Strategic Planning for the Computer Science Security

JORGE A. 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
jruizvanoye@yahoo.com.mx, http://www.ruizvanoye.com
odiazp@uaem.mx, http://www.diazparra.net

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

JUAN CARLOS OLIVARES-ROJAS[4]
[4]Informática. Instituto Tecnológico de Morelia.
Av. Tecnológico 1500, Colonia Lomas de Santiaguito, Morelia, Michoacán
MEXICO
jcolivar@itmorelia.edu.mx, http://antares.itmorelia.edu.mx/~jcolivar/

Abstract: - The necessity of the companies and organizations to adapt the technological changes of the computer science takes to formulated key questions: How to measure the security of my organization?, What type of Computer Science Security needs my company, financial organization, or government? Did my financial organization counts with aspects of computer science security in the correct areas? What new tools of computer science security exist? What security strategies we must follow? What is the data stream of information that needs to be transmitted through the different departments of my organization, in terms of computer security? What kind of users' roles exists in terms of organizational security? Is there a way to classify the information in terms of computer security? In this paper we show a methodology for strategic planning for the computer science security of diverse companies like Banks and Government, cradle in the concepts of strategic administration of enterprise politics, which tries to give answers to the questions before mentioned.

Key-Words: - Methodologies of Security, 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 administration or also well-known as strategic planning is the art or science to formulate, to implement and to evaluate the inter-functional decisions that allow the organization to reach their objectives; in other words the strategic planning is a set of actions that must be developed to obtain the strategic targets, which implies to prioritize the problems to solve, to raise solutions, to determine the people in charge to make them, to assign resource to take them to the end and to establish the form and regularity to measure the advances [1,2,3,4,5,6,7,8].

The strategic administration is applied for the big companies, but what about of the small companies? Also they use it although single it is been from the daily operations of the organization. But a problem that usually is at the time of applying strategic administration to the small businesses is the lack of capital sufficient to operate the opportunities and to defend themselves before the threats.

The formal strategic planning with its modern characteristics was introduced in some commercial companies in the middle of 1950. In 1954 Peter Drucker mentions that: "the strategy requires that the managers analyze their present situation and that they change it in necessary case, knowledge that resources has the company and which must have". In 1962 Alfred Chandler mentions that: "the element that determine the basic goals of the company, in the long term, as well as the adoption of courses of action and allocation of resources to reach the goals".

The Strategic Planning is the logical answer to the necessities of search an uncertain, complex and changing future. It is a diligent process of information compilation, to analyze it, of search the future, producing ideas and to formalize plans. It is an opportune route that follows a methodology, applies varied technical and counts on the creative analytical capacity in those who participates in the strategic planning. For example, where we are? To define the present strategic position (present positioning), To where we go? Search the future and to predict consequences (descriptive positioning), To where we would have to go? = to project to the organization with the strategic position that it must have the future (normative positioning).

The strategic planning in the world of the businesses is the plan to obtain the best yield of the resources. It is the form by means of which a corporation canalizes efforts to be different itself positively from its competitors, using its relative advantages to satisfy better its clients [19].

The Strategic Planning is a continuous process whose modifications go in direct function of the changes observed in the environmental context and closely are related to the sensitivity of external which they affect his organization[19].

The Strategic Planning prepares to the high direction to undertake changes, to take advantage of such, allows to optimize the benefits and to diminish its problems, risks and threats [21].

An effective program of planning consists of providing a guide for the executives in all the aspects of a business to make compatible decisions with the goals and strategies from high direction, understanding the concept of strategy like: the development and advantage of the internal capacity to face different challenges; like answer or anticipation to the changes of the environment; as the form to compete in the market; like the vision of long term or the challenge that turns out to ask In what place we are? And In what place we would have to be? The strategy like the bond between the objectives that are persecuted, the required programs of action and resources and what the strategy treats, which distinguishes it of all the other types of planning of the businesses is, in a word the competitive advantage, since the only intention of the strategic planning comes to be to allow that the company obtains with the greater possible efficiency a sustainable advantage on its competitors. Therefore the strategy concept has a multidimensional character [21].

The planning tries to say, What to do? How to do it? Where to do it? Who is going it to do? When to do it?, it is a process that indicates each action early or activity that is due to make.

The planning is an activity that gives the answers previously to the previous questions, related with the four basic areas of all company: production, markets, finances and this relation depend the life on the company.

The main intention of the strategic planning consists of discovering the future opportunities and dangers to elaborate plans or to operate or to avoid them.

The planning strategic process is to formulate masterful strategies and programs. The masterful strategy is defined as basic missions, intentions, objectives and policies, whereas the program strategies are related to the acquisition, use and disposition of the resources for specific projects.

