Evaluation of IT System Security Training Success

Goran Božić[1], {Miroslav Bača, Markus Schatten}[2]

ABSTRACT

With all the efforts put into IT system security, the issue remains of what the level of such security is and how sure we are that our IT system is secure. The paper starts with the assumption that users are one of the most important components of IT system security, and an aware and trained user takes much more care about security in his daily activities. Such system will have less security incidents, which should reduce the possibility of infiltration by malevolent users or programs. Training is one of the mechanisms for affecting user behavior. The management of user training in the area of security is a demanding process. To implement is efficiently, we need information on training success evaluation. The paper proposes a training success evaluation model using fuzzy logic.

Key Words*: IS Security, management training, fuzzy logic*

1 INTRODUCTION

IT security has become an important issue around the world because a need for it has arisen at all levels – personal, corporate and government (Adams A. et al., 2005). It is important not to allow compromising of confidentiality, integrity and availability of information in any way (Aljifri H, et al., 2003; Buzzard K. 1999). IT system (hereinafter referred to as IS) security management means proactive management of IS risks, threats and vulnerabilities (Lewis A. 2000). To achieve this, individuals and organizations must comply with certain guidelines and frameworks. If IS security consists of people, processes and technology, it is certain that security depends upon human behavior, although the desired level of IS security would be impossible to achieve without contribution of the others. One of the ways to affect human behavior is training, and its better success requires that it be adapted to the environment (Rezgui Y, et al., 2008). Training without information on the effects reflected in user behavior is something that should be avoided if we want to ensure IS security. The model proposed in this paper evaluates the effects of completed training on the basis of quantified magnitudes of selected system security components. The decision-making mechanism is flexible in the way that the rules governing the evaluation incorporate knowledge of the experts working on the system concerned, as well as the security policy requirements for the components observed. As a result of training, user behavior indicates the program and trainer quality i.e. the actual result of training. Success evaluations may be acceptable after training, but what is important is how these users will behave after 3, 6 or 12 months. Training management is carried out for both security reasons and for financial effects to avoid frequent and inefficient trainings.

The paper is organized as follows: In addition to the need for IS security training, it is important to distinguish between areas appropriate to the respective users groups. One such

[1] *Franck d.d. Vodovodna 20, Zagreb, Croatia, corresponding author, goran.bozic@franck.hr*

[2] *Fakultet organizacije i informatike, Pavlinska 2, Varaždin, Croatia,{miroslav.baca;markus.schatten}@foi.hr*

division is provided in Chapter 2. Chapter 3 selects the security components to be quantified with determination of the areas of responsibility for the respective user groups. Chapter 4 shows how to quantify the selected security components and what values were obtained in the analyzed case. Chapter 5 processes the results obtained by using fuzzy logic to evaluate training success. Chapter 6 states the reasons why training improvement is insisted on to achieve higher IS security. At the end, a conclusion on the proposed model is provided

2 TRAINING

The idea of importance of training is based on the assumption of individual responsibility. The individual responsibility of an employee in terms of security should not be restricted to individuals' actions, but should also cover actions in the broader area of the system. Creating a climate where IT system security is paid enough attention will affect the training results. Obstacles in the implementation are normally a result of a lack of knowledge and information, a long-term process of changing attitudes and habits, a lack of interest or motivation, and underestimating of an individual's impact on the entire system. Introduction of such training in regular education reduces the vulnerability of the entire corporate IT system, increases the number of IT system experts, and helps organizations implement their security policies (Victor MW, et al., 2001). With the trend of introducing such course in higher and high education, a certain level of previously acquired knowledge of security issues may be expected of new employees in an organization.

If we contemplate the areas where a training process should be included, we should take into account that IS security has exceeded its technical component or area. For a secure IS environment, we must take into account the non-technical areas as well. The division between the technical and non-technical areas is important for two reasons: it is easier to determine the areas of interest for the respective system user groups and importance is given to the non-technical component (Kritzinger E., et al., 2008). The possible division between the technical and non-technical components is presented in Table 1.

