Available online at www.elixirpublishers.com (Elixir International Journal)

Management Arts

Elixir Mgmt. Arts 37 (2011) 3707-3711

ISSN: 2229-712X

Assessment of social engineering effective criteria in the organization by DEMATEL method

Abbas Toloie-Eshlaghy[1], Sadaf Ashtari[2], Siavash Aflaki[2] and Imad Ibrahimi[2]

[1]Industrial Management Department, Faculty of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2]Information Technology Management, Faculty of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran.

ARTICLE INFO

Article history:

Received: 2 June 2011;
Received in revised form:
16 July 2011;
Accepted: 27 July 2011;

Keywords

Information security,
Social engineering,
Behavioral criteria,
Group decision making model
DEMATEL.

ABSTRACT

Today, one of the problems of managers is information security in the organizations and ways of struggling with those penetrating into the organization. Social engineering technique is one of the ways of access to organizational information through vulnerable behaviors of human beings. This article tries to determine the most important criteria by assessing effective social engineering criteria in the organization in DEMATEL method. At first, views of the experts have been used in order to select effective criteria and then a structure based on theory of graphs was formulated on the basis of experts' judges and a mathematical model has been obtained with regard to relations, manner and intensity of effect and their interactions. Finally, determination of criteria importance helps the managers make decisions and do correct management in the organization.

© 2011 Elixir All rights reserved.

Introduction

In recent years, the organizations have seen considerable changes in the field of management. Therefore, traditional criteria of competition in market cannot be relied especially in another global level and issue of suitable confrontation with internal and external information of the organization has been considered by the managers. One of the issues which are very important for most organizations providing internet services and even institutes with sensitive information is keeping confidentiality and assuring security of the organization information which is regarded as one of the capital of the organization. Unfortunately, most organizations spend huge expenses for providing security hardware and software equipment and take action regarding purchase of all kinds of antivirus, firewalls, and penetration diagnostic systems but they ignore weak points of security in most organizations and are seldom seen and considered.

According to studies of Gartner Research Institute, the most important security risks of the organizations during the last 10 years include social engineering technique. But social engineering attacks can be behavioral or psychological. Behavioral tactics mostly relate to receiving information from the organization or reading organizational documents and psychological tactics include hacking the persons or exploiting human factor. We seek to find social engineering attacks with regard to human factors which cause unauthorized access to information systems, data and networks of the organization.

Social engineering

Social engineering includes a kind of nontechnical entrance to the system with use of information gathered from the organization dependent on behavioral skills, smartness and intelligence of the person. Social engineering is one of the general and simple ways of penetrating into information networks of the organizations. Social engineering includes intelligent misuse of natural tendency of human being to trust which encourages the person to disclose information or perform special work with help of a set of the techniques. Social engineering seduces the human beings in different ways and misuses them for access to the information by encouraging them. Social engineering is art of exploiting vulnerable behaviors of human beings for creating security gap without any suspicion by the victim.

In guidance of CISSP study, social engineering has been defined as follows:" a skill which is used by an unknown person in order to increase trust of the persons inside the organization and to encourage them to make desirable changes in IT systems and achieve the access right".

In English version of Wikipedia, social engineering has been defined as follows: "social engineering is technique of obtaining confidential information by seducing the authorized users".

Types of social engineering:

Technical information –based engineering

Among the technical information-based engineers, the hackers and Fishers maneuver with their information. They act like those who take action regarding design and development of false pages of banks and financial institutes for stealing user names and passwords or those who try to use combination of their technical and engineering sciences like the hackers who force the user to receive the attached files by sending emails with seducing texts.

But in comparison to social engineers based on human beings, they perform all of their goals by establishing communication with persons by phone or physical contact. Such persons have no abundant technical information and double their attacking power by cooperating with skilled specialists. Social

Tele:
E-mail addresses: toloie@gmail.com, s.ashtari@itmen.ir

© 2011 Elixir All rights reserved

engineers take action regarding gathering information which is used later by the technical attacking expert to create access.

Human forces –based engineering:

With social engineering, you don't work with any software or hardware but you work with Wetware which is mind and brain of the human beings. Wetware is a human element in computer sciences. People naturally trust in each other and social engineers take action regarding exploitation of other people with use of this benefit and potential.

Social engineering attacks:

Social engineering attacks originate from three areas:

oInternal: most internal threats are done by the staffs who gather sensitive and important information personally or with use of the staff that have access to IT systems. These persons are the staffs who have limited level of trust in the organization and this has simplified attack by them. This group includes unsatisfactory, temporary staff and workers such as cleaning workers and repair personnel.

