© International Journal of Combinatorial Optimization Problems and Informatics, Vol. 5, No. 2, May-Aug 2014, pp. 2-28. ISSN: 2007-1558.

Strategic Planning for the Computer Security: A Practice Case of an Electrical Research Institute

Jorge A. Ruiz-Vanoye[1], Ocotlán Díaz-Parra[1]
Ana Canepa Saénz [1], Ricardo A. Barrera-Cámara[1]
Alejandro Fuentes-Penna [2] Beatriz Bernabe-Loranca [3]
[1] Universidad Autónoma del Carmen, México
[2] Universidad Autónoma del Estado de Hidalgo, México
[3] Benemérita Universidad Autónoma de Puebla, México

We show a practice case of strategic planning for the computer science security based on the concepts of strategic administration of enterprise politics. The practice case of the computer science security shows information about an Electric Research Institute of Mexican Government. The Electric Research Institute is a public enterprise dedicated to innovation, technological development and applied scientific research, in order to develop technologies applicable to the electrical and oil industries, providing support to the Energy Sector in electrical generation, transmission and distribution processes and improvement oil processes.

Keywords: Computer Science Security, Strategic Planning, Electrical Research.

1. INTRODUCTION

The strategic planning could be seem like a 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 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].

Received Nov 20, 2013 / Accepted Dec 19, 2013

In this paper, we show a practice case (about an Electric Research institute of Mexican government) of strategic planning for the computer science security based on the concepts of strategic administration of enterprise politics. 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 organizations, attackers or competitors; if the computer science security strategy is not effective, then nor all the efficiency of the world will be enough to provide a good security.

The practice case of the computer science security shows information about an Electric Research Institute of Mexican government [24]. The Electric Research Institute is a public enterprise dedicated to innovation, technological development and applied scientific research, in order to develop technologies applicable to the electrical and oil industries, providing support to the Energy Sector in electrical generation, transmission and distribution processes and improvement oil processes. The Electric Research Institute was created by Presidential Decree on behalf of the Mexican Government on the first of December, 1975, as a decentralized organization with its own legal identity and patrimony, whose assignment was scientific and technical in nature. Its main objectives are to carry out innovation, technological research and development; to provide engineering and technical services, training, and the commercialization of the results of research and technological development in electrical generation, transmission and distribution processes and improvement oil processes. The Institute is backed up by an organizational structure that enables it to perform and accomplish its purpose, which is to contribute to technological innovation, scientific research and development of the energy sector. The Institute strives to strengthen technological institutions and channel

their efforts in the fields of processes, equipment and systems in order to increase competitiveness in the electric power and energy sectors, not just in Mexico but abroad as well.

In section 2 will be comment the related works and the matrixes of the computer science security and in section 3 is a practice case of strategic planning for the computer science security.

2. RELATED WORKS

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 analyse their present situation and that they change it in necessary case, knowledge that resources has the company and which must have" [11]. In 1962 Alfred Chandler mentions it as: "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" [12].

The strategic planning adapted in the computer science security [9] was observed in many senses as a military strategy, which take advantage of their forces to operate the vulnerabilities of the competitors or attackers; if the computer science security strategy is not effective, then nor all the efficiency of the world will be enough to provide a good security. Ruiz-Vanoye et al. [9] proposed the strategic planning for the computer science security: a) Strategic Formulation of Computer Science Security. b) Implement the Strategy of Computer Science Security c) Evaluation of the Strategy of Computer Science Security. In this paper, we show a practice case of strategic planning for the computer science security.

The strategic planning was applied to a SMES [21, 22] and Banks [23], but it wasn't applied to an electrical research institute.

3. METHODOLOGY FOR THE STRATEGIC PLANNING FOR THE COMPUTER SECURITY FOR AN ELECTRICAL RESEARCH INSTITUTE

The Strategic formulation of computer science security consists of formulating the mission, identifying the external opportunities and threats, define the forces and vulnerabilities, establishing long term objectives and generate strategies in the computer science security. The methodology used in the practical case consists of the following steps [9]:

(1) Formulating 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) Identifying the external recommendations and threats of security to 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

(3) Define the mechanisms and vulnerabilities in the computer science security. There are those activities that can control the organization at diverse levels. The errors in the network devices configurations, they don't have an intrusion

detection system, or neither have an expert in computer science security within the organization.

