The 8th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 14th 2013

THE HUMAN FACTOR IN INFORMATION SECURITY

Maj. Petruţ – Dănuţ SÂRGHE - CIOBANU

Land Forces

Abstract:

Information security breaches have incurred with increased regularity over the past years. Financial losses due to cybercrime continue to grow. Credit Card fraud, the theft of customer information, identity theft, social engineering, software piracy – these are all on the increasing slope.

Simple human error, ignorance or omissions are nearly always at the root of many of these information breaches. In almost every case there was no technical defense that would have prevented them. The damage to the public's confidence in the ability of any organization – public or private, large or small - to protect personal and financial data is immense.

Despite the vast sums of money spent, information security systems at all levels and within most organizations remain inherently vulnerable to even the most basic of security and fraud weaknesses and vulnerabilities. This is because we have focused almost entirely on the technology. We have not attended in any way the most fragile element – our people.

The human aspects of security and fraud prevention need to be promoted to their rightful place alongside the technical solutions. We must harness the support and assistance of every one of our employees and customers. We must ensure honesty and integrity is paramount alongside effective communication and understanding of what is required of them in their everyday behavior in order to handle information in all its forms in a safe and secure manner. Unless we do this, our information security defense will never be complete.

Key words: Information security; The Power of perception; The Human factor; Security culture; Security mistake; Security model;

1. Introduction

What do we mean by security?

Security is the concept that underlines this era. Security, if not already, will definitely be the main object of work in the years to come. When we say security we think mainly digital information security. With the development of technology, virtual spaces that once existed only in imagination begin to come alive. But we can say that human security refers to the protection, the safety of each of us regardless of social position we occupy or where we operate.

The human need for security is becoming increasingly urgent. Day by day the number of companies that need secure channels of communications increases, the number of people who want confidentiality of information is skyrocketing and the list goes on. Of these desires existing for a long time but otherwise in other forms, were born ideas, theories, and research programs related to information security.

2. The power of perception

In the specialized literature it is considered that the so-called classical approach to security overlap with the realistic vision of security. In terms of perception "security involves self-defense against external factors, visible, tangible. Among the problems related to security perception are: visionary environmental degradation, altered images and resistance to change of approaches on security. Identity, religion, ethnicity are fairly common causes of a perpetual conflict in security. If you can't justly analyze the impact on the security of a particular group or state, you can make grave mistakes from the starting point of your assessment, inducing a representation of issues other than the actual reality.

Under the risk perception concept, it is widely known that an increased factor of risk is considered in the areas related to image, security culture, and false confidence.

Analyzing the above, people decide what is right and what is wrong based on trust. Trust influences the perception of safety. Information transmitted most often is perceived initially based on the transmission mode then according to its meaning, security perception being influenced by what we see.

In conclusion, the perception of safety must be directly related to security culture, the need for security, the standard security model and supported by all of us with the confidence and trust that you show those around us.

3. The human factor

I would like to draw attention to one of the most important factors that endanger the security: the human factor. The human factor is the main issue that we must address to reduce the effects of insecurity. Most times, because of ignorance, carelessness, curiosity or whatever, people do things they should not. In order to prevent such unpleasant and undesirable situations we want a security program to take care of us when we are in times of need.

I will particularly focus on the human factor in achieving information security. Information security is a name... too general. First we need to understand the security needs of a person.

The common need for security of a person generally refers to the following examples:

Protecting against corruption
Protecting against theft
Protection against attacks, etc.

It is hard to realize a security model but not impossible. Security model's role is to integrate all measures in a multilevel security context, with a set of principles and processes for the information security environment.

I will illustrate a few security models:

- BRITISH MEDICAL ASSOCIATION MODEL - is a security model of their patients' medical data. It provides both data security and people safety.
- CHINESE WALL MODEL - bring new perspectives on access to information introducing the principle of separation of duties in various fields

I don’t know what others are doing in this area, but I can say that information security in Romania, from my point of view is more disorganized than others... something like ... "we are more Catholic than the Pope" ... but without great results on this domain.

So far I discussed the human factor in information security’s security model, what others do. Next step would be to cover the need for security awareness. Starting from saying "small stump fell great oaks" I tend to say that examples mentioned (Protection against corruption, theft, attacks), even though known by everyone, they are the ones that give the most problems because of their simplicity.

I think people should be aware of security as something that "helps" not as something that "stalks".

We talked before about the need for security awareness. Human behavior on security is different from person to person so it is very difficult to identify a behavioral standard. However I will give some examples of human behavior:

- Attitudes which may create uncertainty premises or persons information;
- Counter security abnormal events that can lead to corruption of people and information.

