ARTIGO

Validity of information security policy models

Validação de modelos de políticas de segurança de informação

Joshua Onome IMONIANA[1]

ABSTRACT

Validity is concerned with establishing evidence for the use of a method to be used with a particular set of population. Thus, when we address the issue of application of security policy models, we are concerned with the implementation of a certain policy, taking into consideration the standards required, through attribution of scores to every item in the research instrument. En today's globalized economic scenarios, the implementation of information security policy, in an information technology environment, is a condition *sine qua non* for the strategic management process of any organization. Regarding this topic, various studies present evidences that, the responsibility for maintaining a policy rests primarily with the Chief Security Officer. The Chief Security Officer, in doing so, strives to enhance the updating of technologies, in order to meet all-inclusive business continuity planning policies. Therefore, for such policy to be effective, it has to be entirely embraced by the Chief Executive Officer. This study was developed with the purpose of validating specific theoretical models, whose designs were based on literature review, by sampling 10 of the Automobile Industries located in the ABC region of Metropolitan *São Paulo* City. This sampling was based on the representativeness of such industries, particularly with regards to each one's implementation of information technology in the region. The current study concludes, presenting evidence of the discriminating validity of four key dimensions of the security policy, being such: the Physical Security, the Logical Access Security, the Administrative Security, and the Legal & Environmental Security. On analyzing the *Alpha of Crombach* structure of these security items, results not only attest that the capacity of those industries to implement security

[1] Docente, Programa de Pós-Graduação em Administração, Universidade Metodista de São Paulo. Rua do Sacramento, 230, Rudge Ramos, 09735-460, São Bernardo do Campo, SP, Brasil. *E-mail*: <joshua.imoniana@metodista.br>.
Recebido em 13/2/2004 e aceito para publicação em 27/9/2004.

policies is indisputable, but also, the items involved, homogeneously correlate to each other.

Key words: validity, security, policy, models.

RESUMO

Validar é estabelecer evidência para o uso de um método a ser utilizado com um grupo populacional determinado. Portanto, quando nos referimos à questão de aplicação de modelos de política de segurança, estamos nos referindo à implementação de um certo conjunto de regras estabelecidas em consideração a determinados requisitos, através da atribuição de valores a cada item constante do instrumento de pesquisa. Nos cenários econômicos globalizados de hoje, a implementação de políticas de segurança da informação, num ambiente de tecnologia da informação, é condição **sine qua non** *para o processo de gerenciamento estratégico de qualquer organização. Com relação a este assunto, vários estudos apresentam evidências de que, a responsabilidade de manter o regulamento deve ser fundamentalmente delegada ao Chefe de Segurança (Chief Security Officer). Este, ao assumir esse encargo, esforça-se por incentivar a atualização das tecnologias, com a finalidade de satisfazer os mais abrangentes regulamentos do planejamento de continuidade dos negócios. Portanto, para o regulamento da segurança ser efetivo, terá que ser inteiramente ratificado pelo* Chefe do Executivo *(Chief Executive Officer) da organização. Desenvolveu-se este estudo com o propósito de validar modelos teóricos específicos, cujos planos se basearam na revisão da literatura, com a amostragem de dez das Indústrias Automobilísticas localizadas no ABC da região metropolitana de São Paulo. Esta amostragem baseou-se na representatividade de tais indústrias, particularmente no que se refere à implementação da tecnologia da informação que cada uma realizou na região. A conclusão deste estudo apresenta evidências da validez discriminatória das quatro dimensões-chave da política de segurança, a saber: Segurança Física, Segurança do Acesso ao Núcleo Lógico, Segurança Administrativa, e a Segurança Legal e Ambiental. Os resultados da análise da estrutura Alpha of Crombach dessas dimensões da segurança, não só revelam que é indisputável a capacidade daquelas indústrias de implementar suas políticas de segurança, como também atestam que tais dimensões, homogeneamente se correlacionam umas às outras.*

Palavras-chave*: validação, segurança, políticas, modelos.*

RESEARCH CONTEX

The theme under study is current and has a great relevance in today's business corporations. In the context of contemporary management, there are organizations that use information security as a competitive strategy, security being the differential that attracts a certain group of consumers who are prepared to face higher expenditure, in exchange for maintaining peace and stability.

