Strategic planning for the Computer Science Security of Banking Organizations, Companies and Government

JORGE ALBERTO RUIZ-VANOYE[1], OCOTLAN DÍAZ-PARRA[2]
[1]Facultad de Ciencias, [2]Centro de Investigaciones en Ingeniería y Ciencias Aplicadas
Universidad Autónoma del Estado de Morelos
Av. Universidad 1001. Col. Chamilpa Cuernavaca, Morelos
MEXICO

ISMAEL RAFAEL PONCE-MEDELLÍN[3]
[3]Computación. Centro Nacional de Investigación y Desarrollo Tecnológico
Interior Internado Palmira s/n, Col. Palmira. Cuernavaca, Morelos
MEXICO

ALEJANDRO FUENTES-PENNA[4]
[3]Informática. Universidad Politécnica del Estado de Morelos
Boulevard Cuauhnáhuac #566 Col. Lomas del Texcal, Jiutepec, Morelos
MEXICO

JUAN CARLOS OLIVARES-ROJAS[5]
[5]Informática. Instituto Tecnológico de Morelia.
Av. Tecnologico 1500, Colonia Lomas de Santiaguito, Morelia,Michoacán
MEXICO

Abstract: The necessity of the companies and organizations to adapt the technological and computer science change takes to formulated key questions: What type of Computer science Security needs my company, financial organization, or government? My financial organization counts with aspects of computer science security in the correct areas? What new tools of computer science security exist? What strategies of security we must follow? In this paper we show a methodology for strategic planning for the computer science security of Banks, Companies and Government, cradle in the concepts of strategic administration of enterprise politics, which tries to give answers to the questions before mentioned.

Key-Words: - Analysis Methodologies, Security Aspects, Strategic Planning, Computer Science Security.

1 Introduction

This paper proposes to use of techniques for the strategic administration to provide computer science security to companies, financial organizations and government.

The strategic planning [1,2,3,4,5,6,7,8] adapted in the computer science security is observed in many senses like a military strategy, which take advantage of their forces to operate the vulnerabilities of the competitors or the attackers, if the computer science security strategy[9,10,11] is not effective, then nor all the efficiency of the world will be enough to provide a good security.

In section two will be comment the general process to provide computer science security, describing the formulation of the security strategy, its implementation of the security strategy, and on the way to evaluate Computer science Security strategic. In section three are quantitative tools to measure the performance of the strategy of computer science security. In Section four we propose generic strategies for the computer science security.

2 Strategic planning for the Computer Science Security

The planning strategic like science to formulate, implement and evaluate decisions of Computer Science Security that allow the company, financial organization and governments to reach their objectives about computational security.

The strategic planning for the computer science security consists of 3 stages:

1. The Strategic formulation of computer science security. It consists of formulating the mission of computer science security of the company or financial organization, identifying the external opportunities and threats of security to the company or financial organization, define the forces and vulnerabilities in the computer science security, establishing long term objectives and generate strategies of computer science security.

2. Implement the strategy of computer science security. The financial organization or company will have to establish annual objectives to maintain the security computer science, devise policies of computer science security, and motivate the employees to follow the politics of computer science security and to assign resources for it.

3. Evaluation of the strategy of computer science security. In order to evaluate the strategy of computer science security the internal and external factors are due to review, to measure the performance of the computer science security strategy and to make remedial actions to the strategy.

2.1 Formulation of the Strategy of Computer Science Security

The formulation of the computer science security strategy consists of five phases (Fig.1):

1. Formulate the mission of computer science security of the company or financial organization. It describes the values and the priorities in the matter of computer science security of the company, financial organization or government. It is necessary to analyze the actual and future reaches of the tools of computer science security in the computer science market.

2. Identify the external opportunities and threats of security for the company or financial organization. The opportunities and threats are outside the reach of the organization, about technological changes, new computer science vulnerabilities, virus, phising, pharming, new heuristic algorithms for attacks detection and improvements for the prediction of possible computer science attacks.

3. Define the forces and vulnerabilities in the matter of computer science security. There are those activities that can control the organization at diverse levels. For example, errors in the network devices configurations are because they don't have an intrusion detection system, or neither have an expert in computer science security within the organization.

4. Establish long term objectives in the matter of computer science security. They are specifics results in the matter of computer science security of more than a year of duration, feel the bases to plan and to motivate with effectiveness the use of the computer science security in the organization. Objectives for the complete organizational organization and each one of the divisions are due to establish.

5. Generate strategies of computer science security. They are the way to obtain the long term objectives in the matter of computer science security.

