Telematic Journal of Clinical Criminology
www.criminologia.org

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004

The importance of human factor in ICT security policy.

by Roberta Bruzzone[1]

Introduction

Behind every security technology there is a person that has to use it. Hence every sophisticated logic and physical security system can be thwarted by users not trained or not positive about its necessity. Some criminal acts commited by employees (insiders) are tied to a reduced crime perception and this effect is due specially to the "techno-mediation" operated by the computer. In fact the most advanced psychological research on computer crime has pointed out some perceptive modifications caused by digital technology, specially when this technology mediates a relationship between the author of a crime and his/her victim: to commit a crime without drawing away from one's own "familiar and reassuring" workstation and mainly without looking one's own victim in the eyes represents a scenario less worrying for the individual. For this reason Human Psychology represents a factor that has to be considered by who projects and manages ICT security and in the modern"*vulnerability assessment*" an analysis sector dedicated to human factor should find its right place too.

Psychology and security

In the most advanced and developed working ambits Psychology has already got to do with security procedures since several years. Specially in the USA and Great Britain, for example, the *human factor* is particularly looked after within the ambit of physical security at workplace (industrial safety). Within these ambits the psychologist has the function to convince individuals (workers), beyond the rules, to carry out a safe behaviour, even appealing to their motivational world. For example, some workers of the most advanced and modern construction sites are subjected to psychological interventions (training courses, focus-groups, individual interview) to instil into them the habit to use individual and collective protection instruments in order to reduce the number of occupational accidents; workers that carry on dangerous jobs are trained to respect safety rules under the supervision of a psychologist.

Instead on ICT security and crime prevention front research and psychological intervention experiences seem really pioneer and in Europe they are traced to Prof. Marco Strano and his equipe 's experiences (the Author is a member of Prof. Marco Strano's equipe) while in USA they must be traced to another working equipe directed by Prof. Marc Rogers of Purdue University that works in strict scientific contact with the former. Within this ambit, the factors mostly investigated are *crime perception* (for insiders risk assessment) and *attack risk perception* (for security system vulnerability assessment tied to human factor).

Insiders and crime perception

Computer crime, as it's supported by modern specialistic literature (M. Strano 2000), is the result of complex dynamics, strictly tied up to interaction process among the author and penal and social laws/rules, external environment, his/her victim and, definitively, his/her own Self.

In other words, human beings commit illegal acts on the basis of a series of informations coming from their own experiences, from external environment (Rogers M., 2003), mainly from the interaction with other individuals and with laws (and social rules) concerning illegal acts. Then these informations are "processed" by their own mind that generates a decision-making process towards illegality or not. From this point of view to analyze how individuals sense and produce meaning about a particular

[1] Psychologist and Criminologist, Vicepresident of the International Crime Analysis Association (I.C.A.A.)

criminal behaviour is pretty important because this process influences in the final analysis the planning and the perpetration of a crime. Usually some of the factors relevant in a *"criminal decision making"* are the following (M. Strano, 2003):

1. Behaviour gravity perception
2. Assessment of risks to be detected
3. Assessment of risks to be reported
4. Perception of damage caused to the victim
5. Fear of social sanctions
6. Fear of legal sanctions

The above-mentioned factors can be measured with appropriate criminological investigation tools. (M. Strano, 2001).

Computer attack risk perception

The respect of a security measure by individuals centres on a series of cognitive patterns and attitudes that form risk perception:

1. widespread attitudes about security procedure's usefulness
2. knowledge of attack real risk
3. knowledge and fear of sanctions coming from no respect of the procedure
4. assessment of damages provokable by the attack
5. awareness to represent a target for an attacker

Of course, beyond all these factors, the ergonomic conditions of the procedure and the retardation's size/value of the working process have to be considered too (some security procedures pretty long and complex can represent an excessive bother for the operator)

A research on insiders and outsider risk based on human factor

It's interesting to quote a scientific research project on computer crime perceprion and information security culture headed by the International Crime Analysis Association (I.C.A.A.)[2], in collaboration with S.I.P.TECH[3], with The Italian State Police (U.A.C.I. - Communications Police Service[4]), with Purdue University (USA)[5] and with some consultancy companies in the field of Information security[6].

The target of the research is to measure crime awareness levels and risk attack perception levels in samples of both private companies and Public Administration workers, belonging to different hierarchic level. .

This study uses a computer crime assessment inside organizations centred on Human Factor P.R.A. (Psychological Risk Assessment) that includes two structured anonymous questionnaires (WC.P.Q. e C.R.P.Q.) realized by the I.C.A.A. and a case study grid (W.C.A.G.). The assessment is in course of administration in Italy and in USA and can be demanded directly to the I.C.A.A.