(4) Establishing long term objectives and generate strategies of computer science security. To indicate the bases to plan and to motivate with effectiveness the use of the computer science security in the organization. Objectives for the complete organizational and each one of the divisions are due to establish.

(5) Implement the strategy of computer science security. To elaborate a Quantitative Strategic Planning Matrix (QSPM) for Computer Science Security (CSS) or QSPM-CSS. QSPM-CSS is based in the Quantitative Strategic Planning Matrix (QSPM). QSPM is a high-level strategic management approach for evaluating possible strategies. QSPM provides an analytical method for comparing feasible alternative actions.

(6) To 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.

(7) Devise policies of computer science security. They are procedures and established rules to maintain the computer science security in the organization, serve to reach the annual objectives.

(8) Evaluation of the strategy of computer science security. Review the internal and external factors, verify the existing security, technologies and mechanisms on which at the moment the organization counts, measure the performance strategy, take remedial actions, and modify the strategies in the matter of Computer Science Security.

4. EXPERIMENTATION AND RESULTS

In the experimentation, we apply the concepts of Strategic Planning for Computer Science Security, and the techniques of Web engineering to generate a solution that allows Electrical Research Institute make decisions regarding computer security. To develop a web application for strategic planning of computer security of the Electrical Research Institute, we use Microsoft C # (ASP net) contained in Visual Studio 2012, a server with Microsoft Windows with Internet Information Server and SQL Server. The steps contained in the web application are:

(1) Formulate the mission of computer science security. To promote and to support the innovation by means of the computer science security with high added value to increase to the competitiveness of the electrical industry and other industries with compatible needs.

(2) Identify the external recommendations and threats of security: The list of recommendations for the Institute is:

- Firewalls: Firewalls determine whether data packets are permitted into a network, and they restrict access to specific resources. See NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy [13].
- Intrusion Detection: An intrusion detection system (IDS) detects security breaches by looking for anomalies in normal activities, by looking for patterns of activity that are associated with intrusions or insider misuse, or

both. See NIST Special Publication 800-31, Intrusion Detection Systems (IDS) [14].

- Auditing: Install or configure mechanisms to record activities occurring across the interconnection, including application processes and user activities.
- Identification and Authentication: Identification and authentication is used to prevent unauthorized personnel from entering an IT system. If digital signatures are used, the technology must conform to Federal Information Processing Standard (FIPS) 186-2, Digital Signature Standard (DSS) [15].
- Logical Access Controls: Logical access controls are mechanisms used to designate users who have access to system resources and the types of transactions and functions they are permitted to perform. See NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems [16].
- Virus Scanning: Data and information that pass from one IT system to the other should be scanned with antivirus software to detect and eliminate malicious code, including viruses, worms, and Trojan horses.
- Encryption: Encryption is used to ensure that data cannot be read or modified by unauthorized users. When used properly, encryption will protect the confidentiality and integrity of data during transmission and storage, and it may be used for authentication and nonrepudiation. Encryption may be implemented in devices such as routers, switches, firewalls, servers, and computer workstations.
- Physical and Environmental Security: Physical security addresses the physical protection of computer hardware and software. Place hardware and

software supporting the interconnection, including interconnection points, in a secure location that is protected from unauthorized access, interference, or damage. Ensure that environmental controls are in place to protect against hazards such as fire, water, and excessive heat and humidity. In addition, place computer workstations in secure areas to protect them from damage, loss, theft, or unauthorized physical access. For guidance, see the following NIST Special Publications: 800-12, An Introduction to Computer Security: The NIST Handbook, 800-30 [17, 18, 19].

The list of threats for the Institute is:

- Denial of Service (DoS). An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
- Malicious Code. A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
- Unauthorized Access. A person gains logical or physical access without permission to a network, system, application, data, or other IT resource.
- Inappropriate Usage. A person violates acceptable use of any network or computer policies.
- Multiple Components. A single incident that encompasses two or more incidents; for example, a malicious code infection leads to unauthorized access to a host, which is then used to gain unauthorized access to additional hosts.