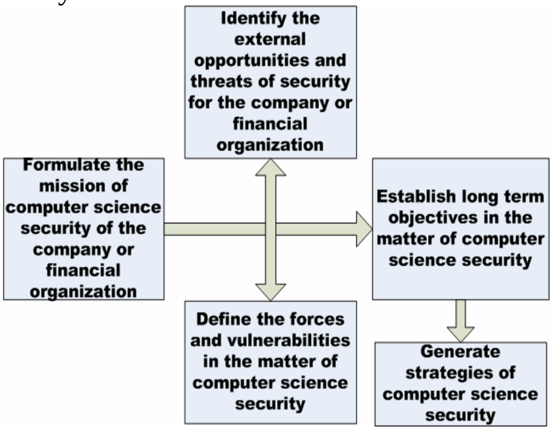

Identify the external opportunities and threats of security for the company or financial organization
Formulate the mission of computer science security of the company or financial organization
Establish long term objectives in the matter of computer science security
Define the forces and vulnerabilities in the matter of computer science security
Generate strategies of computer science security

Fig.1. Strategic formulation of the computer science security

2.2 Implement the Strategy of Computer science Security

The implementation of the strategy of computer science security consists of two phases (Fig.2):

1. Establish annual objectives to maintain the security computer science. They are the goals that are due to reach in the short term to obtain the long term objectives, must be organized in precedence of the computer science factor of safety.

2. Make computer science security policies [10, 11]. They are procedures and established rules to maintain the computer science security in the organization, serve to reach the annual objectives. It is necessary to motivate the employees to do the policies of computer science

security and assign resources to maintain them in operation.

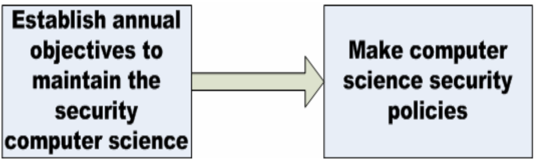

Establish annual objectives to maintain the security computer science
Make computer science security policies

Fig. 2. Implement the strategy of computer science security.

2.3 Evaluation of the Strategy of Computer Science Security

In the evaluation of the strategy of computer science security exists 3 phases (Fig.3):

1. Review the internal and external factors in the matter of Computer Science Security. Verify the existing security on which at the moment the organization counts, as well as technologies and mechanisms to provide computer science security.
2. Measure the performance strategy of the computer science security (to see section 3).
3. Take remedial actions to the strategy of computer science security. Modify the strategy in case of being necessary.

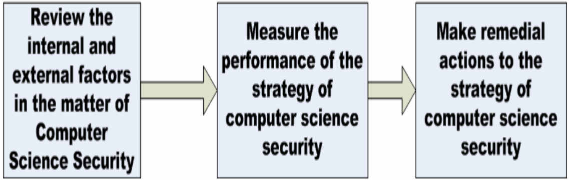

Review the internal and external factors in the matter of Computer Science Security
Measure the performance of the strategy of computer science security
Make remedial actions to the strategy of computer science security

Fig.3. Evaluation of the strategy of computer science security.

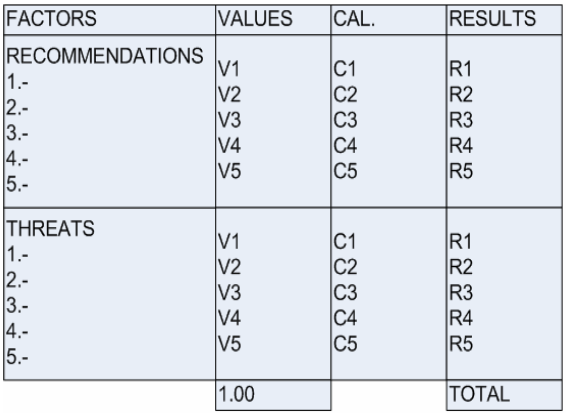
3 Tools to measure the performance of the computer science security

The matrixes of the strategic planning for the Computer Science Security are excellent methods to measure the performance of the security strategies.

3.1 Matrix of Recommendations and Threats (RT)

The procedure to elaborate a matrix RT consists of the following steps:

1. A list between 10 and 20 factors (recommendations and threats), must of being external factors to the organization in the matter of computer science security.
2. Assign a value between 0.0 (it is not important) and 1.0 (it is very important) the sum of all the values must give 1.0, in some cases the values of threads would be greater than the values of the recommendations when the threats are serious
3. Assign a qualification from 1 to 4 to each one of the elements of the list in case that the organization this reacting with effectiveness, 4=Answer superior, 3=Superior to the average, 1=Answer average 2=Answer badly.
4. Multiply the value by its qualification to obtain result of the factor.
5. Add the results of the factors.



