



ORIGINAL

## Improving the security and reliability of a Quality Marketing Information System: a priority prerequisite for good strategic management of a successful entrepreneurial project

### Mejorar la seguridad y fiabilidad de un Sistema de Información Comercial de Calidad: un requisito previo prioritario para la buena gestión estratégica de un proyecto empresarial de éxito

Khalid Lali<sup>1</sup>  , Abdellatif Chakor<sup>4</sup>  

<sup>1</sup>University Moulay Ismail, Polydisciplinary Faculty, Meknès, Errachidia, Morocco.

<sup>2</sup>Mohammed V University, Faculty of Legal, Economic and Social Sciences, Souissi, Rabat, Morocco.

Cite as: Lali K, Chakor A. Improving the Security and Reliability of a Quality Marketing Information System: A Priority Prerequisite for Good Strategic Management of a Successful Entrepreneurial Project. Data & Metadata. 2023;2:40. <https://doi.org/10.56294/dm202340>


Received: 01-03-2023

Revised: 27-03-2023

Accepted: 07-05-2023

Published: 08-05-2023

Editor: Prof. Dr. Javier González Argote 

Guest Editor: Yousef Farhaoui 

Note: Paper presented at the International Conference on Artificial Intelligence and Smart Environments (ICAISE'2023).

#### ABSTRACT

Thanks to the security policy of the marketing information system which includes physical, administrative and logical safeguards, organizations are today able to design marketing and sales strategies that enable them to effectively respond and satisfy their customers' needs and expectations in a timely and cost effective manner and this by protecting the relevant information and data circulating in the said information system against any attempt at attack or malicious intrusion which seeks only to harm its reliability, confidentiality, integrity, availability and credibility. Indeed with this security policy we arrive easily to identify each discrepancy observed in the behavior of persons accessing this marketing information system as well as each mismatch between the service provided to users and the service expected by them, a context that pushes this security system to generate automatically some countermeasures such as encryption, decryption, hashing, electronic signature, intrusion detection and prevention and certification.

**Keywords:** Marketing Information System; Cryptography; Hashing; Intrusions; Encryption; Decryption.

#### RESUMEN

Gracias a la política de seguridad del sistema de información de marketing que incluye salvaguardas físicas, administrativas y lógicas, las organizaciones pueden hoy diseñar estrategias de marketing y ventas que les permitan responder y satisfacer eficazmente las necesidades y expectativas de sus clientes de manera oportuna y rentable y esto protegiendo la información y datos relevantes que circulan en dicho sistema de información contra cualquier intento de ataque o intrusión maliciosa que sólo busque dañar su confiabilidad, confidencialidad, integridad, disponibilidad y credibilidad. En efecto, con esta política de seguridad llegamos fácilmente a identificar cada discrepancia observada en el comportamiento de las personas que acceden a este sistema de información de marketing, así como cada desajuste entre el servicio prestado a los usuarios y el servicio esperado por ellos, contexto que empuja a este sistema de seguridad a generar automáticamente algunas contramedidas como el cifrado, el descifrado, el hashing, la firma electrónica, la detección y prevención de intrusiones y la certificación.

**Palabras clave:** Sistema de Información Comercial; Criptografía; Hashing; Intrusiones; Cifrado; Descifrado.

## INTRODUCTION

Given the importance of regularly and instantaneously exchanging relevant information required by the the magnitude of the commercial transactions which are concluded by companies which have preferred to opt for investment in new information and communication technologies and more particularly the marketing information system where computer applications are integrated which are able to promote a good vision concerning: the orders established, delivered and paid; loyal customers as well as employees with distinctive skills, all managers intervening today in the business and corporate world are convinced that in order to resist the fierce competition exerted by other competitors and thus continue to exist for the longest time possible on the competitive market - especially given the great risks of intrusions and/or attacks likely to harm and cause the vulnerability of the said information system - it is absolutely necessary as a priority to ensure that the main lines of a security policy for the marketing information system are drawn up in order to guarantee the confidentiality, integrity and availability of the information used as a basic support for defining quality marketing strategies and which will be able to satisfy and respond quickly to the needs and expectations of customers.<sup>(1,2,3)</sup>

This work was thus an opportunity to focus on the importance of programming and taking into account the of tools such as the intrusion detection system and the intrusion prevention system, in order to be able to give confidence to users who will access these marketing information systems and who will then be convinced that they are secure and efficient tools. Starting from this indisputable reality, the problem we have tried to answer in this article is as follows:<sup>(4,5)</sup>

How does a manager manage to design an effective and robust marketing information system security policy capable of dealing with all attempts at attacks and intrusions and allowing the company to succeed in imposing its strategic and operational position and to continue to exist as long as possible in the business and corporate world?