The trusted persons: such threats are done by the persons who relate to the organization in a series of legal and formal bases. These persons include contractors, consultants and partners of the organization. Mostly, these persons have high level of the organization's trust and they have access to sensitive and important data of the organization. However, such hidden hazards are rarely considered in security programs of the organizations.

External: these threats are done by the persons who don't communicate with the organization. This set includes hackers, competitors who seek to disclose confidential information of the organization and are the criminals or thieves. There is no level of trust between these persons and organization, therefore, they seek to create short-term trust with use of different techniques of social engineering such as playing role of a independent person inside the organization such as IT manager , repair technician , desolate employee et.

Social engineering attacks cycle:

Gathering information: a set of different techniques which are used by the attacker for gathering information about goal. The attacker gathers simple but useful information such as telephone number list, birth date, organizational chart etc to achieve the desired key information.

Establishing communication: attacker misuses trust and tendency of the victim for creating trust to establish communication. After establishing communication, attacker pretends to be trustworthy to exploit such position.

Exploitation: the victim is affected by trust of the attacker in order to clarify information such as password or perform some work which he had not done naturally such as making user identification code for the attacker etc.

Action and execution: when the target performed the action wanted by the attacker, the cycle was terminated and the attacker has reached his intention.

Each stage of social engineering cycle is unique dependent on different conditions and techniques. Each stage depends on completion and success of the previous stage. In order to do successful attack, this cycle is repeated for times because it is not easy to establish communication and increase trust. The attacker needs to gather enough information about the organization, available systems and its staff. Social engineering attack includes techniques based on computer and human being which will be described later.

Computer-based techniques

o Pop-Up
o Electronic attachments
o Chain and seducing words
o Websites
o Retrieval and analysis of the used tools
o Phishing
o Human being-based techniques
o Direct approach
o Searching in recycle bins
o Forging identity
o Misuse of important users
o Technical support staff
o Desolate user
o Shoulder Surfing
o Rumoring
o Spying and eavesdropping

DEMATEL method implementation

DEMATEL method was applied in late 1971 A.D. for very complex global issues and use of the experts' judgment in scientific, political, economic, social fields and doctrinal leaders and artists. This method which is one of the decision making methods based on pair comparisons presents hierarchical structure of the factors available in the system with interactions of the said elements with use of the experts' judgment in extraction of factors of a system and structuring them systematically with use of principles of theory of graphs so that it determines intensity of the effect of the mentioned relations as numerical point.

One of the points of DEMATEL method compared to other decision making methods based on pair comparisons is acceptance of relations feedback. It means that each element in the obtained hierarchical structure can have effect on all elements of the same levels, higher levels or lower levels and be affected by them. On the other hand, elements available in the system cannot be independent of each other. Importance and weight of each factor in system is determined not only by superior factors or the inferior factors but also by all factors available in the system (and the entire model). Acceptance non-transferable relations and ability to display all possible feedbacks are of the reasons for priority of this method over other methods based on theory of graphs.

For use of DEMATEL, it is not necessary to hold decision making sessions and experts residing in different regions can make decision. Modeling process in this method shows that policy of its executive operations can be easily analyzed. The said method encourages the experts to study deeply on the list of the factors available in the problem by recording and structuring the results obtained from experts' views effectively and systematically and creating interaction and understanding between them and system analyzer. The experts' judgment was simple in pair comparison of this method and didn't require their awareness with DEMATEL process but their view and insight are very effective from different aspects of the problem in result of DEMATEL.

For each problem, one can repeat DEMATEL process for many times and achieve their suitable structure by criticizing and revising the factors constituting system and intensity of effects. Validity of the hierarchy of the final structure has been provided without regard to scientific quality of data. Execution of this method requires time and accuracy especially in cases that the problem is large and extensive and many factors play role. In the research done by writers, DEMATEL method was applied in 9 steps.

First step: in this step, list of the available factors in the problem should be extracted on the basis of the experts' view with one of the innovative methods in experts such as Brain storm, Brain writing, nominal group technique, survey, Delphi method or conference. It is evident that it will be possible to achieve multilateral dimensions of the problem with surveying opinions of the more experts. Number of the expert members has been announced to be 10 to 12 in some sources but one should note that quality of the experts' views and scope of their insights are very important. The experts understanding of relation between elements available in the studied problem is very effective in final structure of the system. In this research, list of criteria was extracted with use of library studies and in interaction with and confirmation of the experts.