Once identified the recommendations and threats, it's necessary to make a Matrix of recommendations and threats (RT) for the Electric Research Institute of Mexican Government. RT is based in the External Factor Evaluation (EFE) matrix method, EFE is a strategic-management tool often used for assessment of current business conditions. The procedure to elaborate a RT matrix (Table 1) consists of the following steps [9]:

a) A list between 10 and 20 factors (recommendations and threats), must be conformed by external factors to the organization in the matter of computer science security.

b) Assign a value between 0.0 (it is not imp)ortant) 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

c) Assign a qualification (Q) 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, 2 = Answer average 1 = Answer badly.

d) Multiply the value by its qualification to obtain result of the factor.

e) Add the results of the factors.

Table 1. RT Matrix

Factors	Values	Q	Results
Recommendations			
1.-Firewalls	0.20	4	0.80
2.-Intrusion Detection	0.15	1	0.15
3.-Identification and Authentication	0.05	2	0.10
4.-Virus Scanning	0.06	4	0.24
5.-Physical and Environmental Security	0.04	2	0.08
Threats			
1.-Denial of Service	0.15	2	0.30

2.-Malicious Code	0.06	3	0.18
3.-Unauthorized Access	0.20	2	0.40
4.-Inappropriate Usage	0.05	2	0.10
5.-Multiple Components	0.04	2	0.08
	1.00		2.43

In Table 1, it can observe the RT Matrix for the institute of electrical research, the result of 2.43 mentions that the institute counts on basic elements to protect itself of threats. The ranks of values allowed for RT matrix are: a) 0-2: the institute is vulnerable of threats, b) 2-3: the institute counts on basic elements of security, c) 3-4: the institute is not vulnerable of threats.

(3) Define the mechanisms and vulnerabilities in the computer science security. The areas of security for mechanisms and vulnerabilities are:

- Access Control (Access Control Policy and Procedures, Account Management, Access Enforcement, Information Flow Enforcement, Separation of Duties, Least Privilege, Unsuccessful Login Attempts, System Use Notification, Previous Logon Notification, Concurrent Session Control, Session Lock, Session Termination, Supervision and Review—Access Control, Permitted Actions without Identification or Authentication, Automated Marking, Automated Labeling, Remote Access, Wireless Access Restrictions, Access Control for Portable and Mobile Devices, Use of External Information Systems).
- Awareness and Training (Security Awareness and Training Policy and Procedures, Security Awareness, Security Training, Security Training Records, Contacts with Security Groups and Associations).
- Audit and Accountability (Audit and Accountability Policy and Procedures, Auditable Events, Content of Audit Records, Audit Storage Capacity,

Response to Audit Processing Failures, Audit Monitoring, Analysis, and Reporting, Audit Reduction and Report Generation, Time Stamps, Protection of Audit Information, Non-repudiation, Audit Record Retention).

- Certification, Accreditation, and Security Assessments (Certification, Accreditation, and Security, Assessment Policies and Procedures, Security Assessments, Information System Connections, Security Certification, Plan of Action and Milestones, Security Accreditation, Continuous Monitoring).
- Configuration Management (Configuration Management Policy and Procedures, Baseline Configuration, Configuration Change Control, Monitoring Configuration Changes, Access Restrictions for Change, Configuration Settings, Least Functionality, Information System Component Inventory).
- Contingency Planning (Contingency Planning Policy and Procedures, Contingency Plan, Contingency Training, Contingency Plan Testing and Exercises, Contingency Plan Update, Alternate Storage Site, Alternate Processing Site, Telecommunications Services, Information System Backup, Information System Recovery and Reconstitution).
- Identification and Authentication (Identification and Authentication Policy and Procedures, User Identification and Authentication, Device Identification and Authentication, Identifier Management, Authenticator Management, Authenticator Feedback, Cryptographic Module Authentication).
- Incident Response (Incident Response Policy and Procedures, Incident Response Training, Incident Response Testing and Exercises, Incident

Handling, Incident Monitoring, Incident Reporting, Incident Response Assistance).