P.R.A assessment tools

W.C.P.Q. (**W**orkplace **C**omputer crime **P**sychology **Q**uestionnaire). The questionnaire is focused on "insiders" phenomenon and analyze the awareness of interviewed workers regarding illegal behaviours acted within the ambit of ICT. This instrument investigates, for example, how individuals interpret and consider different illegal activities connected to computer use within the company where they work.

This instrument measures the awareness of illegal act gravity, social reaction expectations, fear of sanction, estimate of the possibility to be detected and reported to the Police, the level of knowledge of the law on this specific subject and other attitudes and cognitive patterns that usually come into play when an the idea to act in an illegal way emerges into an individual's

[2] International Crime Analysis Association, a no profit association devoted to the spread of scientific research.
[3] Italian Society of Psychotechnologies and New Media Clinic
[4] UACI (Computer Crime Analysis Unit)
[5] Prof. Marc Rogers
[6] Symantec

mind.
The results of ICAA's WCPQ questionnaire suggest directly the variables on which it's possible to intervene to try to reduce the incidence of the phenomenon through training and sensitization paths aimed to legality culture.
C.R.P.Q. (**C**omputer crime **R**isk **P**erception **Q**uestionnaire). This questionnaire values attack risk (inside and outside) perception and the spread of attitudes and behaviors that can facilitate the attacks. The administration of this tool is preceded by an observation phase of the organization in order to identify some specific needs. Before the intervention the researchers effect a brief interview with the leadership of the company and with security managers in order to understand some possible "weak points" to measure. In fact the CRPQ questionnaire contains a general area suitable for all the analyzed organizations (18 questions) and a specific area (4/5 questions) that is calibrated on the organizational and productive characteristics of the company. This instrument allows to point out risk areas regarding the human factor within the ambit of ICT security process in both private and public organizations.
The administration time of both the instruments is pretty brief (about 20 minutes) and the analysis of the data obtained by the research permit to realize a report about security condition of that specific organization/company tied to "human factor" and to project a remedial measure based on risk elements that are present for real within the specific ambit of intervention.
W.C.A.G. (**W**orkplace **C**omputer crime **A**nalysis **G**rid). The case study grid gains all the standardized information (anonymous) about *outsiders* and *insiders*'s modus operandi and it's destined to the creation of an on-line database of free consultation by ICT security service workers (in course of realization by ICAA).

Psychological crime prevention: a professional intervetion.
The production and the administration of psychological tool destined to the measurement of crime and risk perception is an extremely complex and ticklish activity that has to be necessarily conducted by a psychologist with a large experience within the ambit of criminal psychology
In fact to operate within the ambit of a company on these issues in a non professional or awkward manner can give rise among the workers to an unpleasant sensation of control or crimination (rightly)
Moreover the subject "illegality" activates noticeable resistances and fears in the individuals that, even in an absolute anonymity context, often tend to conceal prospective attitudes not in accordance with the law/rules. The expertise and professionalism of a psychologist-criminologist in this ambit are connected just to the ability to produce an investigative tool able to understand even the "secondary markers" and not manifested of attitudes.
Moreover it's necessary to reduce the "resistances" (also the unconscious ones) and fears with a valid briefing before the administration. Then the absolute anonymity of the instrument completes the necessary requirements. The results obtained from administration of ICAA's psychological assessment proved to be pretty useful for the following planning of remedial measures targeted on the specific company reality, feasible through a widespread training of all the personnel or through a sensitization targeted action by executive managers within the ambit of work groups.

Bibliographic references
www.criminologia.org
www.icaa-italia.org
Galdieri P., Giustozzi C. Strano M, *Sicurezza e privacy in azienda*, Apogeo editore, Milano, 2001.

ANNO DI PUBBLICAZIONE DELL'ARTICOLO: 2004

Rogers M., *Organized Computer Crime and More Sophisticated Security Controls: Which Came First the Chicken or the Egg?*, Dept. Of Psychology, University of Manitoba, 1999 –

Rogers, M. *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. Unpublished dissertation, 2001

Rogers M., Psychological *Theories of Crime and "Hacking"*, Department of Psychology, University of Manitoba, Telematic Journal of Clinical Criminology, www.criminologia.org , 2003

Strano M., Computer crime, Edizioni Apogeo, Milano, 2000

Strano M., *Il computer crime nelle aziende* in BYTE, gennaio 1999;

Strano M., Bruzzone R., *Il computer crime nelle aziende: gli insiders*, in: M. Strano (a cura di) Manuale di Criminologia Clinica, See Edizioni, Firenze, 2003