THE LEGEND OF INFORMATION SECURITY

Zoltán Som[1] and Tamás Szádeczky[2]

Abstract
Act 50 of 2013 has served as a new and large scale impetus for both public bodies and local governments regarding information security in Hungary. This naturally means an increased need for professionals on the field. The National University of Public Services has become an institution that may very well be capable of training the required number of professionals. The aforementioned act has been amended by an implementing regulation (no. 41/2015) and as a result the system as a whole has changed regarding information security.[3] This paper aims to highlight any problems that shall be addressed and solved as quickly and swiftly as possible. Basic skills and areas that shall be improved will also be in focus as well as processes that are vital in order to realize the actual situation of information security. Without the possibility to continuously determine the actual situation and without the means to assess such situation, the probability of deterring from the right path increases. Further challenges that this area has to face actually originate from situation assessment and the determination of the "correct" path. The theoretical model (to be presented), developed during the previous years, provides quick and swift possibilities to intervene in such areas if need be. The model guarantees a way to give feedback and is able to set up a communication channel that may be used to support the whole structure on the long run in a cost efficient manner. It is capable to provide feedback from numerous areas of the system while maintaining its structure and applying clarity or additional precision where necessary. Its real advantage is that the whole system (of institutions and/or public bodies) may use it as a single institution or body would not be able to realize or develop the model in its entirety.

Key words*: information security, CISO education, information security measurement, password awareness survey.*

1. The Basis of Information Security

Information security is no other then the loose essence of knowledge in the heads of people, principles, corporate regulations, legal regulations, social and ethical norms and the network that connects such knowledge. This results in the fact that if such knowledge can be kept in sync then regulating the sharing and safety of such knowledge can also be synchronized. Such synchronized state and its continued growth may realize fundamental structural stability. Since the key is that the main area that determines information security is the knowledge that people already possess or that they will possess due to training and development, the current model in which a single person is responsible for the security of the electronic information system (namely the Information Security Officer, to be referred to as "ISO") is obsolete, especially since the law only requires such ISO to attend related training only once a year. Such models shall be reworked and improved. During the

[1] National University of Public Service, Faculty of Political Sciences and Public Administration, Institute of E-Government, Budapest, Ménesi str. 5, som.zoltan.kdi@office.uni-nke.hu
[2] National University of Public Service, Faculty of Political Sciences and Public Administration, Institute of E-Government, Budapest, Ménesi str. 5, Szadeczky.tamas@uni-nke.hu
[3] Numbers of new degrees and regulations: No. 187 of 2015 (13. July), No. 185 of 2015 (13 of July), No. 41 of 2015 (15 of July), No. 42 of 2015 (15 of July). Some of the older regulations have been repealed. These include: No. 233 of 2013 (30 of June), No. 301 of 2013 (29 of July), No.77 of 2013 (19 of December), No. 73 of 2013 (4 of July)

research (conducted by the author, backing up this paper with its findings) information regarding the knowledge of passwords and their use was used as indicators in order to prove how much the level of consciousness towards information security can influence fundamental structural stability. The research was conducted via a questionnaire.[4] The results (in part) can be seen in the following sections.

2. Measuring the Immeasurable

Currently, in most cases the model where the level of information security regarding (an employee, or more commonly) an organizational structure is determined by a scale of five or other means that considers characterizable or typeable actions, activities or features, is considered acceptable.[5]

According to experts, the role of passwords during an authentication process is gradually going to change but they will likely be used in some form or other throughout the next decades. The expression to have a "good password" is inaccurate. Whether the password is good or not cannot be determined solely by how long or complex it is. It is also affected by numerous factors and circumstances regarding its use.[6,7] One should not say that a password is good in itself solely because it is long, complex, etc. as it may be endowed with a 100 different features. A suitable strategy or correctly regulated environment can be more effective regarding possible abuses.[8,] The attitude towards handling ones password can however correctly characterize the situation of information security.