- Maintenance (System Maintenance Policy and Procedures, Controlled Maintenance, Maintenance Tools, Remote Maintenance, Maintenance Personnel, Timely Maintenance).
- Media Protection (Media Protection Policy and Procedures, Media Access, Media Labeling, Media Storage, Media Transport, Media Sanitization and Disposal).
- Physical and Environmental Protection (Physical and Environmental Protection Policy and Procedures, Physical Access Authorizations, Physical Access Control, Access Control for Transmission Medium, Access Control for Display Medium, Monitoring Physical Access, Visitor Control, Access Records, Power Equipment and Power Cabling, Emergency Shutoff, Emergency Power, Emergency Lighting, Fire Protection, Temperature and Humidity Controls, Water Damage Protection, Delivery and Removal, Alternate Work Site, Location of Information System Components, Information Leakage).
- Planning (Security Planning Policy and Procedures, System Security Plan, System Security Plan Update, Rules of Behavior, Privacy Impact Assessment, Security-Related Activity Planning).
- Personnel Security (Personnel Security Policy and Procedures, Position Categorization, Personnel Screening, Personnel Termination, Personnel Transfer, Access Agreements, Third-Party Personnel Security, Personnel Sanctions).

- Risk Assessment (Risk Assessment Policy and Procedures, Security Categorization, Risk Assessment, Risk Assessment Update, Vulnerability Scanning).
- System and Services Acquisition (System and Services Acquisition Policy and Procedures, Allocation of Resources, Life Cycle Support, Acquisitions, Information System Documentation, Software Usage Restrictions, User Installed Software, Security Engineering Principles, External Information System Services, Developer Configuration Management, Developer Security Testing).
- System and Communications Protection (System and Communications Protection Policy and Procedures, Application Partitioning, Security Function Isolation, Denial of Service Protection, Resource Priority, Boundary Protection, Transmission Integrity, Transmission Confidentiality, Network Disconnect, Trusted Path, Cryptographic Key Establishment and Management, Use of Cryptography, Public Access Protections, Collaborative Computing, Transmission of Security Parameters, Public Key Infrastructure Certificates, Mobile Code, Voice Over Internet Protocol, Secure Name /Address Resolution Service (Authoritative Source), Secure Name /Address Resolution Service (Recursive or Caching Resolver), Architecture and Provisioning for Name/Address Resolution Service, Session Authenticity).
- System and Information Integrity (System and Information Integrity Policy and Procedures, Flaw Remediation, Malicious Code Protection, Information System Monitoring Tools and Techniques, Security Alerts and Advisories, Security Functionality Verification, Software and Information Integrity,

Spam Protection, Information Input Restrictions, Information Accuracy, Completeness, Validity, and Authenticity, Error Handling, Information Output Handling and Retention).

Once identified the mechanisms and vulnerabilities, it's necessary to make a Matrix of Mechanism and Vulnerabilities (MV) for the Electric Research Institute of Mexican Government. MV is based in the Internal Factor Evaluation (IFE) matrix, IFE is a strategic management tool for auditing or evaluating major strengths and weaknesses in functional areas of a business.

The procedure to elaborate a MV matrix (Table 2) consists of the following steps [9]:

a) A list between 10 and 20 (it could be less) factors (mechanisms and vulnerabilities), must be conformed by internal factors to the organization in the matter of computer science security.

b) 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.

c) Assign a qualification (Q) 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.

d) Multiply the value by its qualification to obtain result of the factor.

e) Add the results of the factors.

In Table 2, it can observe the MV Matrix for the institute of electrical research, the result of 2.51 mentions that the institute counts on basic mechanisms to

protect itself of vulnerabilities. The ranks of values allowed for this matrix are: a) 0-2: the institute is vulnerable, b) 2-3: the institute counts on basic mechanisms of security, c) 3-4: the institute is not vulnerable.

Table 2 MV Matrix

Factors	Values	Q	Results
Mechanisms			
1.-The organization develops, disseminates, and periodically reviews/updates a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	0.20	4	0.80
2.-The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts at least annually.	0.09	3	0.27
3.-The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy	0.07	3	0.21
4.- The information system implements spam protection.	0.15	4	0.60
Vulnerabilities			
1.-The organization doesn't employ automated mechanisms to support the management of information system accounts.	0.20	1	0.20
2.-The organization doesn't develop and documents security awareness and training policy and procedures.	0.08	2	0.16
3.-The organization don't disseminates contingency planning policy and procedures to appropriate elements within the organization	0.15	1	0.15
4.-The organization doesn't obtain alternate telecommunications services that do not share a single point of failure with primary telecommunications services.	0.06	2	0.12
	1.00		2.51

(4) Establishing long term objectives and generate strategies of computer science security. In order to establish the objectives it is necessary to elaborate a Matrix of Vulnerabilities, Recommendations, Threats and Mechanisms (VRTM) is based in the SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis, method, or model. SWOT is a way to analyze competitive position of the company.

