African Journal of Business Management Vol. 6(3), pp. 762-779, 25 January, 2012
Available online at http://www.academicjournals.org/AJBM
DOI: 10.5897/AJBM10.1615
ISSN 1993-8233 ©2012 Academic Journals

Full Length Research Paper

Strategic planning for computer science security of networks and systems in SMEs

Jorge A. Ruiz-Vanoye[1], Ocotlán Díaz-Parra[2] and José C. Zavala-Díaz[2]

[1]Universidad Popular Autónoma del Estado de Puebla, Mexico.
[2]Universidad Autónoma del Estado de Morelos, FCAeI. Mexico.

Accepted 28 September, 2011

The strategic planning adapted in the computer science security is observed in many senses as a military strategy, which takes advantage of their forces to operate the vulnerabilities of the organizations, attackers or competitors. The need of the companies and organizations to continuously adapt to the technological changes of the computer science formulated the following key questions: what type of security and management is needed by small and medium enterprise (SME) in wireless network systems and devices? and how can the risk for cyber attack on mission-critical devices on the organization be measured? This study proposes to apply the strategic planning for the computer science security of network and systems in SMEs with the following characteristics: easy to understand, easy to apply, and economical in its adoption.

Key words: Strategic planning, computer security, SME, SMB, VSE, Risk analysis, metrics of security, security management.

INTRODUCTION

The strategic administration 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 (David, 1997; Moulin, 1990; Rong-Ji and Gwo-Guang, 2003).

The formal strategic planning with its modern characteristics was introduced in some commercial companies in the middle of 1950. There were numerous early contributors to the literature of the strategic planning: Drucker (1954) mentions the strategy requires that the managers analyze their present situation and that they change it in necessary cases, knowledge that resources have the company and which must have. Selznick (1957) introduced the idea of matching the organization's internal factors with external environmental circumstances. This core idea was developed into what was now call SWOT analysis by Learned, Andrews, and others at the Harvard Business School General.

Management Group. Strengths and weaknesses of the firm are assessed in light of the opportunities and threats from the business environment. Chandler (1962) mentions the elements 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 most influential strategist of the decade was Michael Eugene Porter. Porter (1979) introduced many new concepts including; 5 forces analysis, generic strategies, the value chain, strategic groups, and clusters. Porter modifies Chandler's dictum about structure following strategy by introducing a second level of structure: Organizational structure follows strategy, which in turn follows industry structure. Porter's generic strategies detail the interaction between cost minimization

*Corresponding author. E-mail: jorge@ruizvanoye.com.

Abbreviations: SMEs, Small and medium enterprises; **SMBs,** small and medium businesses; **VSEs,** very small enterprises; **RT matrix,** matrix of recommendations and threats; **MV matrix,** matrix of mechanism and vulnerabilities; **VRTM matrix,** matrix of vulnerabilities, recommendations, threats and mechanism; **QSPM-CSS,** quantitative strategic planning matrix for computer science security; **EFE,** external factor evaluation; **IFE,** internal factor evaluation; **RT,** recommendation and threat; **SWOT,** strengths, weaknesses, opportunities, and threats; **IDS,** intrusion detection system; **DoS,** denial of service.

Table 1. RT matrix.

Factors	Value	Cal.	Results
Recommendations			
1.-	V1	C1	R1
2.-	V2	C2	R2
3.-	V3	C3	R3
4.-	V4	C4	R4
5.-	V5	C5	R5
Threats			
1.-	V1	C1	R1
2.-	V2	C2	R2
3.-	V3	C3	R3
4.-	V4	C4	R4
5.-	V5	C5	R5
	1.00		Total

Table 2. MV matrix.

Factors	Values	Cal.	Results
Mechanisms			
1.-	V1	C1	R1
2-	V2	C2	R2
3.-	V3	C3	R3
4.-	V4	C4	R4
5.-	V5	C5	R5
Vulnerabilities			
1.-	V1	C1	R1
2.-	V2	C2	R2
3.-	V3	C3	R3
4.-	V4	C4	R4
5.-	V5	C5	R5
	1.00		Total

strategies, product differentiation strategies, and market focus strategies.