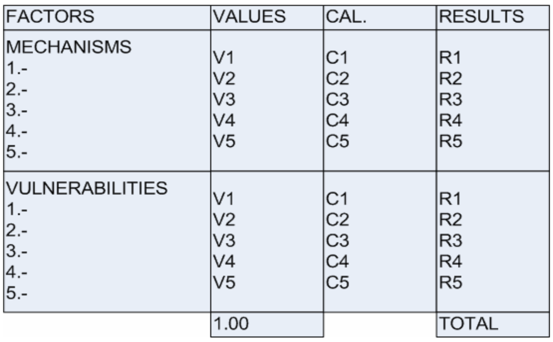
FACTORS	VALUES	CAL.	RESULTS
RECOMMENDATIONS 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
THREATS 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
	1.00		TOTAL

Fig.4. Matrix RT.

3.2. Matrix of Mechanisms and Vulnerabilities (MV)

The procedure to elaborate a matrix MV consists of the following steps:

1. A list between 10 and 20 factors (mechanisms and vulnerabilities), must of being internal factors to the organization in the matter of computer science security.
2. Assign a value between 0.0 (it is not important) and 1.0 (it is very important). The total of all the values must be 1.0.
3. Assign a qualification from 1 to 4 for each one of the elements of the list, 1= greater vulnerabilities, 2=smaller vulnerabilities, 3=mechanisms provides minor security, 4=mechanisms provides greater security.
4. Multiply the value by its qualification to obtain result of the factor.
5. Add the results of the factors.



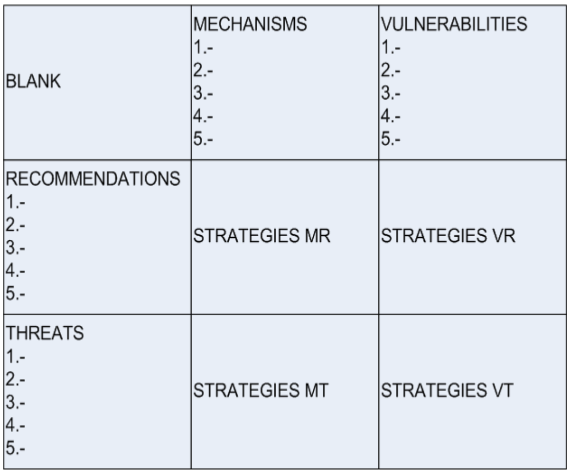
FACTORS	VALUES	CAL.	RESULTS
MECHANISMS 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
VULNERABILITIES 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
	1.00		TOTAL

Fig.5. Matrix MV.

3.3 Matrix of Vulnerabilities, Recommendations, Threats and Mechanisms (VRTM)

The procedure to elaborate the Matrix of Vulnerabilities, Recommendations, Threats and Mechanisms (VRTM) consist of the following steps:

1. Position the list of the vulnerabilities found in the corresponding square.
2. Position the list of security mechanisms whereupon it counts the company in the corresponding square.
3. Position the list of threats in the corresponding square.
4. Position the list of the recommendations or opportunities whereupon it counts the company to protect the computer science assets in the corresponding square.
5. Adapt the mechanisms to the recommendations and register the resulting strategies MR in the corresponding square (Mechanisms+ Recommendations =strategiesMR).
6. Adapt the vulnerabilities to the recommendations and register resulting strategies VR in the corresponding square (Vulnerabilities+ Recommendations = strategiesVR).
7. Adapt the mechanisms to the threats and register resulting strategies MT in the corresponding square (Mechanisms + Threats = strategiesMR).
8. Adapt the vulnerabilities to the threats and register the strategies VT resulting in the corresponding square (Vulnerabilities + Threads = strategiesVT).



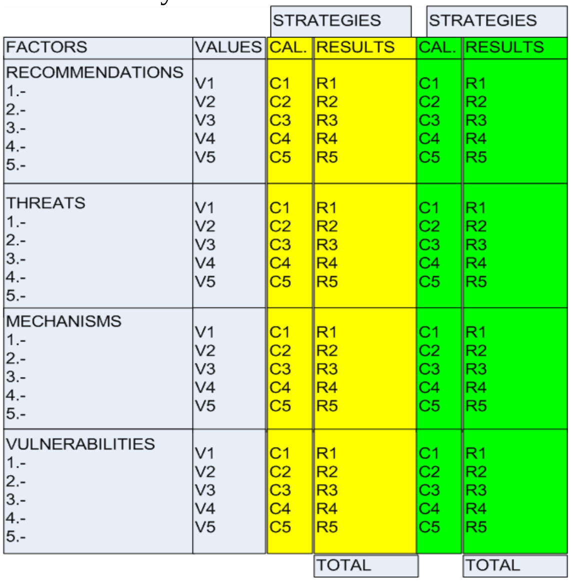
BLANK	MECHANISMS 1.- 2.- 3.- 4.- 5.-	VULNERABILITIES 1.- 2.- 3.- 4.- 5.-
RECOMMENDATIONS 1.- 2.- 3.- 4.- 5.-	STRATEGIES MR	STRATEGIES VR
THREATS 1.- 2.- 3.- 4.- 5.-	STRATEGIES MT	STRATEGIES VT