VRTM matrix (Table 3) consists of the following steps [9]:

a) Position the list of the vulnerabilities found in the corresponding square.

b) Position the list of security mechanisms whereupon it counts the company in the corresponding square.

c) Position the list of threats in the corresponding square.

d) Position the list of the recommendations or opportunities whereupon it counts the company to protect the computer science assets in the corresponding square.

e) Adapt the mechanisms to the recommendations and register the resulting MR strategies in the corresponding square (*Mechanisms* + *Recommendations* = *strategiesMR*).

f) Adapt the vulnerabilities to the recommendations and register resulting VR strategies in the corresponding square (*Vulnerabilities* + *Recommendations* = *strategiesVR*).

g) Adapt the mechanisms to the threats and register resulting MT strategies in the corresponding square (*Mechanisms* + *Threats* = *strategiesMR*).

h) Adapt the vulnerabilities to the threats and register the VT strategies resulting in the corresponding square (*Vulnerabilities* + *Threads* = *strategiesVT*).

Table 3. VRTM Matrix

	Mechanisms M1 M2 M3 M4	*Vulnerabilities* V1 V2 V3 V4
Recommendations R1 R2 R3 R4 R5	***Strategies MR*** (R1,M1,M3)It enforces assigned authorizations for controlling the firewall in accordance with applicable policy. (R2,R3,M1,M2)It enforces assigned authorizations for the intrusion detection in accordance with applicable policy.	***Strategies VR*** (R4,V1)To automate the verification of virus in all the computers of the institute.

Threats	***Strategies MT***	***Strategies VT***
T1 T2 T3 T4 T5	(T2, M4)To buy anti-spyware for the computers of the institute. (T1)The institute does not count on necessary mechanisms. to create access control lists (ACL) in the peripheral devices (switches, AP, firewalls).	(T4,V2) It's necessary to training the personal on aspects of computer science security. (T1,V3,V4)To create a plan of contingency in case of a denial of service.

Where: R1 = Firewalls. R2 = Intrusion Detection. R3 = Identification and Authentication. R4 = Virus Scanning. R5 = Physical and Environmental Security. T1 = Denial of Service. T2 = Malicious Code. T3 = Unauthorized Access. T4 = Inappropriate Usage. T5 = Multiple Components. M1 = The organization develops, disseminates, and periodically reviews/updates a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. M2 = the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts at least annually. M3 = the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. M4 = the information system implements spam protection. V1 = the organization doesn't employ automated mechanisms to support the management of information system accounts. V2 = the organization doesn't develop and documents security awareness and training policy and procedures. V3 = the organization don't disseminates contingency planning policy and procedures to appropriate elements within the organization. V4 = the organization doesn't obtain alternate telecommunications services that do not share a single point of failure with primary telecommunications services.

(5) Implement the strategy of computer science security. In order to generate the order in which the security strategies will be realized must elaborate a Quantitative Strategic Planning Matrix for Computer Science Security (QSPM-CSS).

The procedure to elaborate QSPM-CSS (Table 4) consists of the following steps [9]:

a) Make a list of the recommendations, threats, mechanisms and vulnerabilities, the list can be obtained from MV and RT matrices.

b) Adjudge values to each one of the factors, these are the same to the obtained ones in MV and RT matrices.

c) Analyze the MR, VR, TM and VT strategies obtained from VRTM matrix and position in the superior row of QSPM-CSS.

d) Determine the qualifications (Q) for each strategy, 1 = Not attractive, 2 = some attractive, 3 = So much attractive, 4 = Very attractive.

e) Calculate the result of the qualifications, multiplying the values of the weights by the qualifications.

f) 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.

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 strategy that will be due to make is the one with greater value.