Owing to this reality, management must not neglect the sensitivity of the issue, while deciding which would be the coverage for the involved risks in the Information Technology Plans. Thus, information owners could raise a concern regarding how to debar the application's developers of his company, who is responsible for the maintenance of the system, from practicing fraudulent acts in the specification phase of the application development cycle, thereby leaving a loophole to be perpetrated in the near future. According to Guerra (2001), a ”formidable systems' specification must be structured in independent forms, such as manageable modules, to ensure its modularity”, meaning that a management must safeguard against possible human errors, when molding complex application systems which cannot be dismembered for maintenance purposes.

Historically, tasks relating to information security have been referred to the supervisors or the second level management. Currently, with the growing concerns about security round the globe, the responsibilities of information security exceeds ordinary Help Desk responsibility. This enables the responsibility of the implementation of a security policy being delegated to such functions as line managers.

This concern is not restricted to the Brazilian business environment alone, as foreign researchers would expatiate on the theme. According to Pounder (2001) European Community has decided that it will not leave such an important function as the information systems' security, and the telecommunication network, loosely to the market force. In a proposal submitted to member states, he argues that, legislation and/or other initiatives for harmonization, need to come into place in order to restrain systems' security threats.

Information Security Dimensions

Physical Security

Known as physical security, there are security functions, performed by equipments with adequate mechanisms, aimed at restricting the access of persons to the computer environment, in order to safeguard against any structural risk, be it related to components, to complex and isolated units, or to palmtops. This security involves the control of physical contacts and the protection of human lives, besides the maintenance of equipments peripheral units that hold programs, softwares, or other whose safeguarding is limited to certain employees. Such security avoids losses of hardware or prevents them from malfunction which could generate operational disruptions, resulting in business disadvantages and consequently financial losses.

When discussing physical access control security, there are two areas to consider: The first, concerns the equipments that would restrict indiscriminate access, internally, in the organization, thereby guarantying protection to computer terminals, central processing units, servers, data conversion units, tapes, disks, lives, etc. The second, concerns equipments that would restrict access to outsiders, or whoever have interest in accessing an organization's information, but would not do it for lack of physical permission.

Among the security resources, used to enhance corporate physical access security, are the: Fire fighting equipment, which include: extinguishers, Sprinklers, Gas carbonic, Gas Halon, etc. As relating to restricting physical access to outsiders, physical and transportable access keys to block access, firewalls, etc are used. To achieve an absolute security, physical isolation of the computer environment is practised.

To consolidate the physical access security control in a security policy, the periodic backup programs, jointly with the contingency and disaster recovery plans, are developed and monitored. This is done to enable an off-site processing of normal business transaction, in case of hazards.

Logical Access Security

The logical access security refers to the general protection given by the technological resources in the computer environment, to guide against unauthorized access of sensitive data or information not permitted to other users of the systems, with exception of the owners. Normally, information is restricted in a need-to-know basis. Only individuals who have operational needs of such information, would have access to it logically.

Access security controls are achieved through the use of passwords, individually defined for every authorized user identified in the system. And so, for such user domain, certain privileges or restrictions are attributed, such as the right or limitation to use certain data files, programs, systems, databases, etc. Upon log-on, the individual goes through a process of authentication and authorization to certify that he/she is a legitimate user, whether by knowledge of the passwords or by characteristics that she/he tends to demonstrate to confirm being a *bona fide* owner of the data. Afterwards, having accepted the proofs, the computer allocates to such individual the access to certain resources; compatible with his level of access and the applications he needs to run. For the application, the user is allocated certain data files, programs, databases, remote access or not, including propagation of access if needed; in essence, all the necessary resources to conclude his transaction. It is important to know that, in some cases, users may have *read-only* access authority, not being allowed to write or modify the databases.

For effectiveness of such control, it is recommended the acquisition and implementation of a security software, such as ACF2, TOPSECRET, RACF or similar, which are customised to suite the security policies of different organizations. The complexity of the customisation parameters will be set, taking as reference the users' knowledge of information technology and their awareness of security programmes. This is important, particularly, in order to restrain the hackers' and outsiders' access to the intranet of an organization.

Administrative Security

Administrative security refers to the organisation's security that is nurtured by the proverb: *prevention is better than cure*. The Chief Security Officer (CSO), otherwise known as the Security Administrator, placed in an appropriate level, with the assistance of a Chief Information Officer (CIO), and the ultimate support of the Chief Execute Officer (CEO), should be given autonomy to implement administrative procedures in accordance with the organisation's security policy.

