security means to e-learning and what way it should be treated in future. It is up to the institution to further develop needed mechanisms, guided with given model and its specific elements, to integrate it into their quality control system and align it with current practice.

LITERATURE

[1] Marjan Milošević, Suzana Loškovska, Danijela Milošević: *Towards Quality in E-Learning Quality Assurance – epprobate International Courseware Label*, The Third International Conference on e-Learning - eLearning-2012., Belgrade, September 27-28.2012. ISBN 978-86-912685-7-2 , pp 9-14

[2] Josep Grifoll, Esther Huertas, Anna Prades, Sebastián Rodríguez, Yuri Rubin, Fred Mulder, Ebba Ossiannilsson, Quality Assurance of E-learning, ENQA, workshop report, Helsinki, Finland, 2010. http://www.enqa.eu/files/ENQA_wr_14.pdf

[3] Zuev V. I., "E-Learning Security Models," *Management*, vol. 7, no. 2, pp. 024–028, 2012.

[4] Graf F.: *Providing security for eLearning*, Computers & Graphics 26 (2002) pp 355–365, Elsevier

[5] The Top 20 Most Popular LMS Software Solutions powered by Capterra http://www.capterra.com/infographics/top-lms-software (visited on 20. Avgust 2013.)

[6] Moodle.org: Registrated Sites, https://moodle.org/sites/index.php?country=RS (visited on 20. Avgust 2013.)

[7] M. Jara and H. Mellar, *Quality enhancement for e-learning courses: The role of student feedback*, *Comput. Educ.*, vol. 54, no. 3, pp. 709–714, Apr. 2010.

[8] UNIQUe Information Package, http://cdn.efquel.org/wpcontent/blogs.dir/5/files/2012/09/UNIQUe_guidelines_2011.pdf (visited on 20. Avgust 2013.)

[9] E-Learning Maturity Model Publications, http://www.utdc.vuw.ac.nz/research/emm/Publications.shtml (visited on 24. Avgust 2013.)