The Table 4 shows the Quantitative Strategic Planning Matrix for Computer Science Security (QSPM-CSS), where: R = Recommendations, T = Threats, M =

Mechanisms, V = Vulnerabilities, S = Strategies. R1 = Firewalls. R2 = Intrusion Detection. R3 = Identification and Authentication. R4 = Virus Scanning. R5 = Physical and Environmental Security. T1 = Denial of Service. T2 = Malicious Code. T3 = Unauthorized Access. T4 = Inappropriate Usage. T5 = Multiple Components. M1 = The organization develops, disseminates, and periodically reviews/updates a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. M2 = the organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts at least annually. M3 = the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. M4 = the information system implements spam protection. V1 = the organization doesn't employ automated mechanisms to support the management of information system accounts. V2 = the organization doesn't develop and documents security awareness and training policy and procedures. V3 = the organization don't disseminates contingency planning policy and procedures to appropriate elements within the organization. V4 = the organization doesn't obtain alternate telecommunications services that do not share a single point of failure with primary telecommunications services. Re = results. Va = Values. F = Factors. Q = Qualifications. S1 = It enforces assigned authorizations for controlling the firewall in accordance with applicable policy. S2 = It enforces assigned authorizations for the intrusion detection in accordance with applicable policy. S3 = to buy anti-spyware for the computers of the institute. S4 = the institute does not count on necessary mechanisms. to create access control lists (ACL) in the peripheral devices (switches, AP, firewalls). S5 = to automate the verification of virus in all the computers of the

institute. S6 = It's necessary to training the personal on aspects of computer science security. S7 = To create a plan of contingency in case of a denial of service.

Table 4. Quantitative Strategic Planning Matrix for Computer Science Security (QSPM-CSS)

		S1		**S2**		**S3**		**S4**		**S5**		**S6**		**S7**	
F	**Va**	**Q**	**Re**	**Q**	**Re**	**Q**	**Re**	**Q**	**Re**	**Q**	**Re**	**Q**	**Re**	**Q**	**Re**
R1	0.20	4	0.80	2	0.40	2	0.40	3	0.60	2	0.40	2	0.40	2	0.40
R2	0.15	2	0.30	4	0.60	2	0.30	2	0.30	1	0.15	1	0.15	1	0.15
R3	0.05	3	0.15	3	0.15	1	0.05	4	0.20	1	0.05	1	0.05	1	0.05
R4	0.06	1	0.06	1	0.06	3	0.18	1	0.06	4	0.24	1	0.06	1	0.06
R5	0.04	1	0.04	1	0.04	1	0.04	1	0.04	1	0.04	3	0.12	1	0.04
T1	0.15	3	0.45	4	0.60	1	0.15	2	0.30	1	0.15	1	0.15	4	0.60
T2	0.06	1	0.06	1	0.06	3	0.18	1	0.06	4	0.24	1	0.06	1	0.06
T3	0.20	3	0.60	3	0.60	1	0.20	4	0.80	1	0.20	1	0.20	1	0.20
T4	0.05	1	0.05	1	0.05	1	0.05	1	0.05	1	0.05	4	0.20	1	0.05
T5	0.04	1	0.04	1	0.04	4	0.16	1	0.04	4	0.16	1	0.04	1	0.04
M1	0.20	1	0.20	1	0.20	1	0.20	4	0.80	1	0.20	1	0.20	3	0.60
M2	0.09	1	0.09	4	0.36	1	0.09	1	0.09	1	0.09	1	0.09	3	0.27
M3	0.07	1	0.07	1	0.07	1	0.07	4	0.28	1	0.07	1	0.07	1	0.07
M4	0.15	1	0.15	1	0.15	3	0.45	1	0.15	4	0.60	1	0.15	1	0.15
V1	0.20	1	0.20	1	0.20	1	0.20	1	0.20	1	0.20	3	0.60	1	0.20
V2	0.08	1	0.08	1	0.08	1	0.08	1	0.08	1	0.08	3	0.24	1	0.08
V3	0.15	1	0.15	1	0.15	1	0.15	1	0.15	1	0.15	3	0.45	2	0.30
V4	0.06	2	0.12	1	0.06	1	0.06	3	0.18	1	0.06	1	0.06	4	0.24
			3.61		3.83		3.01		4.38		3.13		3.29		3.56

The order in which the strategies were elaborated is:

- (S4) The institute does not count on necessary mechanisms. To create access control lists (ACL) in the peripheral devices (switches, AP, firewalls).