Thus, and in order to answer this research problem, the following two hypotheses were established:

*Hypothesis 1:* the effectiveness and robustness of the security policy relating to the marketing information system are linked to the need to carry out before hand a good operational inventory explaining what must be secured and protected physically, technically, administratively and logically and which is also capable at the same time of highlighting the list of threats and risks considered drastic and which are likely to harm the operation of the said system without forgetting also to focus on the action plan to be programmed in advance and to be activated in the event of intrusion attempts or attacks that are likely to arise at any time.

*Hypothesis 2:* integrating a work team with irreproachable and respectable skills and which is coordinated by network and marketing information system administrators is a priority condition to guarantee the continuity of the operation of the said information system and the compliance with the provisions of the security policy that characterize it.

### **Planning a marketing information system security policy: a necessary condition to deal with malicious intrusion attempts**

With the appearance of information and communication technologies and the development of the software and computer applications market and an orientation of the leaders of organizations opting for the culture of working in a network, no one can deny today that the marketing information systems have been able to soften the complexity and heaviness of certain tasks weighing on the shoulders of employees without forgetting also the possibility of intelligently managing the secure access of certain users - having the rights of access to these marketing information systems - to crucial and vital information which is likely to provide satisfactory and effective answers to the requests that emanate from the latter.<sup>(6,7)</sup>

However, and despite the advantages provided by these marketing information systems and which are made possible mainly thanks to computer applications such as groupware, workflows and datamining, the risks and threats of attacks and/or intrusions continue to exist, thus risking calling into question the relevance, robustness and reliability of the information circulating and exchanged through these marketing information systems, which consequently imposes the imperative of designing an appropriate security policy which is supposed to plan in advance after a diagnosis and an in-depth analysis of the various drastic risks capable of arising and that the marketing information system will have to face, a certain number of measures and actions to guard against these risks and also to protect against abusive manipulation by malicious people.<sup>(8)</sup>

In this context, it should be specified that the security policy guaranteeing the proper functioning of the marketing information system must take into consideration the factors influencing the internal environment but also those impacting the external environment of the organizations that have these marketing information systems.<sup>(9)</sup>

Thus and in the same direction, it is therefore preferable to define a security policy capable of countering any harmful element aimed at the malfunctioning of a marketing information system and which sets as a priority the requirement to begin by clearly identifying what we want to protect and the actions to plan and take in

case of risk or attempted intrusions for personal abuse or on behalf of other people or companies appear.<sup>(10,11)</sup>

It is therefore in this case, for example, attempted theft or cases of force majeure such as fire, etc. On the other hand, and in order to ensure that our security approach can allow us to be on the right track, thus succeeding in safeguarding and preserving our black box which serves as a support for decision-making, which is composed of relevant information required for the smooth running of activities, managers are then led to opt for organizational determinism. In other words, the effectiveness of any security policy requires the need to revise the distribution and division of pre-existing tasks, thus opting for a new distribution of roles, activities and powers.<sup>(11)</sup>

The last phase characterizing the security policy of a marketing information system to be considered is the one emphasizing the management control of activities and the control of access to these system-based mechanisms.

Indeed, by management control we mean to answer the following main questions: who does what? When? Why? and how? From the same angle, access control to these marketing information systems is much more aimed at identification, recognition, authentication and predefined access authorization, all of which are made possible by the information system. marketing.