The administrative security controls all other procedures/devices that are installed in the organisation, in order to propel the transaction flow of business operations, and to enhance the accomplishment of business goals. However, the effectiveness of such security depends on the organisation's management experience in tracking administrative security risks, an ability which requires higher management skills. In normal circumstances, there should be minimum external influence.

Generally, an environment which is conducive to the dissemination of orders and administrative policy, normally enhances the implementation of administrative security policies. Such environment usually facilitates the propagation of security awareness programmes - whose aim is the attainment of key management objectives.

The manager in a bid to implementing this type of security, firstly delineates functions, and secondly, specifies the responsibilities of every collaborator, in compliance with the necessary activities. This is normally done to avoid conflicts of interest that arise in day-to-day business operations. However, segregation of functions (origination, authorisation, recording, or modification of assets) may not be easily operative in today's computer environment, where someone, in a quick and simple access, could easily transfer funds and update bank balances in a distant foreign country. Therefore, administrative security procedures are meant to control in and independent form and with check and balance controls that could fail otherwise.

Administrative security deals with definition of responsibilities as regards to management limits and authorities in manipulating and safeguarding the organisation's assets during the process of generating values for the stockholders. Therefore, the *Business Continuity Plan-BCP* is also a concern ascribed to this type of security.

Legal & Environmental Security

Legal Security and Environmental Security are provided by the federal and regional laws. The environment in which the business establishment operates drastically affects its security. To formulate directives to maintain legal and environmental security, all the conditions and problems that might affect people, and consequently, federal, municipal, and state laws, must be considered. Some aspects to be considered are the regulating standards for the company's connectivity [?] Be it cabling, refrigeration of computer rooms, or disposal of obsolete equipment and other used materials (such as computers, ink cartridges, etc), the planners of this type of security tend to consider all regulations imposed by law. The ISO 14000, which specifies environmental standards to be followed by the companies, even though not fiscally obligatory, is important for the companies. The compliance with these standards is observed by environmental organisations that issue the certifications of quality to the complying companies. These certifications are quite positive for companies, in social terms, since readers of the financial reports actual and potential company customers/clients, and supporters/investors - can observe how such establishments are avoiding or curbing forest degradation or striving for environmental maintenance and improvement.

Legal and environment security also takes into consideration protection against vandalism, terrorism, hackers and hijackers. Other situations considered are: protests; labour strikes, or acts of sabotage created to hamper the progress of business operation - all of which, undoubtedly have adverse effects on the business community, affecting the country at large.

Validity Measurement

To be valid is to be seen as being in agreement with the facts; or to be logically sound (*valid argument*), or to be in conjunction with a laid out set of laws and, therefore, be binding by, or based on, compelling principles or methods. Validity, in this study, deals with confirming a set of assertions concerning the principles or practices guiding the security policy models; assertions that one could establish and substantiate based on prior knowledge, literature review, and data analysis.

Generally, validity measurement is three-fold: content-related evidence for validity; criterion-related evidence, and construct-related evidence for validation. According to Morgan (2001): content-related evidence, refers to whether the content that makes up the instrument is representative of the concept that one is attempting to measure; criterion-related evidence, refers to corroborating the qualities of the instrument with some form of external, outside criterion; construct-related evidence is evidence based on hypothetical concepts that cannot be observed, substantiated, directly.

As security resources are constituted of tangible or intangible assets, devoted to add a value to the stockholders' equity, their measurement in the form of a security model, signifies a quantification of how well are achieved either, the attainment of the stated goals, or the generation of benefits to the business entity. Therefore, to validate such models, we borrow a leaf from Morgan, by validating the contents of such models implemented by the industries, the concurrent criteria adopted and the construct used in data mining.

After data capturing, analysis with the use of correlation as a validity measure is welcome, and so, to be valid, correlation would be expected to by high, perhaps 0.8, 0.9 or 1.0. However, there could exhist different measurements for different concepts in such industries, hence, motivating different scores and priority for concepts being measured. Therefore, if the measures are convergent, they should not be highly correlated, otherwise, it could generate scepticism, concerning whether two of the concepts being measured are not one and the same.