3. Password Usage as an Indicator

Characteristics of password use is a possible indicator of information security.[9] The level of information security awareness and the general approach to this question is mostly determined by the organizational culture and in many cases it appears as a result of peer pressure within a group. (This conclusion is also backed up by the personal observations of the author, who is a lecturer of the EU Safer Internet Program and has coordinated relating activities and gave lectures by the hundreds.) Peer pressure can be just as effective in 4th grade in an elementary school[10] as it can be within an organization. Professional literature also differentiates between good and bad types of such pressure.[11]

---

[4] Fundamental Stability can be understood in at least two different ways: a) every singly employee within the organizational structure is trained equally or on a high level; b) the information security component is present in each and every work process within the organization.

[5] Brotby, W. Krag, and Gary Hinson. Pragmatic Security Metrics: Applying Metametrics to Information Security. Auerbach Publications., 2013.

[6] Jelszóhasználati trendek és az ügyfélbizalom értéke. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban, [in Hungarian] (Trends Regarding Password Usage and the Value of Customer Trust. Password, trust and e-acceptance in modern days II.), Papp, Gergely Zoltán – Som, Zoltán

[7] Mark Burnett: Perfect Passwords: Selection, Protection, Authentication

[8] This means that in a separate office or room even a password of five characters can be considered good if for example there are only two chances to provide it incorrectly, and upon the third failed attempt an alarm mechanism is triggered where setting back the system to default would be complicated.

[9] Herold, Rebecca. Managing an Information Security and Privacy Awareness and Training Program, Second Edition. Auerbach Publications. 2011.

[10] Based on the observations of the author in Hungarian elementary schools, regarding digital and smart devices and applications.

[11] William M Bukowski, Brett Paul Laursen, Kenneth H Rubin, Handbook of peer interactions, relationships, and groups, 2011

The relation of people towards their passwords also reflects the level of information security awareness. This is also a general characteristic of the given organization. The next examples are to serve as reason behind the above statements. Let there be a "Company A", where it is acceptable to write the passwords down and store it on a post-it ("sticky note") or in a notebook, etc. Let there be a "Company B" where it is common practice that should an employee take a leave (go on vacation or fall ill, etc.), he/she gives his/her password(s) to his/her co-workers so that they can access his/her computer, mails, etc. in his/her absence. (Please note that it is also possible that such co-workers may already be aware of such passwords as they might have been written down somewhere.) How do all of these support above statements?

- peer pressure is clearly present as everyone is doing it this way, it is accepted, even if the regulations would forbid such practice,

- it is a part of organizational culture as neither the employee(s), nor the management has developed or adopted a solution for this situation.

As a result, the attitude and care towards password usage will affect the accessibility of the information and will also have an effect on information security. This is due to the fact that one of the most fundamental principles is being ignored as it can no longer be guaranteed that the unique identifiers are only used by a single person. Throughout the interviews it became clear that the daily routine can influence the attitude and behaviour of employees regarding data access and information processing.

4. Presenting the Research

The period of data collection was between December 2014 and July 2015. Preliminary work lasted for about six months, through which previously acquired research experiences[12] were reviewed and the questions of the questionnaire have also been reviewed based on methodological, demographical and professional aspects. 58 unique links were prepared and these were made public for different groups. 1,243 people answered the questionnaires, most of which were young employees and university students. The questions can be arranged in the following blocks:

- 8 demographical questions (Question Group 1)

- 52 questions regarding passwords (Question Group 2)

- 12 questions relating to IT, ICT skills (Question Group 3)

Due to the high number of expected participants the questions were mostly multiple choice questions in order to make it possible to be processed electronically.

The research in its entirety will only be made public in the future. The most important findings can be found below.

[12] Illéssy, Miklós – Nemeslaki, András – Som, Zoltán, Elektronikus információbiztonságtudatosság a magyar közigazgatásban [in Hungarian] (Electronic Information Security Awareness in Hungarian Public Administration)

Question 2.1: How many different passwords do you use?

- 7% answered that he/she uses only one,
- 50% answered that they use a maximum of five,
- 6.4% answered that they use more than 50.[13]

According to the recommendation[14], it is advised to use a separate (unique) password for every single IT system. This would mean that should any of the passwords be compromised, no additional access would be in danger.[15]

Questions 2.2, 2.3 and 2.10: Do you have any passwords that contain a person's name? Do you have any passwords that contain a word with a meaning either in Hungarian or any in other language? Are there any words, names or expressions that are used in multiple passwords that you use?