Fig.6. Matrix VRTM

3.4 Quantitative matrix of the strategic planning of the computer science security (MCPE-SI)

The procedure to elaborate matrix MCPE-SI consists of the following steps:

1. Make a list of the recommendations, threats, mechanisms and vulnerabilities, the list can be obtained from matrices MV and RT.
2. Adjudge values to each one of the factors, these are the same to the obtained ones in matrices MV and RT.
3. Analyze the strategies MR, VR, TM and VT obtained from matrix VRTM and position in the superior row of matrix MCPE-SI.
4. Determine the qualifications for each strategy, 1=Not attractive, 2=some attractive, 3=So much attractive, 4=Very attractive.
5. Calculate the result of the qualifications, multiplying the values of the weights by the qualifications.
6. Calculate the total of the sum of the results of the qualifications. The difference of totals for each one of the strategies indicates the order in that it is due to apply the strategies of computer science security.



		STRATEGIES		STRATEGIES	
FACTORS	VALUES	CAL.	RESULTS	CAL.	RESULTS
RECOMMENDATIONS 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
THREATS 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
MECHANISMS 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
VULNERABILITIES 1.- 2.- 3.- 4.- 5.-	V1 V2 V3 V4 V5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5	C1 C2 C3 C4 C5	R1 R2 R3 R4 R5
			TOTAL		TOTAL

Fig.7. Matrix MCPE-SI

4 Generic Strategies for the computer science security of Ruiz-Vanoye

As result of the strategic planning for the computer science security are the strategies to provide greater security to the organization, banking organization, company, and government. The obtained strategies can be: Update of security patches, installation of an intrusion detection system, hiring of two experts of computer science security to form the group of administrators of the computer science security.

In this paper show a generic strategies proposed that group strategies obtained of matrix MCPE-SI to provide computer science security:

1. Defensive strategies of security. They are the strategies that conforms is detected the security problem in the same way are solved one by one.

2. Aggressive strategies of security. They are those strategies that are known colloquial way like paranoiacs strategies, which are those strategies that are used when not to trust of all the computer science activities those are made in the organization. In addition to being strategies of automatic solution and counterattack in case of existing a problem of computer science security.

5 Conclusions

The use of the strategic planning in questions of computer science security is an excellent mechanism to administer aspects of security in any organization. The matrixes of the strategic planning are quantitative and high-priority mechanisms to define the actions or strategies to follow. In matrix RT and MV is recommended to obtain values superior to 2, if values smaller to 2 are obtained we considered that the company this too sensible one to problems of computer science security.

References:

[1] Fred R. David, *Conceptos de Administración estratégica*, Prentice Hall, 1997, ISBN: 968-880-796-6

[2] Smith, Allen, Stewart, and whitehouse, *Creating Strategic Vision: Long-range planning for national security*, Diane Pub Co, September 1987, ISBN-10: 0788121464

[3] Michael Allison, *Strategic Planning for Nonprofit Organizations*, Second Edition, Wiley, ISBN-10: 0471445819

[4] Graham Kenny, *Strategic Planning and Performance Management: Develop and Measure a Winning Strategy*, Butterworth-Heinemann, February 3, 2005, ISBN-10: 0750663839

[5] Hien-Chih Yu, Value Based Management and Strategic Planning in e-Business, *5th International Conference Commerce and Web Technologies (EC-Web)*, 2004, pp. 357-368

[6] M. Campos, A. Torres-Macias, Strategic Planning Process: Mexican Government and Industry Application. *32nd Annual Hawaii International Conference on System Sciences (HICSS)*, 1999

[7] Bernard Moulin, Strategic Planning for Expert Systems, *IEEE Expert* 5*(2)*, 1990, pp. 69-75

[8] Rong-Ji Bai, Gwo-Guang Lee, Organizational factors influencing the quality of the IS/IT strategic planning process, *Industrial Management and Data Systems 103(8)*, 2003, pp. 622-632

[9] Peter S. Browne, Computer security: a survey, *ACM SIGMIS*, Vol. 4, Issue 3, 1972, ISSN:0095-0033

[10] Jinx P. Walton, Developing an enterprise information security policy, *Proceedings of the 30th annual ACM SIGUCCS*, 2002, ISBN:1-58113-564-5

[11] Saad Haj Bakry, Development of security policies for private networks, *International Journal of Network Management*, Vol. 13, Issue 3, 2003, ISSN:1099-1190, pp. 203-210