### **Features of an effective marketing information system security policy**

The information and data stored in a marketing information system which constitute a kind of organizational memory and which are the subject of exchanges and transfers between users having access rights to these devices are permanently in the obligation to face obstacles represented by attempts at intrusions and unexpected and illegal disguised and malicious attacks coming from inside but also from outside the organization such as backdoors and which call into question the confidentiality, integrity, availability and reliability of the information and data handled by these marketing information systems and whose added value no longer needs to be demonstrated. In this context, we recall that:

- *Reliability* reflects the adequacy that exists between the service provided to users and the service expected by them and which is regular and continuous over time.
- *Confidentiality* simply means that there is no possibility of spreading information stored in these marketing information systems in response to a given request without the user having prior authorizations recognized by fingerprints by this system.
- *Availability* reflects the capacity of the marketing information system to instantly provide favorable responses to user requests and to facilitate their access to this information without interruption or difficulty and within a reasonable time.
- *Integrity* means the inability to change or improperly modify the information or data stored in these marketing information systems and which are of a personal or professional nature.

### **Deviations in human behavior that may harm the security policy of the marketing information system**

In general, it can be said that there are always anomalies in human behavior or, to put it better, deviations in behavior compared to fingerprints initially saved and memorized by the security system of the marketing information system set up previously and which risks harming the proper functioning of this installed security system, thus generating a malfunction of the latter.

In this context, we can argue that we can encounter two types of anomalies or deviations of human behavior compared to ordinary and normal habitual behavior, namely internal deviations called design and/or development and those of interaction that appear in an accidental but also intentional way without the will to negatively affect the security system of the implanted marketing information system, but there is also the risk of facing or, better said, of being permanently exposed to another type of behavioral deviations that are either internal such as malignant logic - which are guided by the voluntary intention of negatively harming the correct and normal functioning of the policy and the security approach of the marketing information system implemented - without forgetting also the attempts devastating operational emanating from the outside which constitute what is called calculated and voluntary intrusions said to be intentionally harmful.

We note in the same context and returning to the first category of deviation from so-called interaction behaviors which are intentional without the intention of harming, that these types of behavioral anomalies can arise, for instance, from initiatives or actions carried out in order to thwart and to deal with situations that emerge in an unexpected and unanticipated way, thus unconsciously violating the security policy initially defined and put in place, without being able at this precise moment to unfortunately realize the real consequences of these actions taken. Malicious logics include a good number of intrusions manifested in different forms and having names such as Trojan horses, backdoors, logic bombs as well as so-called viruses and worms.

### **The diversified field of the marketing information system security policy's intervention**

In our view, a security policy represents a pragmatic and effective approach allowing an organization to

rationally manage access, distribution but also to carefully follow the routing that certain specific information called very sensitive circulating inside a marketing information system will follow and this in order to guarantee their conservation as long as possible and consequently avoid any intentional attempt to modify them, especially from attacks and/or intrusions caused by people seeking only to harm negatively to the normal functioning of this security system either for their own account or for the account of competing companies and who do not have the right to access these resources.

Thus, a good security approach requires first defining a set of rules and principles governing access rights to the gold mine of information stored in the marketing information system. These principles and rules are related to the confidentiality, to integrity and to availability of so-called relevant and interesting information circulating within this information system and which must be protected, thus making it possible to adequately define what is called the authorization scheme.

In general, it can be said that the security policy of a marketing information system includes three types of security, namely physical security, administrative security and finally logical security. Administrative security specifies and sets the scope of intervention and the limits of responsibility and powers to each member belonging to an organization as well as the new division of tasks decided upon.

Regarding physical security, the latter takes care to regulate physical access, doing so by routinely and instantaneously checking each participant's fingerprints. Logical security, on the other hand, is responsible for electronically verifying the identity of the person wishing to access information and checking, according to a so-called subject-object matrix, whether this person is indeed who he claims to be and whether he has or not the right of access to the desired information.

Then and after having verified his identity and whether or not the person has the right of access, the security mechanism of the marketing information system triggers the permission, authorization or prohibition so that the person can or not benefit from the service or even the information sought.

### **An action plan explaining the countermeasures to be mobilized in a security policy for marketing information systems: an unavoidable priority**

To strengthen the security of the marketing information system and fill the gaps demonstrated by the security policy defined by the decision-makers, the need to provide countermeasures is essential. It is then a question of implementing actions such as encryption, decryption, hashing and the electronic signature, which represent the basic functions of cryptography as well as the detection and prevention of intrusions and certification.