Second step: one opinion survey matrix was prepared among the criteria extracted in the first step so that the criteria constitute rows and columns of this matrix. This matrix was given to the experts and they were asked to insert effect of row action on column factors as numbers between 0 and 4 in the related cells by pair comparison of each factor located on each row of matrix with all factors located on the columns so that these numbers imply the following concepts (these points may be between 0 and 10 or 0 and 100):

0: row factor has no effect on column factor.
1: row factor has little effect on column factor.
2: row factor has effect on column factor
3: row factor has relatively high effect on column factor
4: row factor has intensive effect on column factor.

The important point which the experts should have considered in pair comparisons was that they should give point to only the direct relation of row factors and column factors and make no mistake due to many matrix cells and not consider reverse relations i.e. effect of column factor on row factor. They should withdraw indirect effect of row factor on column factor due to the factors available in the problem because indirect effects appear automatically in final structure of the problem.

Third step: matrices resulting from the second step are gathered and presence or lack of relation between both factors are decided on the basis of majority experts' view (in the accepted matrices which are more consistent with each other) so that if more than half of experts recognized effect of a row factor on column factor to be zero , lack of effect of row factor on column factor and the number of view about point above zero on a matrix cell confirmed effect of row factor on column factor.

Fourth step: average points which experts gave to direct relation of row factor on column factor for each one of the confirmed relations was determined(in case of use of points 0 to 100 in the third step, geometrical mean is applied).

Fifth step: matrix X which indicates effect in direct relations of system was formed with regard to the third and fourth steps. Entries of this matrix have zero (third step) on the basis of the unconfirmed relations and have mean value of the obtained points (fourth step) on the basis of direct confirmed relations. In this step, diagram corresponding to matrix X was drawn as the primary diagram so that its apexes are the same criteria constituting the system and its arcs should be set in direction of the direct relations between both factors of system and effect of each direct relation on the corresponding arc. It is evident that effect of zero represented lack of direct relation in pair comparison and no arch is drawn for it.

Sixth step: row sum of the entries of Matrix X was obtained and Matrix X was multiplied by reverse maximum row sums to obtain Matrix M which is indicative of relative effect on direct relations in system. This multiplication doesn't cause to deviate from trend of the available answers. Because those answers are available for direct relations and indirect effects of factors on each other are less than their indirect effects.

$$M = \lambda X$$

Step 7: on the basis of Matrix S which indicates relative effect on direct and indirect relations available in system, R+J was formed as follows:

$$S = M (I-M)-1$$

Eighth step: in matrix S, row (R) and column (J) sum of entries and sum of (R+J) and deduction of (R-J) were calculated. Sum of (R+J) for each one of the factors constituting system indicated importance (weight) of the factor in system. Value R for each factor indicates effect of that factor on other factors of system and value of J corresponding to it indicates effect of other factors on the said factor. Therefore, R+J indicates sum of interaction of the related factor in the system. On the other hand, factor having the highest value has the highest interaction with other system factors. Final value of effect of each factor on R set of system factors is obtained from deduction of R-J so that;

$R > J$	$R – J > 0$	factor has final effect
$R < J$	$R – J < 0$	factor is finally affected

Ninth step: a Cartesian coordinates set is formed so that its abscissa is calculated in terms of values +J and its ordinate is calculated in terms of R-J and position of each one of the factors was defined with a point in coordinates (R+J, R-J).

Research methodology

During the performed researches, 12 main criteria which are effective on psychological techniques of social engineering were specified by doing library studies and getting views of the experts and confirmed by the experts. Due to widespread subject and different organizational layers, these studies were limited to communication layer of the organization and the related criteria relate to this layer:

Persons' access: the more access the persons have, the more possibility for the intruding persons to have access to the information. Secretary of the organization or administrative technician is among the persons who have access in the organization (a).

Commitment to the organization: If a person is committed to the organization and has organizational identity, he will be rarely attacked by the social engineering. For example, shareholders are among the persons committed to the organization who don't disclose information of the organization (a).

Scope of authority : the more the authority, power and ability of the person , the less the possibility of hackers intruding through social engineering because such person has more control on affairs and decreases unauthorized access to information of the organization(b).

Satisfaction of the staff: when satisfaction of the staff with organization increases, they will be more committed to the organization and give more weight to the organization sources such as its information. The satisfied staff will not intend to disclose confidential information of the organization(c).

Work experience: the more the work experience of the persons, the less the possibility of being victimized against social engineering attacks (d).

Education: staff with high educational level will be more aware of the organization's issues and act more intelligently (f).

Trust: human beings tend to be trusted by others without any logical reason and trust in others. But if the person is more trusted by the organization, he will disclose less information of the organization to others and will not be regarded as good prey for the hackers (g).