The provided answers correspond to the previous data gathered from Hungary.[16]

- more than 1/3 answered that they use a person's name in their passwords,
- more than 2/3 answered that they use words with meanings in their passwords,
- 2/3 answered that they would use the same words for multiple passwords.
- Among those who use the rules of password creation, 1/2 use it in order to make it easier to remember where as 2/3 use it as a security measure.

Numerous researches were conducted focusing on this issue during the past years, which in most cases examined a form of algorithmic pattern in passwords and they also placed focus on predictability in possession of previous passwords upon a password change. A common mistake worth mentioning regarding these researches is that they examined the passwords "taken out of context", meaning no other factors were taken into consideration. It is an especially big problem if the new password only differs from the previous one by a few characters or if the new password "resembles" the old one after a password change.[17]

The solution is to provide an effectively supportive environment (education, training, regulation, software environment) that inspires the user to follow relating regulation and protocol without fail.

---

[13] The fact that there seems to be a distinguishable layer of people who use a greater number of passwords could serve as a basis for further research. Experience shows that regarding data theft on an international level, most examination conducted focuses on easy-to-backtrack hashes, whereas a separate research may be based on cases including users who use random, long passwords consciously.

[14] NIST 800-118 recommendation, available at: http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[15] Som, Zoltán, Interoperabilitási kérdések és informatikai biztonsági tükrében a közigazgatásban [in Hungarian] (Questions Regarding Interoperability in the Reflection of Information Security in the Field of Public Administration) available in Hungarian at: http://real.mtak.hu/41851/7/interoperabilitasi_kerdesek.pdf

[16] Norbert Tihanyi, Comparison of two Hungarian password databases, Pollack Periodica, Vol. 8, No. 2, pp. 179–186 (2013)

[17] https://www.schneier.com/blog/archives/2016/08/frequent_passwo.html

Is the average human being really able to remember a) 10-20 or even more passwords, b) that are at least 8-10 characters long, each, c) that do not contain words with a meaning, or in other words are random, d) that are not algorithmable, e) are changed every three months, f) and are completely different from the previous one? Naturally everyone should know the answer to this question regarding themselves, but no solution is currently being made, or at least not on a scientific level. Technical solution is under development at the moment[18], and biometric authentication may also be a huge leap. It is however a long process to make every system and every single instrument compatible with such methods or to replace them by ones that are. But thinking a bit ahead, the same situation may occur by that time in the future. It is quite possible that by that time it would be possible to influence and cheat even biometric instruments and thus get around the authentication process just like it is possible to hack a password today, by countless methods. This means that no matter what the method of authentication is, whether it is "good" or not, whether it can be considered safe or secure is up to the "context", the environment it is in. And as such, the key factor is the human factor, which can be improved through education and training. It is also worth mentioning that should the level of awareness be below the level of discomfort regarding the processing and usage of the password, then the password will most likely be easily algorithmable and as a result, easy to hack, which is backed up by research.[19] This is due to the fact that such passwords do not follow the corresponding recommendations.

Question 2.11: How common is it to have a password protocol, or mandatory regulation regarding passwords on sites or software that you use?

- 25% of the answers said there usually are no such protocol.

This means that these regulation environments are not adequate or don't even exist, is weak, not noticeable or not transparent. It would be advisable to develop a recommendation that would serve as common guidelines for public and/or private participants.[20]

Questions 2. 14 - 2.17: Have you ever heard of a password safe (programs that specialize in password management)?, If you have heard of password safes, do you use them?, What are some of the good qualities of a password safe, what are the things that you like in them? Please describe it in your own words.

- 47% answered that they have heard of a password safe. 16% actually uses a password safe.

  38% of those who have heard of a password safe actually use it too.

Since we received outstanding results, we had the opportunity to analyze further related questions and factors in specific detail as based on our previous experiences regarding the research conducted in 2013, we were concerned that the answers might not have been truthful.