Table 1. Technical and non-technical components (source: (Kritzinger E., et al.,. 2008)).

Technical Components	Non-Technical components
Access Control	Information Security Culture
Password Protection	Password Protection
Firewalls	Security Policies
Intrusion detection	Legal aspects
Encryption	Ethics
Measurement	Certification
Monitoring	Awareness

Some areas may overlap, such as the password policy that has its technical component and its non-technical user component where the user chooses password strength according to certain criteria. As not all people have the same level of knowledge of the IS security issue or the same degree of responsibility and influence within an organization, this problem should be approached systematically, that is, we should be aware of the different levels of needs. Efficient training should not be unilateral because it should change the general view of and approach to this problem, in addition to informing. Middle and senior management are responsible for creating a positive climate with respect to IS security in an organization. By proper training, the awareness of the problem may be raised and support may be gained in the implementation of the activities

Organizations are becoming aware that large investments in technical solutions will not achieve the desired level of security and neither will training in technical areas only. To achieve the desired IS security level, the training process should include areas within the non-technical component. The training models proposed in this paper are:

- Theoretical (T) (e.g. algorithms used for encryption)
- Informative (I) (e.g. reviews of legal regulations, ethical issued, behavior on the system)
- Practical (P) (e.g. a workshop teaching how to use strong password creation tools, restrictions defined in security policies)

Each of these methods may be adapted to the beginner level (for new users who have just been hired) and the advanced level (for old users undergoing retraining). All of the foregoing, the different user groups, different IT security levels and training models are presented in Table 2. It is important for training to be efficient and for its effects to be measureable. The measurement results would justify the invested funds and could indicate potential flaws.

Table 2. Training models by area and user group (source: own)

			Domain				
			Technical			Non-Technical	
			I	T	P	I	P
Levels	Users	New	√		√	√	√
		Old			√		√
	Systems staff			√	√		√
	Management		√			√	

This is important because IS security also depends on user behavior. The model evaluating training quality may also be used to evaluate other system users. The parameters governing the evaluation should connect training and security. This means that certain significance is given to them through training, that they have impact on IS security and that they may be quantified.

3 SELECTION OF COMPONENTS

IS security depends on many components (Jaquith A. 2007) so it is easy to determine the one that can provide quality relevant information. A number of authors contemplate IT system security measurements in their papers (PSM 2006; Wang C., et al.,. 1997, Alhazmi, YK., et al., 2007) and propose a series of measures by which an IS can be made secure. The measurement itself is defined as a result of a process of collecting data, analysis and reporting for the purpose of easier decision-making. Decision-making may be based on statistical methods or experience and opinion. One direction in IS security measurement is based on collecting and analyzing data generated on all levels the information goes through (Jaquith A. 2007). The other direction, or reason for IS security measurement is to monitor the progress of IT security program implementation, specific security checks, and the related policies and procedures. There are several levels associated with this area: ISO standard (ISO / IEC27004), Security Metrics Guide for Information Technology Systems

(NIST 2008), A Guide to Security Metrics (SANS 2006). The activities referred to here that may provide data for measurement are risk assessment, penetration testing, security assessment and constant monitoring. Other activities, such as training efficiency and awareness program, may also be used as a source of measurement data.

Neither of them indicates a method that would relatively easily, quickly and with certain assurance provide an answer about the results after the training and directly indicate the condition of the IS with respect to security. This is why we need to decide how to perform the measurement or, to simplify it, which question we want answered (Jaquith A. 2007). These include:

- How many employees are aware of their responsibilities as IT system users?
- How many employees have undergone periodic training and been made aware of the corporate security policy?
- Is the system staff in possession of the knowledge and skills required for the establishment, implementation and monitoring of the security policy?
- Have the efforts put into training provided a measurable result?

Through these questions, particularly the last one, we attempt to find the answer as to whether there is a causal relationship between training and security and how to measure it. The components that have been identified as measurable and that could form a basis for decision-making are:

- Software upgrades
- Computer antivirus program upgrades
- Password quality.