- (S2) It enforces assigned authorizations for the intrusion detection in accordance with applicable policy.
- (S1) It enforces assigned authorizations for controlling the firewall in accordance with applicable policy.
- (S7) To create a plan of contingency in case of a denial of service.
- (S6) It's necessary to training the personal on aspects of computer science security.
- (S5) To automate the verification of virus in all the computers of the institute.
- (S3) To buy anti-spyware for the computers of the institute.

(6) To establish annual objectives to maintain the security computer science. The objectives for the Electric Research Institute of Mexican Government are:

- To contribute to the diffusion and implantation, within the electrical industry, of those security technologies that better adapt to the economic development of the country.
- To maintain effective relations with similar institutions of other countries and academic institutes.
- To distribute update and specialization courses of knowledge in science, technology and industrial administration in the area of computer science security for the electrical industry.
- To offer consultant's office to the Federal Commission of Electricity (FCE), to the industry of electrical manufactures and the companies of engineering and consulting services related to the electrical industry.

- To propose to the Secretariat of Energy and to the FCE, applied and technological research programs for computer science security, and the corresponding plans of operation, investment and short, medium financing to and long term.
- To patent and to license the developed technologies and the results of the investigation that it obtains and that is originating.

(7) Devise policies of computer science security. It is necessary to realize the following policies of security and plans for the Electric Research Institute of Mexican Government are:

- Policy of security for the creation of access control lists.
- Plan of contingency in case of disasters.
- Plan of recovery in case of denial of service.
- Policy of security for the suitable use of institutional the computer science resources.
- Plan and calendar of qualification of basic aspects of security for the personnel of the institute.
- Plan and calendar for the acquisition and installation of anti-spyware software.
- Policy of security for the use of the electronic mail.
- Policy of security for the suitable use of Internet and Internet 2.

(8) Evaluation of the strategy of computer science security. It is necessary to do every 6 months the following thing: Evaluation of the Strategy of Computer

Science Security, review the internal and external factors in the matter of Computer Science Security, measure the performance strategy of the computer science security and take remedial actions to the strategy of computer science security.

5. CONCLUSIONS

We show a practice case of strategic planning for the computer science security based on the concepts of strategic administration of enterprise politics and web engineering. The practice case of the computer science security shows information about an Electric Research Institute of Mexican Government. 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 RT and MV matrixes are 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.

The objectives for the Electric Research Institute of Mexican Government are: To contribute to the diffusion and implantation, within the electrical industry, of those security technologies that better adapt to the economic development of the country. To maintain effective relations with similar institutions of other countries and academic institutes. To distribute update and specialization courses of knowledge in science, technology and industrial administration in the area of computer science security for the electrical industry. To offer consultant's office to the Federal Commission of Electricity (FCE), to the industry of electrical manufactures and the companies of engineering and

consulting services related to the electrical industry. To propose to the Secretariat of Energy and to the FCE (In Mexico CFE), applied and technological research programs for computer science security, and the corresponding plans of operation, investment and short, medium financing to and long term. To patent and to license the developed technologies and the results of the investigation that it obtains and that is originating.

It is necessary to realize the following policies of security and plans for the Electric Research Institute of Mexican Government are: Policy of security for the creation of access control lists. Plan of contingency in case of disasters. Plan of recovery in case of denial of service. Policy of security for the suitable use of institutional the computer science resources. Plan and calendar of qualification of basic aspects of security for the personnel of the institute. Plan and calendar for the acquisition and installation of anti-spyware software. Policy of security for the use of the electronic mail. Policy of security for the suitable use of Internet and Internet 2.

As result of the strategic planning for the computer science security are the strategies to provide greater security to the institute: The institute does not count on necessary mechanisms. To create access control lists (ACL) in the peripheral devices (switches, AP, firewalls). It enforces assigned authorizations for the intrusion detection in accordance with applicable policy. It enforces assigned authorizations for controlling the firewall in accordance with applicable policy. To create a plan of contingency in case of a denial of service. It's necessary to training the personal on aspects of computer science security. To automate the verification of virus in all the computers of the institute. To buy anti-spyware for the computers of the institute.