Ruiz-Vanoye et al. (2008) proposes to apply the strategic planning for the computer science security. 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.

In this paper, the study proposes to apply the strategic planning based on the concepts of strategic administration of enterprise politics for the computer science security to the SMEs with the following characteristics: Easy to understand, Easy to apply, and Economical in its adoption. The Small and Medium Enterprises (SMEs), Small and Medium Businesses (SMBs) or Very Small Enterprises (VSEs) are companies with fewer than 10 employees (Micro enterprises), 50 employees (small) and those with fewer than 250 (medium). In most economies, smaller enterprises are much greater in number (DaeSoo et al., 2008). The paper is organized as describing the strategic planning for the computer science security to the SMEs, the results, discussion and the conclusions.

Strategic planning for computer science security

Ruiz-Vanoye et al. (2008) are the first to propose to apply the strategic planning for the computer science security. 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 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. The methods of strategic planning for computer science security are:

a) The matrix of recommendations and threats (RT matrix).
b) The matrix of mechanism and vulnerabilities (MV matrix).
c) The matrix of vulnerabilities, recommendations, threats and mechanism (VRTM matrix).
d) The quantitative strategic planning matrix for computer science security (QSPM-CSS).

Matrix of recommendations and threats (RT Matrix)

Recommendation and threat (RT) matrix 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 (Ruiz-Vanoye et al., 2008):

1. A list between 8 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.

Matrix of mechanism and vulnerabilities (MV Matrix)

MV matrix 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 (Ruiz-Vanoye et al., 2008):

1. A list between 8 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

Table 3. VRTM Matrix.

	Mechanism	**Vulnerabilities**
Blank	1.- 2.- 3.- 4.- 5.-	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

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.

Matrix of vulnerabilities, recommendations, threats and mechanism (VRTM Matrix)

The VRTM matrix, VRT matrix 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. The procedure to elaborate the VRTM matrix (Table 3) consists of the following steps (Ruiz-Vanoye et al., 2008):

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 = MR strategies).
6 Adapt the vulnerabilities to the recommendations and register resulting strategies VR in the corresponding square (Vulnerabilities+ Recommendations = VR strategies).
7. Adapt the mechanisms to the threats and register resulting strategies MT in the corresponding square (Mechanisms + Threats = MR strategies).
8. Adapt the vulnerabilities to the threats and register the strategies VT resulting in the corresponding square (Vulnerabilities + Threads = VT strategies).

Quantitative strategic planning matrix for computer science security (QSPM-CSS Matrix)

The QSPM-CSS is based in the QSPM. QSPM is a high-level strategic management approach for evaluating possible strategies. QSPM provides an analytical method for comparing feasible alternative actions. The procedure to elaborate QSPM-CSS (Table 4) consists of the following steps (Ruiz-Vanoye et al., 2008):

1. Make a list of the recommendations, threats, mechanisms and vulnerabilities, the list can be obtained from MV and RT matrices.
2. Adjudge values to each one of the factors, these are the same to the obtained ones in MV and RT matrices.
3. Analyze the MR, VR, TM and VT strategies obtained from VRTM matrix and position in the superior row of QSPM-CSS matrix.
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.

Strategic planning for computer science security of networks and systems in SMEs

The study proposes to use strategic planning methods for computer science security (Ruiz-Vanoye et al., 2008) to evaluate a case of SME. The methodology used in the practical case of SMEs consists of the following steps:

1. Identifying the external recommendations and threats of security to the company or financial organization and Elaborate the RT matrix.
2. Define the mechanisms and vulnerabilities in the computer science security and Elaborate the MV matrix.
3. Elaborate the VRTM matrix to generate strategies of computer science security for the SME.
4. To elaborate the QSPM-CSS for the evaluation of the strategy of computer science security.