Hypothesis & Justification

For the development of this study, the following hypotheses were adopted:

- **H_1**: The key four dimensions of security Physical Security, Logical Access

Security, Administrative Security and Legal & Environmental Security constitute a valid backbone for the implementation of the security policy in an organization, due to the fact that the items composing its conception and development can be harmoniously applied in any organization.

- **H_2**: The key four dimensions of the security policy correlate to each other significantly; thereby, the concepts involved in such policy have a similarly high level of acceptance during their implementation.

- **H_3**: As a result of market perspectives and customer driven business strategies, apparently demonstrated by the observed industries, discrepancies about the implemented security models should not be seen as very relevant.

This study is justified by the scarcity of literature in this area; besides that, it exposes to researchers, the process by which the generally accepted security principles have been implemented in the industries. This scientist is charged with the task of fetching information that should be of importance and serve as reference to the business entities; therefore, this study barely serves as a contribution to this task.

METHODS

The sample of the study is composed of 10 industries in the automobile sector of ABC region of the metropolitan *São Paulo* city. No distinction was made whether the respondents were male or female because, for the purpose of this research, such data is not so relevant.

The mining of data was centred on a cluster of representatives, composed of employees of second echelon, who have the responsibility to implement the security policy models in their organisation.

Data collection was accomplished through the use of an instrument that contains four nominal scales, forming the basis for the construction of a security policy, notably: Physical Security (PHSEC, 5 items), Logical Access Security (LASEC, 6 items), Administrative Security (ADSEC, 6 items) and Legal & Environmental Security (LESEC, 4 items). The last item constitutes a question to gather data about the position of the employee responsible for the implementation of security policy.The items which sums 22 in the research instrument, were elaborated based on the functions and operational definition of construct, as it is considered in the theoretical definitions.

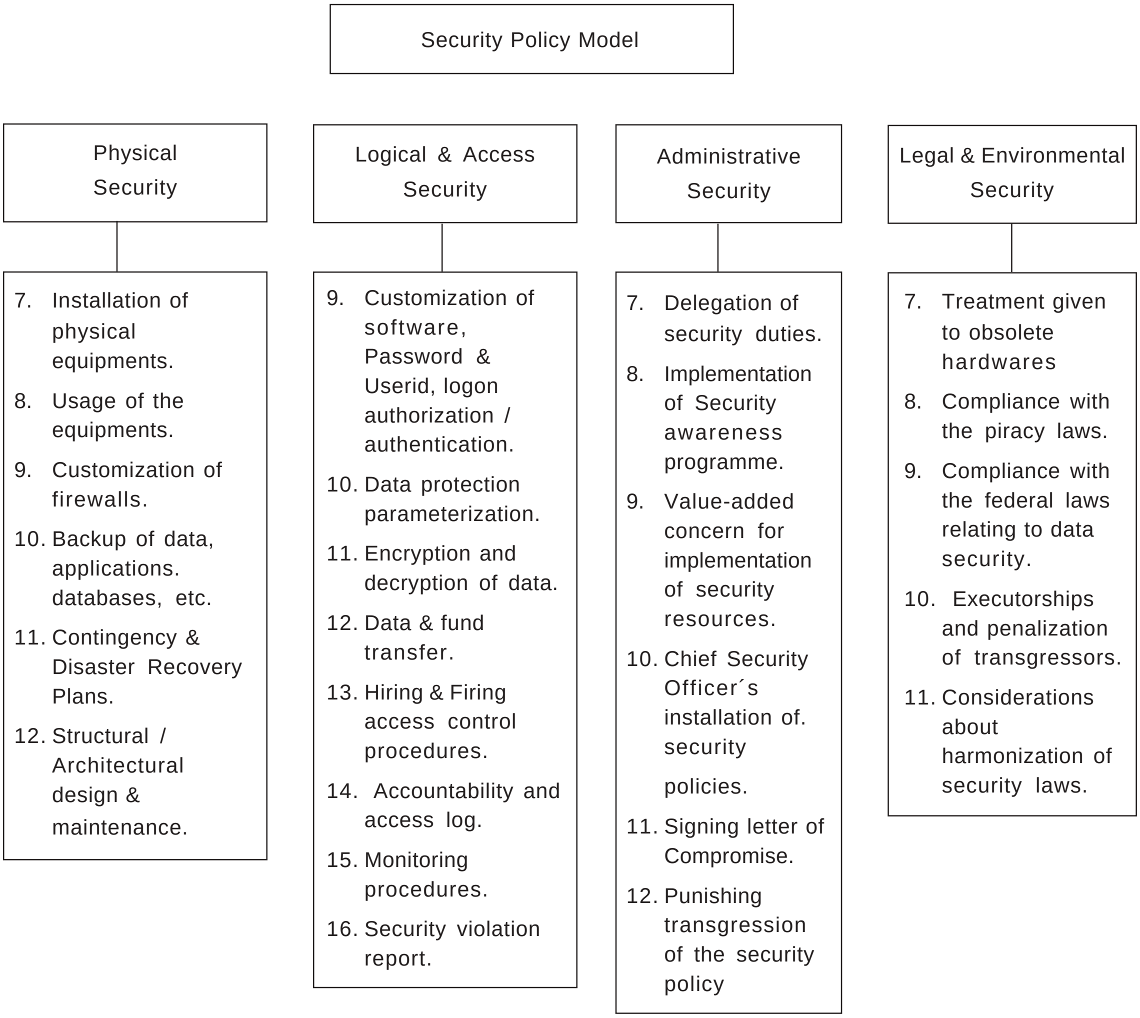
For our literature review, we divided the security policy dimensions in four, thus, permitting us to formulate a model, as shown in Figure 1. Therefore, based on said sketch, we adopted some criteria to elaborate the items in the research instrument, which permit a right or wrong answer.