- The basic principle of encryption is to rewrite a clear, readable and understandable text into another in the form of secret codes, using numbers and using what is called an encryption key. On the other side, the decryption is responsible for returning to the original initial text using a decryption key but also decryption algorithms.

- The hash function does not rely on secret codes as is the case for encryption and decryption and makes it possible to identify and generate the main fingerprint characterizing a message or a text without there being any chance that two different texts have the same imprint.

- The automatic generation function of signatures is based on using a signature key and whose verification is supposed to always give negative answers as a result meaning that the person having this signature is well recognized and that its signature is identical to that stored by the security system of the marketing information system installed.

- The certification also aims to verify if what the person declares as identity is really his and that he is really what he claims to be, that is to say that he does not lie and finally also ensures that non-repudiation is respected and which allows us to be convinced that the person who has had access to information and who has used it cannot deny that she has done so and realized it previously.

## **METHODS**

Given the very limited number of research works and scientific publications relating to the security of marketing information systems and given the importance of cultivating this new orientation in the minds and mentalities of administrators of networks and marketing information systems as well as with other users of these mechanisms in order to guarantee a certain sustainability in terms of the normal and efficient functioning of said information systems dedicated to managing access to and exploitation of data and information of capital value and creator of added value, the nature of our research is therefore descriptive, exploratory and analytical. In the same context and given all these considerations, we can then affirm that our main objective through this modest article is therefore centered around the following points:

- Sensitize decision-makers as well as managers dealing with the management of marketing information systems of the need to draw up a list of the various anomalies, attacks and/or malicious intrusions risking calling into question the security policy of the marketing information system that must be chosen and put into

place later.

- Enable administrators of networks and marketing information systems to demonstrate great speed in terms of anticipating intrusion attempts and in terms of intervention by taking care to decide on the preventive measures to be taken for the counter and eliminate them.

From all the above and in order to be able to respond to our problem mentioned at the beginning of this article and therefore verify the relevance and validity of our two pre-established hypotheses, we have established an interactive version of a questionnaire that we have sent to the managers and specialists in security of marketing information systems which come from organizations carrying out commercial activities and which are installed in Morocco without forgetting also some university teachers specialized in this field and whose answers to the questions of our conducted survey were at the origin of the constitution of a quantifiable database.

In this context, it is clear that:

- Responses were entered and processed using SPSS software.
- Data processing was carried out using Correspondence Factor Analysis (CFA) since it is a qualitative variable followed by dynamic cluster analysis

It is also important to specify that once after collecting the data from the respondents, we codified and entered them and then, in order to verify the accuracy and validity of each of our two established hypotheses, we took care to define for each hypothesis two variables as well as the indicators which are associated with it and in this way and by resorting to the combined analysis of each two variables delimiting each hypothesis then and by applying to them the Correspondence Factor Analysis and the analysis in dynamic clusters in two classes we were therefore able to come out with deductions and results approving the validity of each of our two hypotheses and which will be detailed later in the context of this modest work.

## RESULTS AND DISCUSSION

According to our analysis carried out and relating to the highlighting of the specificities and characteristics of the security policies of the marketing information systems relating to our sample of companies surveyed, we came out with the following results:

- 62 % of those surveyed are male while 38 % are female.
- 28,8 % of those surveyed said that these security policies are rather aimed at eliminating any attempt to destroy or alter data and which are due to attacks or unexpected incidents;
- 33,5 % of individuals surveyed said that the particularity of these security policies is that they are oriented against the disclosure of confidential data due to intrusion, attacks by pharming, phishing or by accident;
- According to 36,2 % of participants in our survey, these security policies consist of managing the sometimes unavailability of marketing information system services due to an external attack (denial of service attack for example);
- Finally, we note that 1,5 % of the people surveyed did not give us their opinion concerning the existence of a security policy for marketing information systems intended to counter certain unexpected risks likely to appear in organizations where they practice.