The list of possible recommendations for the SME is:

1. Firewalls: Firewalls determine whether data packets are permitted into a network, and they restrict access to specific resources.
2. 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.
3. Auditing: Install or configure mechanisms to record activities occurring across the interconnection, including application processes and user activities.
4. Identification and authentication: Identification and authentication is used to prevent unauthorized personnel from entering an IT system.
5. 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.
6. 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.
7. Encryption: Encryption is used to ensure that data cannot be read or modified by unauthorized users.

Table 4. QSPM-CSS Matrix.

Factors	Value	Strategies		Strategies	
		Cal.	**Results**	**Cal.**	**Results**
Recommendations					
1.-	V1	C1	R1	C1	R1
2.-	V2	C2	R2	C2	R2
3.-	V3	C3	R3	C3	R3
4.-	V4	C4	R4	C4	R4
5.-	V5	C5	R5	C5	R5
Threats					
1.-	V1	C1	R1	C1	R1
2.-	V2	C2	R2	C2	R2
3.-	V3	C3	R3	C3	R3
4.-	V4	C4	R4	C4	R4
5.-	V5	C5	R5	C5	R5
Mechanisms					
1.-	V1	C1	R1	C1	R1
2-	V2	C2	R2	C2	R2
3.-	V3	C3	R3	C3	R3
4.-	V4	C4	R4	C4	R4
5.-	V5	C5	R5	C5	R5
Vulnerabilities					
1.-	V1	C1	R1	C1	R1
2.-	V2	C2	R2	C2	R2
3.-	V3	C3	R3	C3	R3
4.-	V4	C4	R4	C4	R4
5.-	V5	C5	R5	C5	R5
			Total		Total

Physical and Environmental Security: Physical security addresses the physical protection of computer hardware and software.

The list of possible threats for the SME is:

1. Denial of service (DoS). An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
2. Malicious code. A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
3. Unauthorized access. A person gains logical or physical access without permission to a network, system, application, data, or other IT resource.
4. Inappropriate usage. A person violates acceptable use of any network or computer policies.
5. 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.

The areas of security for mechanisms and vulnerabilities are:

1. 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, auto-mated labeling, remote access, wireless access restrictions, access control for portable and mobile devices, use of external information systems).
2. Awareness and training (Security awareness and training policy and procedures, security awareness, security training, security training records, contacts with security groups and associations).
3. 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).
4. 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).
5. 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).

Table 1. RT Matrix.

Factors	Values	Q	Results
Recommendations			
R1. Firewalls	0.17	2	0.34
R2. Intrusion Detection	0.13	1	0.13
R3. Identification and Authentication	0.05	3	0.15
R4. Virus Scanning	0.11	4	0.44
R5. Physical and Environmental Security	0.04	3	0.12
Threats			
T1. Denial of Service	0.13	1	0.13
T2. Malicious Code	0.18	3	0.54
T3. Unauthorized Access	0.10	2	0.20
T4. Inappropriate Usage	0.05	2	0.10
T5. Multiple Components	0.04	2	0.08
	1.00		2.23

6. 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).
7. Identification and authentication (Identification and authentication policy and procedures, user identification and authentication, device identification and authentication, identifier management, authenticator management, authenticator feed-back, cryptographic module authentication).
8. Incident response (Incident response policy and procedures, incident response training, incident response testing and exercises, incident handling, incident monitoring, incident reporting, incident response assistance).
9. Maintenance (System Maintenance Policy and Procedures, Controlled Maintenance, Maintenance Tools, Remote Maintenance, Maintenance Personnel, Timely Maintenance).
10 Media protection (Media protection policy and procedures, media access, media labeling, media storage, media transport, media sanitization and disposal).
11.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).
12. Planning (Security planning policy and procedures, system security plan, system security plan update, rules of behavior, privacy impact assessment, security-related activity planning).
13. Personnel security (Personnel security policy and procedures, position categorization, personnel screening, personnel termination, personnel transfer, access agreements, third-party personnel security, personnel sanctions).
14. Risk assessment (Risk assessment policy and procedures, security categorization, risk assessment, risk assessment update, vulnerability scanning).
15. 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).
16. 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).
17. 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).