[18] Universal Authentication Framework

[19] Yinqian Zhang, Fabian Monrose, Michael K. Reiter: The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis, available at: https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf

[20] This means that both intent and knowledge are required. The case where the method of using so called "password safes", which is considered to be a good (or even best) practice among professionals is made impossible as the service provider does not allow the user to input his/her password using the copy-paste method, can be mentioned as a counterexample.

- 84% of the people who use a password safe have been using it for more than a year by the time they answered the questions, this being 13.5% of the total number of people who participated in the questionnaire.

- 6% of those who use a password safe started using it less than a year before the time of our research.

  This could hint a relatively high growth rate.

- 83% of those who use a password safe also provided comments in writing in relation of these questions.

Our goal was to implement a method of checking the truthfulness of answers, but since 83% gave valid reasons why they use a password safe, these numbers can safely be assumed to be true.

- 27% of the total of the total number of people who participated in the questionnaire answered that they are familiar with the term "password safe" but they do NOT use one.

Despite this relatively high number (of those who either heard of a password safe or actually use one), the ones who have heard of it but still do not use it still make up the majority.) Unfortunately we do not know exactly what the reasons behind this are, but we assume that the combination of the following factors play a key role: 1) ICT skills (or the lack of them), 2) Comfort/ the comforting factor of safety and 3) low level of awareness regarding possible threats.

Question 2.18: How often do you change your password(s)?

- More than 40% answered that they usually use the same password for more than a year before (if even) changing it.

This means that there is a need to change the usual behaviour of people as well.[21] This also points however at the need for a higher level regulation and a need for recommendations. This fact also means that a security risk may linger for a long period of time. Should someone acquire a password unauthorized that password may be used for months before the security breach is even found out.

Questions 2.19, 2.42, and 2.43: Do you have any passwords that is known by someone else as well, or any that you use together with someone? Have you ever revealed your password to anyone, even for a short period of time or temporarily? If you have provided your password to someone temporarily, have you changed the password once the reason was no longer viable?

- 50% answered that they have passwords that are known to others as well.

- 2/3 answered that they have shared their passwords with others before.

- 30% of those who shared their passwords with someone temporarily have not changed it afterwards.

[21] Zoltán, Som, Gergely, Papp, Hungarian Trends in Password Usage, in an International Comparison, Ceegov 2015

When a password is used by multiple people the problem arises that the identifier that is supposed to be unique and belong to a single person is used by someone else. The risk of such passwords getting in unauthorized hands is also multiplied in such cases.

Question 2.45: What do you think, are your passwords better or worse than those used by your acquaintances?

- As it can be seen below on Graph (Figure 1), almost everyone answered that their passwords are at least as good as the ones used by their acquaintances if not better. This reveals yet another problem, namely that most users don't even know that the passwords they use might not be satisfactory.

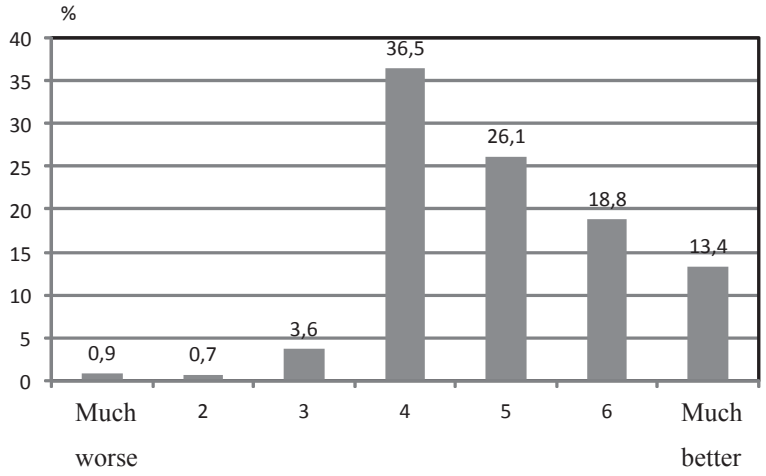

Figure 1: Question 2.45

Previously the focus was placed on circumstances, on education and training, organizational culture and peer pressure. In the following, focus shall be placed on something that helps deepen this approach. Assessing the answers briefly, the ones who provided answers wrote the following: "My password isn't any worse than passwords used by others". This supports all previous statements that the organizational structure, the culture and regulations of the given group will indeed influence individual behaviour. People tend to compare themselves to others and judge themselves based on such comparisons. If there is no related training within an organization and there is no relevant source of information on what is considered to be a "good password", then users and employees can only compare their passwords to passwords of other or to password-cultures that they now or think to be generally acceptable. This also applies to the general level of information security.