Regarding the actions ordered by the hierarchical superiors of the companies surveyed in order to successfully implement the various data security policies circulating within their marketing information systems, we were able to note the following results:

- According to 21,4 % of the people surveyed, these actions consist of establishing physical access controls to the servers (using, for example, badges, biometrics, etc.);
- According to 40,6 % of the individuals surveyed, these actions undertaken by the entities which are under investigation consist in carrying out remote access controls by firewall (firewall, software, etc.);
- For 35,8 % of survey participants, these actions consist of securing mobile devices (example: password control, etc.);
- Finally, we note that 2,2 % of people did not want to reveal to us the various actions carried out by the the hierarchical managers of the organizations in which they work in order to achieve the data security policies of their marketing information systems.
- According to 75,2 % of those surveyed, the security policy of the marketing information system defined and decided by their hierarchical superiors is said to be flexible and has enabled this marketing information system to demonstrate a high level of interoperability; to promote the instantaneous and rapid exchange of relevant information between users with diverse profiles; easily handle a voluminous mass of sensitive and heterogeneous personal and professional information; to stimulate the spirit of collaboration and communication with users who have access to this marketing information system; and to create a climate of trust and transparency between the participants accessing this marketing information system and this through the applications which

are integrated into it and which are characterized by their capacity to interact instantaneously with each other and to provide answers of quality to the requests expressed by the users of said marketing information system. On the other side, we have 24.8% of people who do not share the same opinions and who say that the security policy designed unfortunately does not allow either the marketing information system or the users who access it to obtain the advantages advanced by the first category of people.

- According to 81,4 % of those surveyed, the security policy of the marketing information system made it possible to guarantee the confidentiality, integrity and availability of the information and data circulating in the said information system against 18,6 % of people who do not share the same opinion as that advanced by the first category.

- For 69,6 % of those surveyed, the security of the marketing information systems available to the organizations where they work was carried out and helped above all by a good inventory carried out previously by the managers of the said organizations and which preceded the definition the main lines characterizing the said security policy and which was characterized above all by the prior determination: of the technical, human, logistical and financial resources constituting its main strengths as well as the gaps in terms of computer security from which these organizations suffer and that need to be addressed urgently; the software solutions, computer applications and hardware to be acquired; the list of risks of attacks and dangerous intrusions likely to cause vulnerability in the marketing information system; anticipating the countermeasures to be activated in the event of a subsequent appearance of intrusions or attacks; without forgetting also finally the list of authorizations, permissions, prohibitions and obligations to be defined and that each user of the said information system is supposed to respect thereafter. On the other side, we have 30.4% of people who do not share the same convictions and declarations as the first category of people questioned.

- According to 60,45 % of those surveyed, the effectiveness and robustness of the security policy of the marketing information system was the result of human capital responsible for carefully monitoring compliance with said security policy and which has distinctive skills including: its ability to successfully audit and analyze the risks of attacks or intrusions as well as their consequences; its ability to quickly detect anomalies in human behavior and those also relating to the marketing information system and which undermine its security policy put in place; its ability to easily verify the identity and the accuracy of the access rights declared by the users of said information system; its capacity for in-depth analysis of the various communication channels as well as the interaction that exists either between each user and the marketing information system but also that which takes place between users among themselves; and which is also distinguished by its accumulation of great years of know-how and know-to act. On the other hand, we have 29,55 % of those questioned who advance that the security policy of said information system has not been a success because the human capital to which the task of controlling the proper execution has been assigned and compliance with the regulatory provisions governing it do not have the skills explained by the first category of people surveyed.

## CONCLUSION

Managers of innovative and entrepreneurial projects within the framework of small and medium-sized enterprises which operate permanently in a constantly changing competitive market where they are always forced to face the fierce competition exerted by other competitors in order to strengthen their strategic position and also trying at the same time to open new other niches and profitable investment opportunities, are more than ever convinced that in order to ensure safety concerning the routing of relevant information from a marketing information system , it is absolutely necessary to design a security policy for said information system which is considered today as a priority or even a condition for survival and a determining factor alone capable of enabling the company to meet the challenge of its sustainability in a world ever-changing business and enterprises.

Indeed, the protection of this information which traces the list of the various partners of these companies as well as the history of the commercial transactions concluded by the latter on which their business depends and which are the subject of intrusion attempts - which are likely to cause a malicious diversion, a modification of the information thus generating a dysfunction at the level of the interaction taking place between the users and the marketing information system as well as at the level of the interaction existing between the users between them- has become today a question of life or death for these organizations and which therefore imperatively implies making diagnoses, even an in-depth inventory, in a preliminary stage, but also analyzes which are both capable of tracing the main lines of a real intrusion detection system as well as those relating to the intrusion prevention system.