Helpfulness: some staffs are very kind and want to help all people .such persons are good prey for social engineering attacks because hackers will get access to the required information by misusing this feeling (h).

Ignorance: it means that staffs are unaware of consequences of incorrect use of information or damage integrity and authenticity of the information by forgetting correct work of information systems (i).

Feeling of access to reputation: some persons who intend to seek reputation may want to achieve such position by publishing critical information of the organization (j).

Excessive fatigue of the staffs: when the staffs are excessively fatigue, they will make more mistake and be victimized (K).

Fearing loss of job: if a staff fears loss of job or organizational position, he will think that he can prevent from such event by giving important information which he has (l).

Analysis of final structure:

It is not possible to study final model with more than 100 direct relations in this writing but some parts of the general attitude of the mentioned model can be presented. In the lowest parts of diagram 1 i.e. the most negative values of (R-J) are criteria which are affected by other criteria
(-1.6> R-J > 0).
L: fearing loss of job (job security)
e: work experience
b: commitment to organization
h: kindness and helpfulness
a: access of the people
g: excessive fatigue of the staff

On the other hand, these criteria can be affected by change in other criteria inside the model. The criteria which are on the left side of the coordinates (i.e. small values of R+J) include:

Fearing loss of job (criterion l), ignorance (criterion i), work experience (criterion e). l and e criteria which have negative R-J are less affected by other criteria. But criterion I which has positive R-J are more affected than effective and generally, there is weakness in the necessary substructures.

By moving from left side to right side in diagram 1 i.e. gradual increase of *R+J* in average values limit (positive and negative) ,more effective criteria will be evident in social engineering gradually and finally degree of kindness and helpfulness (index h) with the maximum value of *R+J* is placed on the right side of the diagram.

On top of the diagram, i.e. maximum value of *R-J*, are two criteria of authority (criterion *c*) and education (criterion *f*). These two criteria with average weigh priority are less affected than other criteria are and have effect intensively on them.

Conclusion

As shown in analysis of system final structure and diagram 1, the most serious criteria in effectiveness of the social engineering attacks include:

- Helpfulness
- Satisfaction of staff
- Authority
- Commitment to organization

Social engineering is one of the main security hazards and serious problem of most organizations. Since technology progress causes to increase hardware and software security level of the organization, hackers tend to use social engineering psychological techniques for intruding the organization and gathering information. In fact, change in psychological reactions of staffs in large organizations is not simple. But security managers can reduce risk of social engineering hazards by training the staffs and promoting organizational culture of persons.

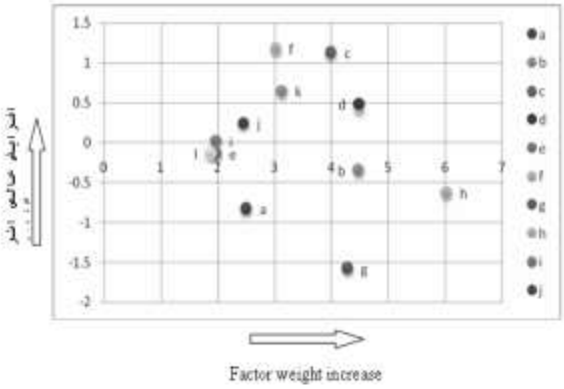

Figure 1: final coordinates in(R+J, R-J)

For example, managers can ask the persons to have less trust in others. On the other hand, organizations should make their staffs sensitive to asking question and not allow them to ask a question to remove helpfulness and excessive trust in them. In addition, staffs should know that information security is useful for the organization and themselves and effect of this behavioral change is more evident in long term. Therefore, training and increasing awareness of the staffs are the most important work for prevention from social engineering attacks. The trained staffs can prevent from these attacks. Security information program should be continuous and dynamic.

References

1. Asgharpour. M.J. (2003).Group decision making and games theory with a operations research approach.Book-Tehran University Publications, Tehran, Iran.
2. Chin, P. (2003). The Spy Who Flubbed Me: Intranet Security Begins with Education. The intranet Journal. Retrieved from The Intranet Journal web site:
http://www.intranetjournal.com/articles/200312/ij_12_12_03a.html
3. D'Agostino.D.(2003). What is Social Engineering. Retrieved from Castle Cops web site:
http://castlecops.com/article2934.html
4. Garceau. L.(1997). The Threat of Social Engineering. The Ohio CPA Journal. Retrieved from HighBeam Research web site: http://www.highbeam.com/library/index.asp
5. Granger.S.(2002).Social Engineering Fundamentals. Part II: Combat Strategies.
6. Gulati. R.(2003). The Threat of Social Engineering and Your Defense against It. Retrieved from SANS Institute web site: http://www.sans.org/rr/whitepapers/engineering/1232.php
7. Hall. M.(2005). Secure the People. Computer world. Retrieved Computerworld web site:
8. How to Protect Insiders from Social Engineering Threats.(2006).available at:
http://technet.microsoft.com/en-us/library/cc875841.aspx
http://www.computerworld.com/securitytopics/security/story/0,10801,100448,00.html
http://www.securityfocus.com/infocus/1533