The strategic planning has not been used or adapted for the computer science security to date of elaboration of this paper, which indicates that it is an excellent niche of investigation.

The strategic planning adapted in the computer science security is observed in many senses as 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 2 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 3 are quantitative tools to measure the performance of the strategy of computer science security. In Section 4 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 phases:

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.

The declaration of the security mission can vary as far as content and format, but in general it is a statement with the mission of computer science security, is important that it contains basic aspects of computer science security for the company, for example, how it is the level of computer science of the users? How they are the main applications or systems with which the users interacted? Whereupon technology of computer science security counts the organization? It is necessary to mention that the security mission does not have to contradict to the enterprise mission; one must be complement of the other with the purpose of assuring that the company counts on greater computer science security.

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, phishing, pharming, new heuristic algorithms for attacks detection and improvements for the prediction of possible computer science attacks.

In order to identify the opportunities and threats it is necessary to make audits to verify the logical and physical security of the organization, with the external audit it is possible to obtain a finite list of opportunities and threats that can repel on the organization. Towards it the organization knows and is able to respond in offensive or defensive form to the threats that appear.

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.

No company has same forces and vulnerabilities in all its areas. In order to determine the forces and vulnerabilities that exist in the matter of computer science security it is necessary to make internal audits.

The process to make an internal audit is similar to the external audit, with the only difference in which it stops to make an internal audit is required to collect, to assimilate and to evaluate data of the procedures that the members of the organization make to be able to determine that actions are making badly or good in the matter of computer science security.

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.

In addition to the writing of the mission of computer science security, it is necessary to define objective to long, medium and short term in the matter of computer science security.

The objectives can be defined as the results of computer science protection that it tries to reach an organization by means of the fulfillment of his mission of security. The security objectives must be reasonable, consistent and clear; can be to short, medium and long term.

The last element of this phase is the policies of computer science security; the policies are the average ones to fulfill the objectives of short, medium and long term.

The policies of computer science security must contain the established rules to reinforce the activities to effect to reach the defined objectives of security.

The policies of computer science security must be created for each computer science assets of the company, and must contain rules for the users of the information and the people in charge to administer the information of the organization.

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

The generation of strategies would be incomplete if the strategies are not implemented, is to say the organization after it establishes the objectives, and creates security policies.

It is necessary to develop a culture that maintains the strategy in the organization; some times the employees of the organization are customary to diminish excellent aspects for the computer science security generally.

The change of mentality is very difficult for some employees, reason for which the implementation of the policies and objectives of security of the organization must of being established by means of an effective and effective organizational procedure.

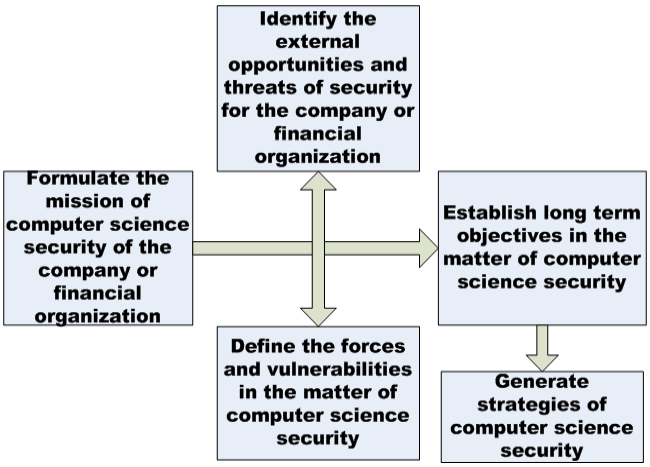

Fig.1 Strategic formulation of the computer science security

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.

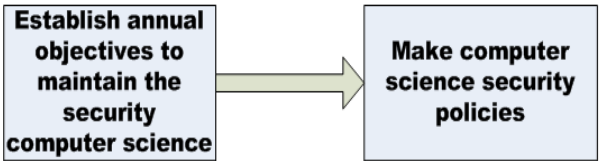

Fig. 2 Implement the strategy of computer science security.

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.

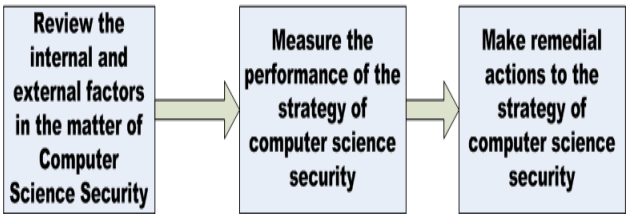

Fig.3 Evaluation of the strategy of computer science security.