RESULTS

In this paper, the study evaluated a company (SME) dedicated to technologies of information with an ample portfolio of solutions for the industry of manufacture, financial, education, services, health, communications, energy, consumer, Transports and Government. The company has four divisions: 1) Services: Development of systems custom-made, web solution, technical support of software. 2) Licensing of proprietary software and diverse manufacturers knowledge. 3) Training and Outsourcing de Personal (staffing) innovation. 4) Investigation and development in new technologies and solutions. The study use the Strategic Planning for Computer Science Security for evaluates Networks and Systems in the SME.

a) Elaborate the RT matrix: First, the study must identify the recommendations and threats. Once identified the recommendations and threats, it's necessary to make the RT matrix (Table 5) for the SME.
b) Elaborate the MV matrix: First, the study must identify the mechanism and vulnerabilities. Once identified the mechanisms and vulnerabilities, it's necessary to make the MV matrix (Table 6) for the SME.
c) Elaborate the VRTM matrix: It´s necessary to adapt mechanisms, recommendations, vulnerabilities and recommendations to generate strategies of computer science security for the SME (Table 7).
d). To elaborate the QSPM-CSS (Table 8).

DISCUSSION

In Table 5 shows the RT matrix for the SME, the result of

Table 5. RT Matrix.

Factors	Values	Q	Results
Recommendations			
R1. Firewalls	0.17	2	0.34
R2. Intrusion Detection	0.13	1	0.13
R3. Identification and Authentication	0.05	3	0.15
R4. Virus Scanning	0.11	4	0.44
R5. Physical and Environmental Security	0.04	3	0.12
Threats			
T1. Denial of Service	0.13	1	0.13
T2. Malicious Code	0.18	3	0.54
T3. Unauthorized Access	0.10	2	0.20
T4. Inappropriate Usage	0.05	2	0.10
T5. Multiple Components	0.04	2	0.08
	1.00		2.23

Table 6. MV Matrix.

Factors	Val	Q	Res
Mechanisms			
M1. The SME has a Personnel Security.	0.07	3	0.21
M2. The SME has a Physical and Environmental Protection (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
M3. The SME enforces assigned authorizations for controlling access to the network and systems.	0.15	3	0.45
M4. The SME has been contracted recently an administrator of security.	0.20	4	0.80
Vulnerabilities			
V1. The SME constantly receives DoS that does that their network slowly.	0.20	1	0.20
V2. The computers of the SME constantly become infected of virus.	0.15	1	0.15
V3. The SME don’t have a contingency planning policy and procedures to appropriate elements within the organization.	0.08	2	0.16
V4. The SME don’t have Spam Protection.	0.06	2	0.12
	1.00		2.36

Table 7. VRTM Matrix.

	M	**V**
	M1	**V1**
	M2	**V2**
	M3	**V3**
	M4	**V4**
R	**MR Strategies**	**VR Strategies**
R1	(R1,M4) The administrator of security must to verify the rules of the firewall (R5, M1, M2) It enforces assigned authorizations for the physical security in accordance with applicable physical policy.	(R4,V2,V3) To automate the verification of virus in all the computers of the SME.
R2		
R3		
R4		
R5		

T	MT Strategies	VT Strategies
T1	(T1,M4,M4) To verify the access control	(T1,V1,V3) It's necessary to verify the configurations of the ALL networks devices, to change the passwords, to create new policies. To create a plan of contingency in case of a denial of service (T2,V4) To acquire anti-spam, anti-spyware or anti-malware.
T2	list, changes the passwords of the	
T3	peripheral devices (switches, AP,	
T4	firewalls) and systems.	
T5	(T4,M4) To create a policy of correct usage of the SME computers.	