In addition, it is important to determine user groups' responsibilities and their impact on the selected components. The responsibility for software upgrades (hereinafter referred to as patches) may be distributed among the system staff and users. The system staff should deliver the patches to the user's computer and the user should implement them, provided this does not threaten the business process he is responsible for. The responsibility for the updating of the antivirus program lies with the system staff. The users are deemed responsible for password quality. Their treatment of the said components is a result of training and awareness. Figure 1 presents the model for responsibility distribution by area, providing the necessary information for the decision on the effects of training.

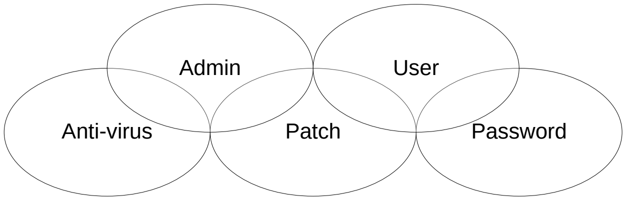

Figure 1. An area of responsibility users IS (source: own)

Such distribution aims to show that all IS users have impact on the selected components relevant to IS security. The responsibility distribution was simplified for the purposes of the paper.

4 QUANTIFICATION OF THE SELECTED COMPONENTS

An important prerequisite for measurements is the possibility of quantification of a selected component. Applications managing such components or other methods such as surveys, including information on password quality through questionnaires, may be used as a source of information used for collection of data necessary for quantification (NIST 2008).

4.1 Password Quantification

Many papers (Bishop, M., 1991; Bishop, M., 1992a; Bishop, M., 1992b; Bishop, M., 1995) provide analyses showing us how to use a password properly, as well as mechanisms for quantification of the password strength. Password strength may also by checked by using the so-called cracker programs that are able to provide information on the password by using different methods. Examples of such programs[3] are *L0phtCrack*, *John the Ripper*, *Cain and Abel*, and we can also use techniques proposed for elimination of the use of weak passwords (Blundo C., et al., 2004). By using one of the above programs, we can obtain information on the number of strong or weak passwords and how many of them are not in compliance with the requirements laid down in the security policy. The status may be analyzed according to an agreed scenario, within defined periods of time on a defined sample. The effect of efficient training should be reflected in a small number of weak passwords. For the purposes of the paper, we analyzed a system where the password is changed on a monthly basis. The minimum number of password characters is 6 and no special symbols need to be used. After the training, ~36% of the users used the recommendations received in training. ~30% used the recommendations about the password length, but they used specific words they warned about in training. In case where the training results have two statuses, this user group is classified in the group of those who did not use the recommendations received in training.

4.2 Patch Quantification

The second component that may provide a basis for conclusion as to the effects of training is patches. Timely installation of patches is one of the basic requirements for a secure and reliable IS (Post G., et al., 2003).. An increasing number of security faults in operating systems and program packages poses a serious threat to IS security. One of the ways is to automate the computer inspection process and patch implementation. To obtain information on patches and their number, we can use the 'Ecora Patch Manager's Reporting Centre' program[4]. The report received should be tailored for the purpose of obtaining information of interest in this case (Jaquith A. 2007). These are primarily patches that are not installed (on the average per computer), their importance and the time frame for their implementation i.e. the expected time of implementation, Figure 2. Such times may be changed depending on the type of IS and security requirements. The average time for a patch group may be a value after which the decrease of the number of patches in a group should be measured. Any deviation from the mean value should be interpreted as noncompliance with the prescribed security policies and may also be interpreted as a result of poor training. Such information may be used to define the patch security policy (FIRST 2007).