In a bid to obtaining the discriminating validity of the security models implemented by the researched industries, the items in the research instrument were submitted to a descriptive analysis, involving also, the obtaining of the reliability of the model in which the research was based. Additionally, the dimensions of security policy were submitted to the test of correlation. Data were treated with the assistance of the SPSS (Statistical Package for Social Sciences) software.

RESULTS AND DISCUSSION

Our objective was to test the rules surrounding the similarity of the security policy models, implemented by the automobile industries located in the ABC region of the metropolitan *São Paulo* city.

Results of our tests reveal that there is a significant relationship between the principal items that compose the security policy models implemented by the industries. Table 1 shows the items in the instruments, the mean and standard deviation from the original scores stated for the measurement of the items.



Security Policy Model

Physical Security

7. Installation of physical equipments.
8. Usage of the equipments.
9. Customization of firewalls.
10. Backup of data, applications. databases, etc.
11. Contingency & Disaster Recovery Plans.
12. Structural / Architectural design & maintenance.

Logical & Access Security

9. Customization of software, Password & Userid, logon authorization / authentication.
10. Data protection parameterization.
11. Encryption and decryption of data.
12. Data & fund transfer.
13. Hiring & Firing access control procedures.
14. Accountability and access log.
15. Monitoring procedures.
16. Security violation report.

Administrative Security

7. Delegation of security duties.
8. Implementation of Security awareness programme.
9. Value-added concern for implementation of security resources.
10. Chief Security Officer´s installation of. security policies.
11. Signing letter of Compromise.
12. Punishing transgression of the security policy

Legal & Environmental Security

7. Treatment given to obsolete hardwares
8. Compliance with the piracy laws.
9. Compliance with the federal laws relating to data security.
10. Executorships and penalization of transgressors.
11. Considerations about harmonization of security laws.

Figure 1. Security Policy Model.

Table 1. Descriptive statistics.

Description	Item Code	Mean	Standard Deviation	n
Physical Security	PHSEC1	5.00	.000	10
Physical Security	PHSEC2	4.30	.483	10
Physical Security	PHSEC3	5.00	.000	10
Physical Security	PHSEC4	4.70	.483	10
Physical Security	PHSEC5	4.40	.516	10
Logical Access Security	LASEC1	5.00	.000	10
Logical Access Security	LASEC2	4.90	.316	10
Logical Access Security	LASEC2	4.90	.316	10
Logical Access Security	LASEC3	4.70	.483	10
Logical Access Security	LASEC3	4.70	.483	10
Logical Access Security	LASEC4	4.50	.707	10
Logical Access Security	LASEC4	4.50	.707	10
Logical Access Security	LASEC5	4.70	.483	10
Logical Access Security	LASEC6	4.80	.422	10
Administrative Security	ADSEC1	4.60	.516	10
Administrative Security	ADSEC2	4.90	.316	10
Administrative Security	ADSEC3	4.50	.527	10
Administrative Security	ADSEC4	4.70	.675	10
Administrative Security	ADSEC5	4.40	.699	10
Administrative Security	ADSEC6	4.50	.527	10
Legal & Environmental Security	LESEC1	3.90	.316	10
Legal & Environmental Security	LESEC2	5.00	.000	10
Legal & Environmental Security	LESEC3	5.00	.000	10
Legal & Environmental Security	LESEC4	5.00	.000	10