Organizational culture is extremely important. Momentary micro-decisions are based on the culture in each employees heads. Based on the personal experiences of the author the following is a common occurrence: "An easy/ quick/ short password is enough for now, I'll just change it later." This applies to numerous roles within the organization. These include the following: IT operator, user, manager, etc. Experience shows that the "I'll just change it later" part usually is often not realised.

Questions 2.47-2.48: Do you know any of your acquaintances' passwords? How did you get to know the password?

The answers are also indicated on Graph (Figure 2)

- 70% answered that they do no someone elses password.
- Fortunately in 93% of the cases the source to provide such password was the actual (original owner).

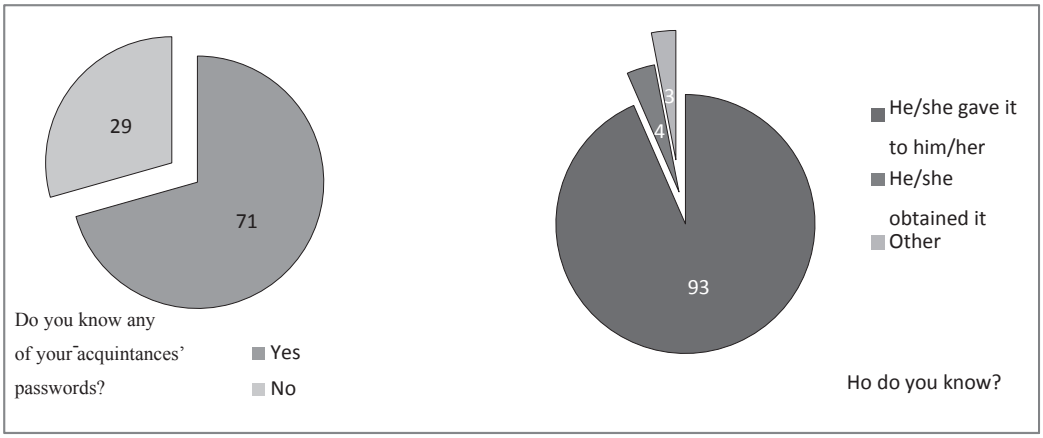

Figure 2: Questions 2.47-2.48

It is also clearly visible from the answers received to other questions not listed in this paper that expectations greatly influence the changing of passwords.[22] Usually the minimum password length required by the supplier becomes the *actual* (maximum) length of the password. This means that it is also the responsibility of the supplier to provide adequate requirements in order to minimize risks and threats and also to communicate them appropriately.

Summarizing the outcomes of the abovementioned research, the main highlights are as follows:

- it is the person who should be trained, he/she has to be provided information in possession which he/she feels supported in a situation that requires decision making,[23]
- there is a need for organized (centralized) education and training, which should be part of the National Cyber Security Strategy[24,25,26],

[22] Bruce Schneier, Choosing Secure Passwords, https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

[23] Tipton, Harold F., and Micki Krause. "Chapter 46 - Beyond Information Security Awareness Training—It Is Time To Change the Culture". Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications, 2007.

[24] Som, Zoltán, Az információbiztonság oktatási kérdései: igények és lehetőségek, NKE KDI Kutatási Fórum, 2014 [in Hungarian] (Questions Regarding Information Security Trainings: Needs and Opportunities)

[25] Government Degree No. 1139 of 2013 (21 of March) on Hungary's Cyber Security Strategy, Article 10

- the training program shall be based on international good (best) practices,
- the system should be measurable and should have positive results,
- to some extent it has to be modular and customizable to fit the actual needs of the organization,
- it should support the creation of separate modules which can later be shared by other organizations,
- it should be able to effectively support the ITSec organizational system that operates on low budget and with only a small number of personnel, as well as be able to personally support the ISO.