[3] *http://sectools.org/crackers.html*

[4] *http://www.ecora.com/ecora/products/patchmanager.asp*

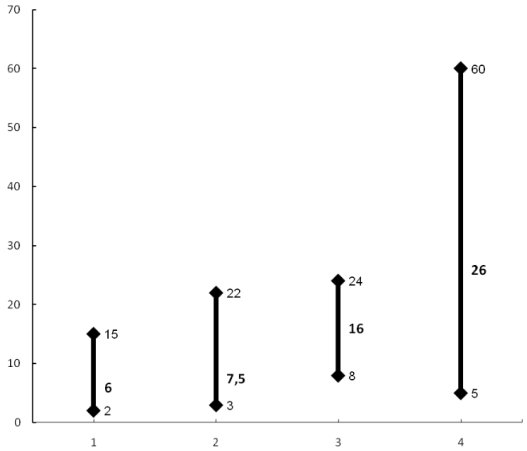

Figure 2. A presentation of the dependence of patches on the time for the implementation of the respective patches (source: own)

Software upgrades are provided to the user in the analyzed system, and the user implements them when it least bothers him. Figure 3 shows upgrades according to criticalness and the time for implementation expected of the user. For the purposes of the paper, the time of status survey was the same as that for the passwords i.e. one month. In such conditions, ~60% of the users implemented 90% of the upgrades. Half of them failed to comply with the security policy requirements of implementing upgrades 1 and 2 (Figure 3) within a week.

4.3 QUANTIFICATION OF ANTIVIRUS PROGRAM UPGRADE

The third component providing a conclusion as to the effects of training is the antivirus program upgrades. To obtain information required for the quantification of this component, we used the reporting part of the same application managing and monitoring this process. The system staff is responsible for the updating of this process’s functioning. The user may also see if his program has the latest upgrades, but the entire responsibility was assigned to the system staff alone for the purposes of this paper. Figure 3 presents a report indicating the number of updated clients. The first group (1 in Figure 3) contains the users whose upgrades are within the prescribed security policy. The second group (2 in Figure 3) contains users who failed to implement the upgrades for justified reasons (business trip, vacation, sick leave, etc.). The last group (3 in Figure 3) contains the users who failed

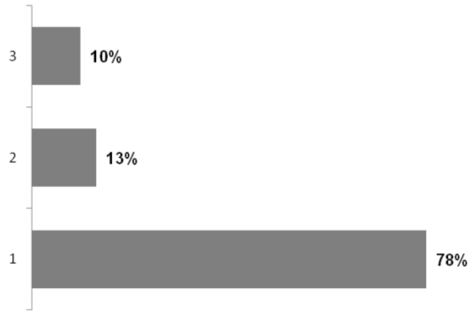

Figure 3. Information on antivirus program upgrade (own source)

to upgrade (3 in Figure 3) contains the users who failed to upgrade their antivirus program base within the observed period for some reason, and this is considered to be an omission of the system staff.

The model to evaluate training success must be able to be adapted to different requirements arising from different ISs. In addition, it must be able to be changed and upgraded over time as IS priorities change. If there are no security policies in place well defining the acceptable values of the respective components, the option of incorporating expert knowledge acquired by work on the system must be provided, which would be a guarantee that the decisions made reflect the IS requirements. Requirements so defined may be met by using a fuzzy logic model.

5 THE USE OF A FUZZY LOGIC SYSTEM TO EVALUATE TRAINING SUCCESS

The theory of fuzzy logic is part of a broader theory of fuzzy sets (Zadeh LA. 1965). It extends the standard logic onto a perpetual area of values within a segment [0, 1]. This enables definition of transitional values, which is essential for description of natural systems. In fuzzy sets, an element may be partially within a set, and this is determined by the membership function. The membership function uses values from intervals [0, 1], while only values {0, 1} are used for standard sets.

If $X = \{x_1, x_2, ..x_n,\}$ is a set of x elements, we can define fuzzy set A and its membership function μ_A as:

$$A \subseteq X$$

$$A = \left\{\frac{\mu_A(x_i)}{x_i}\right\}$$

$$\mu : X \rightarrow [0,1]$$

Fuzzy set A is a subset of set X, the elements of which are contained in A only to a certain degree. Membership function μ_A (1) mirrors set X to the segment [0, 1] and shows how much element x from set X is contained in set A.

When we want to describe a complex system with as exact relations as possible, we encounter increasingly complex mathematical problems requiring an increasing number of parameters and more complex numeric solution methods (Sowell TE. 2008). The fuzzy approach rationally approximates system description based on the model of how person (process expert) solves a management task. Fuzzy conclusion is based on fuzzy logic and imitates human conclusion with approximate information and uncertainty in conclusion.