From a specialized analysis, we can say that people or human factor is very easy to handle, easy to be directed by what we actually do, feel or perceive. This shows that simple things can often be very complicated and we need security measures in order to prevent the possible corruption.

The results of studies show the following paradox: there is a huge gap between awareness of security issues and identifying solutions to maintain a sense of normality in security.

Participants identifying security issues and strategies that must be implemented or addressed need to improve the measures taken in order to maintain confidentiality. However, people fail to face problems because of the high rate of development of new technologies.

A different aspect of human security is related to technologies, new and old, modern or in desuetude.

Emergence and continued development of technologies at a high rate makes human security to suffer, to be more vulnerable. Vulnerability can be estimated looking at the large number of gadgets on the market. We should not say no to technology just so we can feel secure, but we can study and take measures so it doesn’t harm us. For this we need to know where the vulnerabilities are, which and how many measures we have to take to achieve our secure environment.

We talked about consciousness, skills and still think security is a very complex process. This process should identify a multitude of risks that threaten the human factor, which can give you a feeling of the behavior of this factor in a proper security environment.

Security must evaluate facts, and you should try to improve human behavior and always be ready to meet technological innovations.

Like I said before we need to be constantly aware of the risks that we expose ourselves to, consider all possibilities to ensure an almost complete security. I say almost complete because in reality there is no perfectly secure, one hundred percent sure environment.

4. SECURITY CULTURE

To succeed we must get involved and support ongoing studies, improve our security culture, to point out all risks and threats during analysis processes, because in order to get efficient results we must constantly adapt our security system to all emerging risks.

A very simplistic explanation of security procedures fall prey and are not effective because of the occult meaning associated with the word security, although the real meaning nowadays is transparent and is a positive one, based on justice.

Therefore, when we talk about security culture of a people should consider the implementation of democracy in that society and how competent state institutions working in security have failed to awaken, in the population, the roles, duties, benefits and expectations in order to achieve the individual security status.

Knowledge is power – and this is not a slogan used for justification, but simple reasoning. With a more complete vision of the increasingly complex world we live in, each can assume greater responsibilities, including the protection of personal existence; everyone can better understand the role of state institutions called upon to provide security and, consequently, may adopt a correct attitude in relation to them.

Security culture is a term that causes a real intellectual ecstasy to the military, police, CIA officers, Secret Services, the intelligence and paramilitary, entities rooted in this domain, converging towards “country security”.

Security is essential to life of individuals, communities and states. Virtually, the security is needed and can be applied in any area of individual and social life.

Communication to promote a culture of security must include a variety of forms and media. Also, the inadequate language, scientifically false, must be replaced with a language understood by all, but it can be done only by both policy makers and citizens alike!!

5. Conclusion

Reducing security risks requires the design and development of a safety culture that takes into account the human factor, the deficiencies inherent in the people. Proactive actions in addressing security can reduce the chances of success of "attacks", even if there is no absolute guarantee of security.

Staff training on possible risks is a very useful means of increasing the awareness to security needs.

Hoping to limit security risks caused by this primary vulnerability - the human factor – it is mandatory to design rules, and more precisely, rules designed and implemented so that it can not be easily bypassed or avoided by personnel.

The way ahead is not easy. To meet the challenges of the twenty-first century requires the implementation of the concept safety culture, and significant financial efforts from all. Moreover, it takes cooperation and solidarity of all members of the community to safeguard the common values.

In conclusion, the human factor is directly responsible for creating insecurity, and also is the main factor that can reduce, through its action the effect of threats and risks, maintaining a climate of normality in human and information security. The wrong perception of security is determined mostly by the human factor so the only one that can solve situation remains the humans.

References:

[1] http://www.humanfactorsinsecurity.com/

[2] http://www.google.ro/books - Managing the Human Factor in Information Security, by David Lacey

[3] http://www.sri.ro/fisiere/protectia-inf-cls-ghid.pdf

[4] http://www.datasecurity.ro/?p=6

[5] http://www.securitatea-informatica.ro/securitatea-informatica/globalizarea-si-riscurile-securitatii-informatiilor/

[6] http://www.securitatea-informatiilor.ro/modele-de-securitate/modelul-de-securitate-bma-211.html

[7] http://www.arts.org.ro/pdf/cn2011/04_S.Arion.pdf

[8] http://securitatea-romaniei.blogspot.ro/p/romania-cultura-de-securitate-si.html - Fragmente extrase din cartea lui Paul Carpen : Ferestre spre Securitate

[9] Chalk, P. (2000). *Non-Military Security and Global Order*. NY: Palgrave.

[10] Franck, T. & M. Glennon. *Foreign Relations and National Security Law. Belmont, West/Wadsworth,* 1993.