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

The obtained total value for each strategy will determine the order whereupon the activities related to the strategy will be made.

For example, if two strategies with total value of 2 and 1.3 exist, the first strategy that will be due to make is the strategy with greater value.

3.5 Indicators of the computer science security

The determination of the threat and the risk is within a specialized field, and you can be that it is necessary a consultant of the security or a specialist of the risk to determine the diverse aspects of the security.

But, the next security indicator of computer science was created to measure the security (or insecurity) degree that has the organization or company. We propose an indicator of the risk of the security (equation 1).

$$Risk = MatrixRT.T + MatrixMV.T \quad (1)$$

Where *MatrixRT.T* is the total value obtained in the Matrix of Recommendations and Threads, *MatrixMV.T* is the total value obtained in the Matrix of Mechanisms and Vulnerabilities. The risk balances the total danger that a particular threat raises with the security mechanisms of the company.

In other words, the that we propose to measure the whichever security has a company this given based on the obtained value of the risk to which this exposed the company

Later altogether with the indicator of Risk another indicator of prioritization will be used, the indicator will have to use the value obtained in the Risk indicator and to multiply it against the value of the assets, with the purpose of being able to have another mechanism to measure the degree of security and importance of the assets (information, server and network problems costs or active cost) to be able to make the corresponding decisions (equation 2).

$$\Pr ioritization = Risk * active\cos t \quad (2)$$

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.

For example, the establishment of policies of security focused to prevent infections with virus, and the use non-adapted of the technologies of the information.

In addition to qualification on the suitable use of the technologies of the information in the matter of computer science security, distribution of information updated with respect to security problems that could damage the information of the company.

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.

For example, avoiding of automatic way the uses of certain activities through Internet, supervising with detectors of intruders to the company, to act of automatic way detects of internal or external intruder and to counterattack to protect the information of the company; to have an expert in computer science security able to defend with the attack to the information of the company, to mention some examples.

5 Roles of the computer science security managers

The computer systems' data are in latent danger for many and various reasons: user's mistakes or intentional and fortuities attacks. Unintentional accidents could happen, causing that some persons could try to attack the system in advantage to access it and interrupt the running services, cripple the systems or modify, delete or stole the company's information.

5.1 Managers of the computer science security

It is really important that the company recruit a group of computer security experts, it could be a group or even only one person dedicated only and exclusively to manage the company's computer science security.

The administrators must count on ethics in the matter of computer science security.

The ethics can be defined as the principles of conduct of the security administrators and serve as guide for the decision making of the administrators.

The ethics of the computer science security does not only apply to the administrators of the security, must apply for all the elements of the organization.

The ethics code can serve as base to elaborate political of security that will serve as guide for the conduct and the decisions within the organization.

5.2 Confidential information for the managers of computer science security

It is also important to avoid that, without authorization, the security's responsible get access, use or modify, in order to affect others, confidential personal or familiar information from others that could be found in the company's files or any other computer or electronic support or in any other files or public or private registries.

Also, it is necessary to avoid that the information reveals ideologist postures, religious or personal beliefs, health status, race or sexual preferences; the managers of computer science security don't get it with profit intentions and using any informatics trick or social manipulation, someone gets a non-authorized transaction of any confidential company's patrimonial active, in order to harm others, caused by any mean, virus infection or another way that can destroy, modify, stop or cause any kind of damage to the data, software, electronic files or databases.

6 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.

It is necessary to consider that the security depends on the grade of paranoia we have, i.e. the more security we want, the more we need to wary anyone and anything, and ask ourselves if the used security technologies are providing us the necessary protection [12].

Also it is recommendable which the security audit that is made to the company was realized by experts in the area and not by those companies that single makes an analysis of detection of open ports and lack of updates to the operating systems.

And within the company to have experts in administration of the information technologies on which it counts the company, that only this dedicating to solve problems of computer science security, that tells on ethics, that knows the value of the information of the company.

In order to conclude we think that the use of the strategic planning in the area of computer science security will be used for the manager decision making within the company with the purpose of safeguard the information and the prestige of her. And non-single to give a false sense of security but to approach standards of security on which it can count the company.

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.

[12] Ruiz-Vanoye J.A., Díaz-Parra O., Fuentes Penna A., Ceyca Castro J.O., Olivares-Rojas J.C., An Alternative Solution Initiative to problematic of computer science security of virus and malware with experimentation of firewalls and antivirus. *The Second International Multi-Conference on Computing in the Global Information Technology* (*ICCGI*), IEEE Computer Society, 2007, pp 34, ISBN: 0-7695-2798-1.