Fuzzy rules associate premises with the conclusion, and conditions with actions. The algorithm governing the decision is in accordance with experience where the decision has a general form: IF (*the system status is like this)* THEN (*we need to do this)*. The fuzzy logic system is defined by or composed of three basic components (Kasabov NK. 1998).

The membership function shows how much a value is included in a fuzzy term. The transformation of input variables from crisp into fuzzy will be carried out by using the relevant membership functions. Membership functions may be provided in mathematical and tabular forms. A set domain is normally segmented by approximating the membership function value by fixed or linear approximation according to the borderline values. Division by domain should not be too great. Training success evaluation may generally be described by using a fuzzy logic system having binary values obtained by quantification of the observed components as the input, and the value representing training success evaluation as the output. To determine the number of elements in a fuzzy set, assigned to a linguistic variable, we will use the parameters provided in Table 3. These values are not strictly defined in security policies, but a result of experience. In the system analyzed, these values are considered to be acceptable and they have the same division by value for the purposes of the paper.

Table 3. Values of variables (source: own)

	Very Bad	Bad	Medium	Good	Very good
Password	~ 20%	~ 50%	~ 70%	~ 80%	~ 95%
Patch OS	~ 20%	~ 40%	~ 60%	~ 70%	~ 80%
Patch AV	~ 20%	~ 40%	~ 50%	~ 65%	~ 75%
Education	~ 35%	~ 50%	~ 60%	~ 70%	~ 85%

Based on the above-defined borderline values, a linguistic value is introduced for each input variable, describing the amounts of such variable through the following attributes;
{very bad, bad, medium, good, very good}.

A fuzzy expert system makes decisions on the basis of fuzzy logic and represents a set of membership functions and conclusion rules. An advantage of this system is that it makes its conclusion by computing rather than symbolic conclusion. A set of rules is called a knowledge base or rule base. When the conditions of a rule are met, the rule is executed and the value of conclusion for that rule is computed. The rule is applied when the value exceeds the defined value defining system sensitivity. A fuzzy rule base is a place where expert knowledge is incorporated. The secret to the success of fuzzy systems is that they are easy to implement, maintain, and are comprehensible. We should also be aware of the flaws of this method where some rules do not have to affect the inference (in the final inference, the results of different rules are concealed). If we apply MIN inference to individual rules, the impact on some input values on the final conclusion may be insignificant.

To process the input variable values representing quantified security component values, we used the mathematical tool *Matlab*[5], with an addition of fuzzy logic.

For input variable values obtained by measurement (Chapters 4.1, 4.2 and 4.3); Password= 36%, Patch OS= 60% and Patch AV = 90%

The percentage of the training success evaluation is 22.8%. The values provided in Table 3 indicate that the training results are 'very bad'.

The training success evaluation was made on the basis of the prescribed security policies and experience. Definition of the limits of acceptability for a component through security policies is something that should be done to avoid a 'liberal' evaluation. One could not conclude the training results were so bad on the basis of the input value data. This method ensures training success evaluation based on the prescribed security policies with expert knowledge of the people who worked on the system.

The result obtained is important for user training management because it indicates the application of acquired knowledge. User behavior after a period of time is also important for training management, in addition to the training success evaluation. If we could foresee user behavior, it would help schedule new training.

[5] *http://www.mathworks.com/products/matlab/*

6 DISCUSSION

The training success evaluations obtained indicate that, in a system with no strict rules, the results are not encouraging. Based on the knowledge incorporated in the decision-making model, the result was surprisingly low. A user behavior evaluation for a longer period of time shows what can be expected. This problem can be solved in two ways:

1. Introduce tools that will force the user to use 'strong' passwords. Patches would be implemented automatically, regardless of user's present activities.
2. Change the training concept by approaching a problem in the way to make the results better.

In the observed system, we started with the presumption that user training and awareness were an important component of the modern IS concept. This is why training will not be given up on.