Table 2 shows the validity of Alpha of Crombach of the items that compose the instruments, Administrative Security (ADSEC) Physical Security (PHSEC), Access & Logical Security (LASEC), Legal and Environmental Security (LESEC). Showing that the involved items were logically arranged so that data gathering processes would not be jeopardized.

The reliability coefficient (Alpha of Crombach) obtained in this analysis is 0,8251. The measure is considered significant, thereby validating the construct evidence. In this regard, comparing the measure 0,8251 reached in this research with the coefficient initially presented by Allen & Meyer (1990), which holds the ratios of the *Alpha* of *Crombach* between 0.61 and 0.70, one would conclude that this is an excellent result.

In addition to the aforementioned, we also reached a possibility of raising the Alpha of Crombach, if some items in the instrument were deleted as shown in Table 3.

Table 2. Reliability of the Items in the Instrument.

Alpha of Crombach	Standard Alpha of Crombach
Reliability Coefficients	0,7259
n of Cases = 10.0	
n of Items = 22	
Alpha = 0.8251	

As shown in Table 4, the development and implementation of the security policy model was homogenously accepted as the responsibility of the Chief Security Officer (CSO), which used to be known as the security administrator. This is due to the need to maintain a professional who is capable of following the internal and external scenarios to foment implementation of a consistent security policy.

In the discriminant analysis of the responses' scores, it was observed that employees highly discriminated against the nomination of the Chief Information Officer to be responsible for the implementation of security policy as shown in Table 5. From another perspective, it was observed that, whenever the responsibility for the implementation of the security policy was laid upon a Chief Security Officer, better and more viable had been the opportunity to implement such policy. This latter conclusion resulted from the analysis of the scores obtained from employees' responses, in the industries that have their security model under the control of a Chief Security Officer, as compared to industries that have the same task under the control of other employees.

Table 3. Alpha of Crombach if some items were deleted.

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Alpha if Item Deleted
PHSEC1	96.7000	20.4556	.0000	.8270
PHSEC2	97.4000	18.2667	.4736	.8137
PHSEC3	96.7000	20.4556	.0000	.8270
PHSEC4	97.0000	17.1111	.7785	.7977
PHSEC5	97.3000	19.5667	.1362	.8312
LASEC1	96.7000	20.4556	.0000	.8270
LASEC2	96.8000	19.5111	.3023	.8216
LASEC3	97.0000	17.1111	.7785	.7977
LASEC4	97.2000	15.2889	.8439	.7860
LASEC5	97.0000	18.2222	.4850	.8131
LASEC6	96.9000	18.5444	.4773	.8141
ADSEC1	97.1000	17.8778	.5292	.8105
ADSEC2	96.8000	18.4000	.7208	.8078
ADSEC3	97.2000	16.8444	.7705	.7965
ADSEC4	97.0000	15.5556	.8348	.7875
ADSEC5	97.3000	16.6778	.5759	.8073
ADSEC6	97.2000	18.6222	.3420	.8207
LESEC1	97.8000	20.1778	.0626	.8291
LESEC2	96.7000	20.4556	.0000	.8270
LESEC3	96.7000	20.4556	.0000	.8270
LESEC4	96.7000	20.4556	.0000	.8270
SECRSP	98.5000	22.9444	-.4768	.8695

Table 4. Security responsibility.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	CIO	1	10.0	10.0	10.0
	CSO	7	70.0	70.0	80.0
	Technical Support	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

Table 5. Discriminant Analysis - Case Processing Summary.

Unweighted Cases		n	%
Valid		9	90.0
Excluded	Missing or out-of-range group codes	1	10.0
	At least one missing discriminating variable	0	.0
	Both missing or out-of-range group codes and at least one missing discriminating variable	0	.0
	Total	1	10.0
Total		10	100,0

Table 6. Correlation.