[13] Antiphising Working Group. *Crimeware Taxonomy & Samples According to classification in June 2006*. Phishing Activity Trends Report July. 2006.

[14] Escamilla T., *Intrusion Detection: Network Security beyond the firewall*. John Wiley and Sons, Inc. 1998.

[15] ISO/IEC. *Engineering Capability Maturity Model* (*SSECMM*). ISO/IEC 21827. Information Technology System Security.

[16] U.S. Commerce Departament. *National Vulnerability Database*. http://nvd.nist.gov.

[17] Tang Y. and Chen S. Defending against internet worms: a signature-based approach. *Proceedings of the 24th Annual Joint Conference of IEEE Computer and Communication societies* (*INFOCOM*), 2005.

[18] Hispasec Sistemas. *Virus Total*. http://www.virustotal.com.

[19] King W.R. and Cleland D.I., *Strategic Planning and Policy*, New York, Van Nostrand Reinhold, 1979.

[20] Pearce J. and David F., *Corporate mission statements: The Bottom line*, Academy of management Executive 1, N. 2, 1987.

[21] Steiner G., *Strategic Planning: What every manager must know*, New York, the Free press, 1979.

[22] McGinnis V., *The mission statement: A key step in Strategic Planning*, Business 31, N.6, 1981.

[23] Porter M., *Competitive Strategy: Techniques for Analyzing industries and companies*, New York, Free Press, 1980.

[24] Gellerman S., *Managing Ethics from the Top Down, Sloan Management Review*, 1989.

[25] D Gollmann: *Computer security*, John Wiley & Sons, Inc. New York, NY, USA 1999.

[26] DD Clark, DR Wilson: *A Comparison of Commercial and Military Computer Security Policies*, IEEE Symposium on Security and Privacy, Oakland, CA p. 184, 1987.

[27] EG Amoroso: *Fundamentals of computer security technology*, Prentice-Hall, Inc. Upper Saddle River, NJ, USA, 1994.

[28] L. A. Gordon, M. P. Loeb, W. Lucyshyn, R. Richardson: *CSI/FBI Computer Crime and Security Survey*, Computer Security Institute CSI, 2005.

[29] M. A. Bishop: *Computer Security: Art and Science*, ISBN 0201440997, Addison-Wesley 2003.

[30] N. Doraswamy, D. Harkins: *IPSec: The New Security Standard for the Internet, Intranets,*

and Virtual Private Networks, ISBN 013046189X, Prentice Hall, 2003.
[31] U. Lindqvist, E. Jonsson: *How to Systematically Classify Computer Security Intrusions*, IEEE Symposium on Security and Privacy, 1999.
[32] E. Casey: *Digital Evidence and Computer Crime*, ISBN 0121631044, Academic Press 2004.
[33] R. J. Anderson: *Security Engineering: A Guide to Building Dependable Distributed Systems*, ISBN 0-4071-38922-6, Wiley 2001.
[34] R Panko: *Corporate Computer and Network Security*, Prentice-Hall, Inc. Upper Saddle River, NJ, USA, 2003.
[35] B. W. Lampson: *Computer security in the real world*, Computer Vol. 37, Issue 6, pps. 37-46, ISSN 0018-9162, IEEE, 2004.
[36] M. Bishop: W*hat is computer security?* Security & Privacy Vol. 1 Issue 1, pps. 67-69, ISSN 1540-7993, IEEE, 2003.
[37] S. Bosworth, M. Kabay, M. E. Kabay: *Computer Security Handbook*, John Wiley & Sons, Inc. New York, NY, USA, 2002.
[38] J. Pieprzyk, J. Seberry: *Fundamentals of Computer Security*, ISBN 35404301012, Springer 2003.
[39] K. J. Soo Hoo: *How Much is Enough? A Risk-Management Approach to Computer Security*, Consortium for Research on Information Security and Policy (CRISP), CISAC, 2000.
[40] R. Anderson: *Why Information Security is Hard-An Economic Perspective*, 17th Annual Computer Security Applications Conference (ACSAC'01), IEEE, 2001.
[41] T. Bernstein, A. B. Bhimani, E. Schultz, C. A. Siegel: *Internet Security for Business*, ISBN 0471137529, John Wiley & Sons, 1996.
[42] L. A. Gordon, M. P. Loeb, W. Lucyshyn: *Sharing information on computer systems security: An economic analysis*, Journal of Acounting and Public Policy, Vol. 22 Issue 6, pps. 461-485, Elsevier, 2003.
[43] A. Nash, W. Duane, C. Joseph: *PKI: Implementing and Managing E-Security*, McGraw-Hill, Inc. New York, NY, USA, 2001.