7 CONCLUSION

Today, user training in the area of security is considered to be a mandatory task, rather than a necessity. Management of such training is required for optimal utilization of resources. This primarily refers to employee time and fees paid to the trainer. To implement this process as efficiently as possible, we need information that will help choose a program and trainer, and to define the training schedule. The paper offers a model providing information on training success evaluation. The evaluation is based on the knowledge of the experts monitoring and working on the system, and the security policies defining the values acceptable to the system. The information obtained indicates the training program, trainer and trained users' quality. What needs to be done is to incorporate a function foreseeing user behavior over the desired period of time in the model.

REFERENCES

Aljifri H, Navarro DS. 2003. *International legal aspects of cryptography. Computers & Security*; 22(3):196–203

Lewis A. 2000. *Time to elevate IT security to the boardroom. e Secure*,1(1):28.

Kritzinger E., Smith E. 2008. *Information security management: An information security retrieval and awareness model for industry*, Computers & Security, Volume 27, Issues 5-6, October, Pages 224-231

Adams A, Blandford A. 2005. *Bridging the gap between organizational and user perspectives of security in the clinical domain.* International Journal of Human-Computer Studies; 63(1/2): 175–202.

Victor MW, Corey DS, Daniel R, Don W. 2001. *A model for information assurance: an integrated approach. In*: Proceedings of the 2001 IEEE workshop on information assurance and security. West Point, NY: United States Military Academy

Buzzard K. 1999. *Computer security — What should you spend your money on?* Computers & Security, Volume 18, Issue 4, Pages 322-334

NIST 2008. *Performance Measurement Guide for Information Security*. SP 800-55 Rev 1. http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf *(accessed 20-03-2010).*

SANS 2006. *A Guide to Security Metrics*, http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55 *(accessed 10-02-2010).*

PSM 2006, *Security Measurement*, http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf *(accessed 10-01-2010).*

Wang C. Wulf W.A. 1997, *Towards a framework for security measurement*, Department of Computer Science University of Virginia**,** http://csrc.nist.gov/nissc/1997/proceedings/522.pdf *(accessed 18-01-2010).*

Jaquith A. 2007. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley Professional; 1 edition (April 5,)

Alhazmi, YK. Malaiya, RI. 2007. *Measuring, analyzing and predicting security vulnerabilities in software systems*, Computers & **Security**, Volume 26, Issue 3, May, Pages 219-228

Bishop, M., 1991. *Password management.* In: Proceedings of COMPCON 1991, pp. 167–169.

Bishop, M., 1992a. *Anatomy of a proactive password checker*. In: Proceedings of the Third UNIX Security Symposium, pp. 130–139

Bishop, M., 1992b. *Proactive password checking*. In: Proceedings of the Fourth Workshop on Computer Security Incident Handling, pp. W11:1–9.

Bishop, M., 1995. *Improving system security via proactive password checking*. Computers and Security 14 (3), 233–249.

Blundo C., D'Arco P, De Santis A., Galdi C. 2004. *HYPPOCRATES: a new proactive password checker,* Journal of Systems and Software, Volume 71, Issues 1-2, April, Pages 163-175

Post G., Kagan A. 2003. *Computer security and operating system updates*, Information and Software Technology, Volume 45, Issue 8, 1 June, Pages 461-467

FIRST 2007. *Example of CVSS based Patching Policy*, http://www.first.org/cvss/cvss-based-patch-policy.pdf *(accessed 19-01-2010).*

Sowell TE. 2008. *Fuzzy Logic for "Just Plain Folks* (Online Tutorial), http://www.fuzzy-logic.com/ *(accessed 09-01-2010).*

Zadeh LA. 1965. "*Fuzzy Sets"*, Information and Control, Vol. 8.

Kasabov NK. 1998. "*Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering*", The MIT Press, Vol. 2,. MathWorks, MATLAB$^{®}$
http://www.mathworks.com *(accessed 08-01-2010).*

Rezgui Y., Marks A. 2008. *Information security awareness in higher education: An exploratory study* Computers & Security, Volume 27, Issues 7-8, December, Pages 241-253