9. Stich, P. (2005) .IT Security: The Human Factor. ISSA Journal.

10. The Complete Social Engineering FAQ. Available at: http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt

Table 1: matrix X

	a	b	c	d	e	f	g	H	i	j	k	L
a	0	0	0	0	1	0	0	3	0	1	0	0
b	2	0	0	2	1	0	2	3	1	2	1	0
c	0	2	0	3	0	2	3	3	0	1	0	3
d	3	4	0	0	0	1	2	4	0	0	2	0
e	0	0	0	0	0	0	3	2	0	0	0	2
f	0	0	2	2	0	0	2	2	1	3	0	0
g	0	3	4	0	0	0	0	0	1	0	0	0
h	3	3	2	2	2	2	3	0	0	0	2	0
i	0	0	0	0	0	0	4	0	0	1	0	4
j	0	2	0	2	1	0	0	2	0	0	1	0
k	0	0	0	3	0	0	2	3	4	0	0	0
l	0	0	0	0	1	0	0	3	0	0	1	0

Table 2: Matrix S

	a	b	c	d	E	f	G	h	I	j	K	l
a	0.0584	0.0748	0.0422	0.0576	0.0954	0.0342	0.0834	0.2336	0.0195	0.0771	0.0424	0.0205
b	0.2317	0.1783	0.1028	0.2107	0.1319	0.0636	0.3072	0.3581	0.1162	0.1684	0.1426	0.0538
c	0.1658	0.3230	0.1360	0.3210	0.0941	0.1923	0.3636	0.4156	0.0740	0.1460	0.1208	0.2087
d	0.3363	0.3892	0.1255	0.1656	0.1000	0.1306	0.3341	0.4542	0.0913	0.0968	0.2120	0.0491
e	0.0462	0.0850	0.0665	0.0479	0.0340	0.0287	0.2358	0.1651	0.0272	0.0222	0.0368	0.1218
f	0.1242	0.2013	0.2326	0.2442	0.0725	0.0774	0.3147	0.3342	0.1085	0.2303	0.0930	0.0672
g	0.0748	0.2690	0.2528	0.1035	0.0433	0.0511	0.1405	0.1504	0.0924	0.0624	0.0508	0.0642
h	0.3090	0.3617	0.2179	0.2702	0.1934	0.1852	0.3851	0.2957	0.0945	0.1067	0.2064	0.0743
i	0.0333	0.0813	0.0638	0.0450	0.0338	0.0202	0.2592	0.0937	0.0278	0.0758	0.0370	0.2236
j	0.1029	0.2038	0.0568	0.1984	0.1063	0.0463	0.1372	0.2565	0.0468	0.0423	0.1228	0.0296
k	0.1279	0.1737	0.0955	0.2800	0.0619	0.0641	0.2814	0.3351	0.2509	0.0570	0.0861	0.0730
l	0.0599	0.0731	0.0444	0.0622	0.0929	0.0352	0.0915	0.2380	0.0309	0.0217	0.0965	0.0230

Table 3: priority of criteria by order of weight and pure intensity

Weight priority	criterion	*R+J*	descending order of effects of *R+J*	No	criterion	*R-J*	Type
1	*h*	6.0303		1	*f*	1.1712	0<*R-J* Effective factors
2	*d*	4.4911		2	*c*	1.1241	
3	*b*	4.4795		3	*k*	0.6393	
4	*g*	4.2890		4	*d*	0.4783	
5	*c*	3.9975		5	*j*	0.2432	
6	*k*	3.1335		6	*i*	0.0143	
7	*f*	3.0290		7	*k*	-0.1396	0>*R-J* Affected factors
8	*a*	2.5097		8	*e*	-0.1423	
9	*j*	2.45665		9	*b*	-0.3489	
10	*e*	1.9768		10	*h*	-0.6302	
11	*i*	1.9743		11	*a*	-0.8312	
12	*l*	1.8783		12	*g*	-1.5783	