		Physical Security	Logical Acess Security	Administrative Security	Legal & Environmental Security
Physical Security	Pearson Correlation	1	1.000	.716	-.218
	Significant (2-tailed)			.020	.545
	n	10	10	10	10
Logical Access Security	Pearson Correlation	1.000	1	.716	-.218
	Significant (2-tailed)			.020	.545
	n	10	10	10	10
Administrative Security	Pearson Correlation	.716	.716	1	-.156
	Significant (2-tailed)	.020	.020		.667
	n	10	10	10	10
Legal & Environmental Security	Pearson Correlation	-.218	-.218	-.156	1
	Significant (2-tailed)	.545	.545	.667	
	n	10	10	10	10

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

Table 6 demonstrates information gathered concerning the correlation between the items in the four dimensions of the security policy model. We observed that, where the correlation is low, it does not entirely signify a misconception of the principles and practice of security controls adopted in the construction of the security models.

Therefore, one notes that the report shows the level of inherent control risk that the management of the sampled industries is prepared to shoulder, indicating that the model was planned for such coverage.

CONCLUSION

The current study analysed the validity of the security models operating in the automobile industries in the ABC region of Metropolitan *São*

Paulo city. The objective envisaged the precision of the factors PHSEC, LASEC, ADSEC & LESEC presented in the research instruments.

The analysis performed in this study clarifies the doubts that industries could not be entirely implementing security policies distant from the standards; sufficient to minimize the security risks to which that organization is exposed.

It was proved that the first hypothesis of this study, that the four pillars of information security policy comprehend the dimensions of Administrative Security, Physical Security, Access & Logical Security and Legal & Environmental Security because the items that constitutes the research instruments demonstrates the overall view of this concepts.

Upon analysis of the said dimensions, significant correlation is observed among the items that constitute the research instruments, thereby confirming the second supposition.

The objective of this study was not directed towards identifying more appropriate security tools for every policy implemented, since information security policy is a condition *sine qua non,* independent of the computer operating environment. Therefore, we suggest that further studies be developed towards proposing security softwares, that will be appropriate for diverse computer environments, classified as requiring minor, moderate or complex security.

REFERENCES

ALLEN, N.J.; MEYER, J.P. The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of Occupational Psychology*, v. 63, p.710-720. 1990.

GUERRA, S. Composition of Default Specifications, Journal of Logic & Computation; v.11 n.4, p.559, 2001.

MORGAN, A.G. Measurement Validity. *Journal of the American Academy of Child* and *Adolescent Psychiatry*. v.40, n.6, p.729-731, 2001.

POUNDER, C. The European Union proposal for a policy towards network and Information security, Computer & Security v.20 n.7, p.573, 2001.

APPENDIX – QUESTIONNAIRE

The phrases below refer [indicate at which extension] to the extension of how the security policy models were implemented in your organization. Indicate how much you agree or disagree with [what each phrase indicates[?] each one of the phrases. Respond by noting, in the parentheses that appear in front of each phrase, the score (from 1 to 5) that better reflects [your belief that the security policy was actually implemented in that area[?] your answer.

1- Totally disagree, 2- Disagree, 3- Indifferent, 4- Agree, 5- Agree totally

Physical Security

( ) Installation of physical equipments
( ) Usage of the equipments
( ) Backup of data, program files, applications and databases
( ) Contingency & Disaster Recovery Plans
( ) Structural / Architectural design & maintenance

Logical & Access Security

( ) Customization of access authorization and authentication
( ) Data protection parameterization
( ) Hiring & Firing access control procedures.
( ) Accountability and access log
( ) Monitoring procedures
( ) Security violation reporting;

Administrative Security

( ) Delegation of security duties
( ) Implementation of security awareness programme
( ) Value-added concern for implementation of security resources
( ) Chief Security Officer installation of security policies
( ) Signing letter of compromise
( ) Punishments for the transgression of the security policy

Legal & Environmental Security

( ) Treatment given to obsolete hardware
( ) Compliance with the piracy laws
( ) Compliance with the federal laws relating to data security
( ) Executorships and penalties for transgressors

Responsibility for Security Policy:

Indicate with X who is directly responsible for the activities of security administration in your industry:

( ) CEO-Chief Executive Officer
( ) Chief Security Officer
( ) CIO-Chief Information Officer
( ) Technical Support
( ) Systems Analyst
( ) Others