In this context, we specify that in order to continue to show great rapidity at the level anticipation of drastic threats and at the level intervention and this through the stimulation of countermeasures capable of dealing with the risks of intrusions which seek to at all costs to harm the reliability, confidentiality, integrity, availability and credibility of the information circulating within a marketing information system, the managers of small and medium-sized companies must define a security policy for said information systems that must obey

well-defined rules and principles.

Admittedly, it is obvious that these security policies will enable a network and marketing information system's administrator to guarantee physical, administrative, technical and logical security and who clearly explains in advance the list of authorized persons having the access rights as well as the data and information to which they each have the right to access and whether or not they can modify them while making sure to also prepare in advance the procedures to be generated in the event of identification of a deviation observed in the behavior of people accessing this marketing information system in relation to a reference made up of a set of attack scenarios known in advance and which are deemed to be destructive or in relation to a list of behaviors known and mastered in advance and which are considered normal and finally we also cite the deviations observed in the functioning of the system itself, especially when there is an inadequacy between the service provided to users and the service expected by them.

By doing so, organizations opting for such an orientation will easily succeed in strengthening the commercial links which bind them with a specific range of their oldest customers and endowed with certain specific characteristics, thus succeeding in continuing to make profit margins and to continue by therefore to exist as long as possible in the competitive market.

## REFERENCES

1. Bennani A-E, Laghzaoui S. The articulation between the monitoring of the company's environment and the information system: The contribution of a systemic approach. *Int J Econ Intell.* 2009;1(2):257-270.
2. Bertino E, Ferrari E, Atluri V. The specification and enforcement of authorization constraints in workflow management systems. *ACM Trans Inf Syst Secur.* 1999;2(1):65-104.
3. Brien RH, Stafford JE. Marketing Information Systems: A New Dimension for Marketing Research. *J Mark.* 1968;32(3):19-23.
4. Chandola V, Banerjee A, Kumar V. Anomaly detection: A survey. *ACM Comput Surv.* 2009;41(3):1-58.
5. Cox DF, Good E. How to build a marketing information system. *Harv Bus Rev.* 1967;45(3):145-154.
6. Denning DE. An Intrusion-Detection Model. *IEEE Trans Softw Eng.* 1987;13(2):222-232.
7. De Séréville E. In terms of information systems security, are normalization and standardization factors of efficiency? *Int J Econ Intell.* 2009;1(2):271-287.
8. Goudalo W, Kolski C, Vanderhaegen F. Towards advanced engineering for enterprise IS security: A joint approach to security, usability and resilience in socio-technical systems. *Inf Syst Eng.* 2017;22(1):65-107.
9. Majdalawi YK, Hamad F. Security, Privacy Risks and Challenges that Face Using of Cloud Computing. *Int J Adv Sci Technol.* 2019;13(3):156-166.
10. Ruault J, Kolski C, Luzeaux D, Vanderhaegen F, Goudalo W. Built-in resiliency of system safety and security: Monitor the system and alert operators to navigate on sight. *Software Eng.* 2016;117:2-12.
11. Vistro DM, Rehman AU, Mehmood S, Idrees M, Munawar A. A literature review on security issues in cloud computing: Opportunities and challenges. *J Crit Rev.* 2020;7(10):1446-1455.

## FINANCING

No financing.

## CONFLICTS OF INTEREST

There are no conflicts of interest.

## AUTHORSHIP CONTRIBUTION

*Conceptualization:* Khalid Lali, Abdellatif Chakor.

*Data curation:* Khalid Lali, Abdellatif Chakor.

*Formal analysis:* Khalid Lali, Abdellatif Chakor.

*Research:* Khalid Lali, Abdellatif Chakor.

*Methodology:* Khalid Lali, Abdellatif Chakor.

*Writing - original draft:* Khalid Lali, Abdellatif Chakor.

*Writing - revision and editing:* Khalid Lali, Abdellatif Chakor.