References

1. F.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. M. Allison, Strategic Planning for Nonprofit Organizations, Second Edition, Wiley, ISBN-10: 0471445819.

4. K. Graham, Strategic Planning and Performance Management: Develop and Measure a Winning Strategy, Butterworth-Heinemann, February 3, 2005, ISBN-10: 0750663839.

5. Y. Hien-Chih, 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. B. Moulin, Strategic Planning for Expert Systems, IEEE Expert 5(2), 1990, pp. 69-75.

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

9. J. A. Ruiz-Vanoye, O. Díaz-Parra, I.R. Ponce-Medellín, J.C. Olivares-Rojas: Strategic Planning for the Computer Science Security. WSEAS TRANSACTIONS on COMPUTERS. Issue 5, Volume 7, pp 387-396, May (2008) ISSN: 1109-2750

10. J.A. Ruiz-Vanoye, O. Díaz-Parra, A. Fuentes Penna, J.O. Ceyca Castro, J.C. Olivares-Rojas, 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

11. P.F. Drucker, The Practice of Management, Harper & Row publishers, New York 1954.

12. A.D. Chandler, Strategy and Structure: Chapters in the History of the American Industrial Enterprise. Cambridge, MA: MIT Press 1962.

13. P.S. Browne, Computer security: a survey, ACM SIGMIS, Vol. 4, Issue 3, 1972, ISSN:0095-0033.

14. J.P. Walton, Developing an enterprise information security policy, Proceedings of the 30th annual ACM SIGUCCS, 2002, ISBN:1-58113-564-5.

15. S.H. Bakry, Development of security policies for private networks, International Journal of Network Management, Vol. 13, Issue 3, 2003, ISSN:1099-1190, pp. 203-210.

16. Antiphising Working Group. Crimeware Taxonomy & Samples According to classification in June 2006. Phishing Activity Trends Report July. 2006.

17. T. Escamilla, Intrusion Detection: Network Security beyond the firewall. John Wiley and Sons, Inc. 1998.

18. ISO/IEC. Engineering Capability Maturity Model (SSECMM). ISO/IEC 21827. Information Technology System Security.

19. U.S. Commerce Departament. National Vulnerability Database. http://nvd.nist.gov.

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

21. Jorge A. Ruiz-Vanoye, Ocotlán Díaz-Parra, José C. Zavala-Díaz: Strategic Planning for Computer Science Security of Networks and Systems in SMEs.

African Journal of Business Management Vol. 6, No. 3, pp. 762-779, Academic Journals (2012) ISSN 1993-8233, DOI: 10.5897/AJBM10.1615.

22. Jorge A. Ruiz-Vanoye, Ocotlán Díaz-Parra, Juan Arturo Nolazco-Flores, Ana Alberta Canepa Saenz, Victor H. Hernández, Heriberto Gongorá. Quality Function Deployment (QFD) House of Quality for Strategic Planning of Computer Security of SMEs. International Journal of Combinatorial Optimization problems and informatics. Vol. 4, No. 1 (2013) 39-53. ISSN:2007-1558.

23. Jorge A. Ruiz-Vanoye, Ocotlán Díaz-Parra, Ismael R. Ponce-Medellin, Alejandro Fuentes-Penna, Juan C. Olivares-Rojas: Strategic planning for the Computer science Security of Banking Organizations, Companies and Government. Modern Topics of Computer Science. Proceedings of the 2nd WSEAS International Conference on Computer Engineering an Applications (CEA 2008). pp. 60. Acapulco, México. January 25-27, 2008. Electrical and Computer Engineering Series A Series of Reference Books and Textbooks. WSEAS Press. (2008) ISSN:1790-5117. ISBN:978-960-6766-33-6.

24. Electrical Research Institute, http://www.iie.org.mx
25. Jorge A. Ruiz-Vanoye, Ocotlán Díaz-Parra, Ma. De los Ángeles Buenabad Arias, Ana Canepa Saenz. A Model for Evolutionary Software development with Security (MESS) applied to an Electrical Research Institute. Mexican Journal of Scientific Research (MJSR). Vol. 2, No. 1 (2013) 2-22. ISSN: 2007-5146.