5. The National Model of Developing Cyber-Skills

Different trends appear, others disappear and yet others strengthen within a period of a few weeks or months.[27] This means that it would be required to have a method through which even public administration would be able to quickly react to such trends (or trend changes) by reaching the masses but also staying cost effective. For this to become possible, different cyber-skills need to be strengthened. An effective support can only be provided to the organizations in question if all (multiple millions of) employees of the state (and even suppliers) can be reached by the 15-25 minute message in an early stage in order to ensure end users realize, defend against and exercise preventive measures whenever possible. *Neither regulations or law nor technology will ever be able to keep up with real life, the everyday life of an organizational structure, which means that it is only advisable to create regulations to an extent that it would not become anachronistic in a short time.[28] This also means that it is possible to realize a regulation and also to take advantage of opportunities that are presented by technology and legal regulations by developing ones knowledge.* This is one of the most important reasons why it would be necessary to set up centralized coordination on the areas of education, training and measurement.

As the biggest employer of the country, the state has yet to set up a knowledge base through the mandatory awareness training (as required by law), analyzing which would result in greatly affecting cyber-skills.

The most important characteristics of the model include:

- the possibility to notice changes relatively quickly and react accordingly,
- the possibility of rapid spread of information,
- ensuring quick reaction,

[26] Beláz, Annamária – Berzsenyi, Dániel, Kiberbiztonsági Stratégia 2.0, A kiberbiztonság stratégiai irányításának kérdései [in Hungarian] (Cyber Security Strategy 2.0, Questions Regarding the Strategic Control of Cyber Security)
[27] Numerous malicious software have a short lifespan but their effect can be quite intensive, such as in the case of: malware, ransomware, or other program-codes that specifically target a specific vulnerability.
[28] Dr. Szádeczky, Tamás, Az IT biztonság szabályozásának konfliktusa, Infokomminukáció és jog [in Hungarian] (The Conflict of IT Security Regulations, Info-Communication and Law)

- all results can be monitored accurately,
- creates culture, moulds the way of thinking,
- generates changes on systemic level,
- e.g.: should a new threat be discovered, its detection, best response to it or methods for its prevention could quickly be included in the curriculum or training materials and these could be printed and made public right away,
- training modules would be processed by organizations in a rotational system,
- as opposed to the yearly mandatory training, it is possible to share knowledge at different times,
- measurements are being made that have outcomes that may require others to react,
- different measurements may be processed based on different factors, such as demography, geo-location, organizational aspects or others,
- it may induce organizational changes within an organization,
- may induce social changes,
- it is modular, it may be assigned to a given role only, it is flexible,
- it is cost effective, as it does not require the employees to be absent from work, the given employee may schedule the training to whatever time is most suitable for him/her within the given month,
- the question bank is randomizable,
- it makes the testing of ICT skills possible, including the absence or possession of basic skills, fundamental knowledge, key terms, etc.
- it makes it possible to set up a common vocabulary of the most important key terms and also allows it to later be improved, which would result in the creation of *common definitions: cyber language*,
- measurement results can be made available on a timeline.

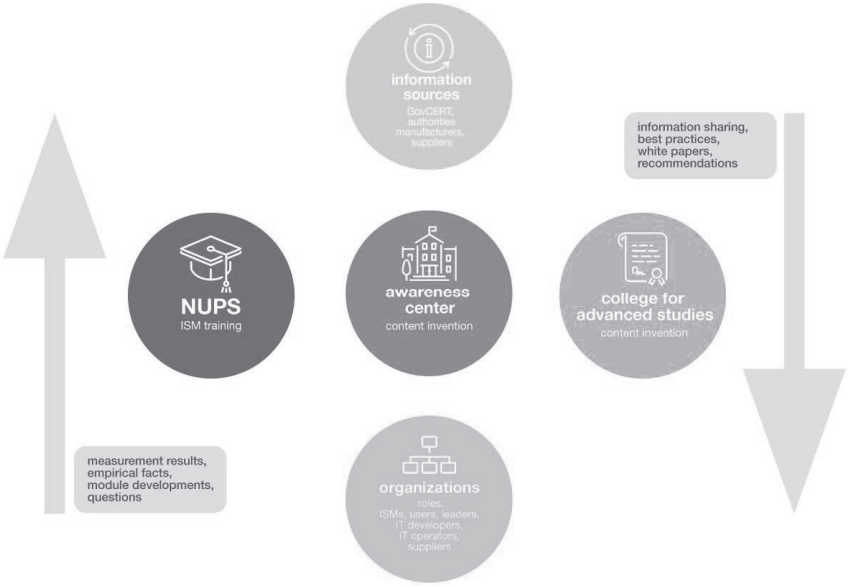

Figure 3: National Model of developing cyber-skills (hypothetical)