Where: R = Recommendations, T = Threats, M = Mechanisms, V = Vulnerabilities, 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 SME has a Personnel Security. M2 = The SME has a Physical and Environmental Protection (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 SME enforces assigned authorizations for controlling access to the network and systems. M4 = The SME has been contracted recently an administrator of security. V1 = The SME constantly receives DoS that does that their network slowly. V2 = The computers of the SME constantly become infected of virus. V3 = The SME do not have a contingency planning policy and procedures to appropriate elements within the organization. V4 = The SME don't have Spam Protection. Val = Values. Res = Results.

Table 8. QSPM-CSS matrix.

F	Va	S1		S2		S3		S4		S5		S6		S7	
		Q	Re	Q	Re	Q	Re	Q	Re	Q	Re	Q	Re	Q	Re
R1	0.17	4	0.68	1	0.17	1	0.17	4	0.68	1	0.17	4	0.68	1	0.17
R2	0.13	3	0.39	1	0.13	1	0.13	4	0.52	1	0.13	4	0.52	1	0.13
R3	0.05	2	0.10	1	0.05	1	0.05	3	0.15	3	0.15	2	0.10	1	0.05
R4	0.11	1	0.11	1	0.11	3	0.33	1	0.11	1	0.11	2	0.22	4	0.44
R5	0.04	1	0.04	3	0.12	1	0.04	1	0.04	1	0.04	1	0.04	1	0.04
T1	0.13	4	0.52	1	0.13	1	0.13	3	0.39	1	0.13	4	0.52	1	0.13
T2	0.18	1	0.18	1	0.18	2	0.36	1	0.18	1	0.18	1	0.18	4	0.72
T3	0.10	1	0.10	2	0.20	1	0.10	1	0.10	3	0.30	4	0.40	1	0.10
T4	0.05	1	0.05	1	0.05	1	0.05	1	0.05	1	0.05	1	0.05	1	0.05
T5	0.04	1	0.04	1	0.04	1	0.04	1	0.04	1	0.04	1	0.04	1	0.04
M1	0.07	1	0.07	3	0.21	1	0.07	1	0.07	1	0.07	1	0.07	1	0.07
M2	0.09	1	0.09	3	0.27	1	0.09	1	0.09	1	0.09	1	0.09	1	0.09
M3	0.15	4	0.60	3	0.45	1	0.15	4	0.60	1	0.15	4	0.60	1	0.15
M4	0.20	4	0.80	1	0.20	2	0.40	4	0.80	1	0.20	2	0.40	2	0.40
V1	0.20	4	0.80	1	0.20	1	0.20	4	0.80	1	0.20	2	0.40	1	0.20
V2	0.15	1	0.15	1	0.15	4	0.60	1	0.15	1	0.15	1	0.15	3	0.45
V3	0.08	1	0.08	1	0.08	1	0.08	1	0.08	1	0.08	1	0.08	1	0.08
V4	0.06	1	0.06	1	0.06	3	0.18	1	0.06	1	0.06	1	0.06	4	0.24
			4.86		2.8		3.17		4.91		2.3		4.6		3.55

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 SME has a Personnel Security. M2 = The SME has a Physical and Environmental Protection (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 SME enforces assigned authorizations for controlling access to the network and systems. M4 = The SME has been contracted recently an administrator of security. V1 = The SME constantly receives DoS that does that their network slowly. V2 = the computers of the SME constantly become infected of virus. V3 = The SME don't have a contingency planning policy and procedures to appropriate elements within the organization. V4 = The SME don't have Spam Protection. Re = results. Va = Values. F = Factors. Q = Qualifications. S1 = the administrator of security must to verify the rules of the firewall. S2 = It enforces assigned authorizations for the physical security in accordance with applicable physical policy. S3 = To automate the verification of virus in all the computers of the SME. S4 = to verify the access control list, changes the passwords of the peripheral devices (switches, AP, firewalls) and systems. S5 = to create a policy of correct usage of the SME computers. S6 = It is necessary to verify the configurations of the ALL networks devices, to change the passwords, to create new policies. To create a plan of contingency in case of a denial of service. S7 = to acquire anti-spam, anti-spyware or anti-malware.