The model actually does more than developing information security. People that are around the age of 30 today would still be an employee for the next 30 years. Since we live in a society that is based on knowledge, it is a basic requirement that these employees would be professionally trained and be competitive. The research shows yet another interesting value, namely the high ratio of young employees and university students, which means that a training profile should be created for them as it would seem that this is an equally important question for young employees as well. Since the ICT sector accounted for 21% of the GDP growth in the EU in the last 5 years[29], it would seem that electronic authentication and trust services are literally in the interest of national economy. Regarding mid- and long terms it would open possibilities through which – through Open Data or other means – it would become possible to utilize such data as part of the national data asset. The centralized educational and training model could also serve as a good example in the future for other sectors and areas as well.

6. The Information Security Model

In today's modern society it is a structural part of our everyday lives to (continuously) use IT systems. However, most users are not aware of the (inner, structural) mechanics of the equipment they use, they mostly only come in contact with such devices as (end) users and in most cases the manufacturer also tries to keep as much of this hidden from the average user as possible. As a result a trend has seemed to emerge: Users learn to use the systems and equipment "on the go". Provided that there are no error messages displayed and the users actually succeed in whatever their objective was when they accessed the equipment in question, it is generally considered that the user is indeed capable of using such equipment (correctly).

[29] Zoltán Som, Laws aiding cyber security in the EU

The model basically (as can be seen on Graph, Figure no.3.) focuses on creating a knowledge centre that takes up a central role in developing materials that raise awareness. Once the materials are successfully developed, they would be available to all organizations covered by the scope of the corresponding regulations and also offer support in accessing and utilizing such materials. All required modifications, development, or updating as well as needs for potential new modules could be processed. The other function showed in the model (which is currently not available) would be the *professional college* of the graduates of the Information Security Leader (Chief Information Security Officer) Program on the National University of Public Services, which could gather all professionals of the field and form them into a community and provide a place for them to converse or even actively support each other.

The *main recommendation of this paper is to institutionalize the educational and training network of information security with special regard to creating and developing the centralized training of awareness in order to support public organizations.* Currently there is no specialized unit dedicated to develop or improve educational or tutoring skills within the university study program of two semesters[30]. The model aims at making the effectiveness of the training programs as well as the indicators of the level of cyber awareness measurable and also make the good and best practices catalogable.

7. Summary

In order to make developing information security possible, a relatively accurate picture is needed of the actual situation, but that alone is not enough, it should also be made possible to constantly and continuously monitor and measure changes. Following this, it would be possible to focus on different areas and "fine-tune" them based on geo-location, gender, age or organizational structure.
The model opens up numerous perspectives that are able to positively influence national cyber security and the level of awareness. In the same time, valid information is able to actively support aimed development and increase the speed of reaction to possible new threats. Information security trainings may also affect ICT skills and the situation of the economy and employment as well. It has been highlighted that peer pressure[31] and culture[32] both play an important role within an organization regarding information security awareness and the creation of fundamental stability. The method (that has been developed throughout the hundreds of lectures held by the author) could become an effective instrument that would be able to generate fundamental changes in the area in 6-18 months time.

8. References

[1] KARÁCSONYI, A.: A leadership és szervezeti kultúraés kapcsolatuk jellegzetességei a magyar szervezetek esetében, [in Hungarian] (Leadership and Organizational Culture and Characteristics of Their Relations Regarding Hungarian organizations) available in Hungarian at: http://phd.lib.uni-corvinus.hu/7/1/karacsonyi_andras.pdf

[30] National University of Public Services, Chief Information Security Officer training.
[31] N. Kollár, Katalin, Szabó, Éva, Pszichológia pedagógusoknak, (2004) [in Hungarian] (Psychology for Psychologists) available in Hungarian at:
http://www.tankonyvtar.hu/en/tartalom/tamop425/2011_0001_520_pszichologia_pedagogusoknak/ch17.html
[32] Karácsonyi, András, A leadership és szervezeti kultúraés kapcsolatuk jellegzetességei a magyar szervezetek esetében, [in Hungarian] (Leadership and Organizational Culture and Characteristics of Their Relations Regarding Hungarian organizations) available in Hungarian at: http://phd.lib.uni-corvinus.hu/7/1/karacsonyi_andras.pdf

[2] BELÁZ, BERZSENYI: Kiberbiztonsági Stratégia 2.0, A kiberbiztonság stratégiai irányításának kérdései [in Hungarian] (Cyber Security Strategy 2.0, Questions Regarding the Strategic Control of Cyber Security)

[3] BROTBY, W. K. and HINSON, G.: Pragmatic Security Metrics: Applying Metametrics to Information Security. Auerbach Publications, 2013.

[4] SCHNEIER, B.: Choosing Secure Passwords https://www.schneier.com/blog/archives/ 2014/ 03/choosing_secure_1.html

[5] Government Degree, No. 1139 of 2013 (21 of March) on Hungary's Cyber Security Strategy, Article 10.

[6] HEROLD, R.: Managing an Information Security and Privacy Awareness and Training Program, Second Edition. Auerbach Publications, 2011.

[7] ILLÉSSY, M., NEMESLAKI, A. and SOM, Z.: Elektronikus információbiztonságtudatosság a magyar közigazgatásban [in Hungarian] (Electronic Information Security Awareness in Hungarian Public Administration)

[8] BURNETT, M.: Perfect Passwords: Selection, Protection, Authentication.

[9] KOLLÁR, N.K., SZABÓ, Éva, Pszichológia pedagógusoknak, (2004) [in Hungarian] (Psychology for Psychologists) available in Hungarian at: http://www.tankonyvtar.hu/en/ tartalom/tamop425/2011_0001_520_pszichologia_pedagogusoknak/ch17.html

[10] NIST 800-118 recommendation, available at: http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

[11] TIHANYI, N.: Comparison of two Hungarian password databases, Pollack Periodica, Vol. 8, No. 2, 2013, pp. 179–186.

[12] PAPP, G., SOM, Z.: Jelszóhasználati trendek és az ügyfélbizalom értéke. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban, [in Hungarian] (Trends Regarding Password Usage and the Value of Customer Trust. Password, trust and e-acceptance in modern days II.),

[13] SZÁDECZKY, T.: Az IT biztonság szabályozásának konfliktusa, Infokomminukáció és jog [in Hungarian] (The Conflict of IT Security Regulations, Info-Communication and Law)

[14] TIPTON, H. F. and KRAUSE, M.: "Chapter 46 - Beyond Information Security Awareness Training—It Is Time To Change the Culture". Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications, 2007.

[15] BUKOWSKI, W.M.: Brett Paul Laursen, Kenneth H Rubin, Handbook of peer interactions, relationships, and groups, 2011.

[16] ZHANG, Y.: Fabian Monrose, Michael K. Reiter: The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis, available at: https://www. cs.unc. edu/~reiter/papers/2010/CCS.pdf

[17] SOM Z.: Laws aiding cyber security in the EU.

[18] SOM, Z.: Az információbiztonság oktatási kérdései: igények és lehetőségek, NKE KDI Kutatási Fórum, 2014 [in Hungarian] (Questions Regarding Information Security Trainings: Needs and Opportunities).

[19] SOM, Z.: Interoperabilitási kérdések és informatikai biztonsági tükrében a közigazgatásban [in Hungarian] (Questions Regarding Interoperability in the Reflection of Information Security in the Field of Public Administration) available in Hungarian at: http://real.mtak.hu/41851/7/interoperabilitasi_kerdesek.pdf

[20] SOM, Z., Gergely, Papp, Hungarian Trends in Password Usage, in an International Comparison, Ceegov, 2015.