2.23 mentions that the SME counts on basic elements to protect itself of threats. The ranks of values allowed for RT matrix is: 0-2: the SME is vulnerable of threats, 2-3: the SME counts on basic elements of security, 3-4: the SME is not vulnerable of threats. In Table 6 shows the MV matrix for the SME, the result of 2.36 mentions that the SME counts on basic mechanisms to protect itself of vulnerabilities. The ranks of values allowed for this matrix are: 0-2: the SME is vulnerable, 2-3: the SME counts on basic mechanisms of security, 3-4: the SME is not vulnerable.

In Table 7 shows the strategies of computer science security for the SME but not the order to use. Mechanisms-recommendations strategies: The administrator of security must to verify the rules of the firewall and it enforces assigned authorizations for the physical security in accordance with applicable physical policy. Vulnerabilities-recommendations strategies: To automate the verification of virus in all the computers of the SME. Mechanisms-threats strategies: to verify the access control list, changes the passwords of the peripheral devices (switches, AP, firewalls) and systems and to create a policy of correct usage of the SME computers. Vulnerabilities-threats strategies: It's necessary to verify the configurations of the ALL networks devices, to change the passwords, to create new policies; to create a plan of contingency in case of a denial of service and to acquire anti-spam, anti-spyware or anti-malware. The Table 8 determines the order (importance) in which the strategies were elaborated is:

a) To verify the access control list, changes the passwords of the peripheral devices (switches, AP, firewalls) and systems.
b) The administrator of security must to verify the rules of the firewall.
c) It's necessary to verify the configurations of the ALL networks devices, to change the passwords, to create new policies and to create a plan of contingency in case of a denial of service.
d) To acquire anti-spam, anti-spyware or anti-malware.
e) To automate the verification of virus in all the computers of the SME.
f) It enforces assigned authorizations for the physical security in accordance with applicable physical policy.
g) To create a policy of correct usage of the SME computers.

The security policies and plans are: security policy for physical security, security policy for the correct use of the electronic mail, Internet, Internet 2 and SME computers. Plan of recovery in case of denial of service. 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.

Conclusions

The study concludes that is possible to use the strategic planning and the computer science security to provide solutions of SMEs security problems. The measure of the risk for cyber attack on networks, systems or mission-critical device on the SME can do it by means the strategic planning and the computer science security. It is necessary to do the strategic planning for computer science security every 3 to 6 months to the SMEs.

The use of the strategic planning in questions of computer science security is an excellent mechanism to administer aspects of security in any SME. The matrixes of the strategic planning are quantitative and high-priority mechanisms to define the actions or strategies to follow. The determination of the threat and the risk is a specialized field, and could be necessary to resort to a security consultant or a specialist of the risk to determine the diverse aspects of the security.

REFERENCES

Chandler A (1962). Strategy and Structure: Chapters in the history of industrial enterprise, Doubleday, New York.

DaeSoo K, Ow TT, Minjoon J (2008). SME strategies: an Assessment of High vs. Low Performers. Commun. ACM, 51(11): 113-117.

David FR (1997). Concepts of strategic planning. Prentice Hall.

Drucker PF (1954). The Practice of Management, Harper and Row publishers, New York.

Moulin B (1990). Strategic Planning for Expert Systems. IEEE Expert, 5(2): 69-75.

Porter M (1979). How competitive forces shape strategy. Harv. Bus. Rev., 137-145.

Rong-Ji B, Gwo-Guang L (2003). Organizational factors influencing the quality of the IS/IT strategic planning process. Ind. Manage. Data Syst., 103(8): 622-632.

Ruiz-Vanoye JA, Díaz-Parra O, Ponce-Medellín IR, Olivares-Rojas JC (2008). Strategic Planning for the Computer Science Security. WSEAS Trans. Comput., 5(7): 387-396.

Selznick P (1957). Leadership in Administration: A Sociological Interpretation, Row, Peterson, Evanston.