Strategic balance between prevention and response and adherence of employees to security policies in information security: a case study

Abstract

Information has become one of the most important assets for maintenance of organizations. The growing concern regarding the protection of these assets should be considered by the board of managers and by the company's employees. This study aimed to identify the strategic balance between company's prevention and response actions and adherence of employees to security policies in information security in a company of towed cars, located at Brazil. The qualitative research was conducted through an interview with the coordinator of IT and a quantitative approach was used through a questionnaire applied to 40 employees. The results show that the company's policies and the employees' intention to cooperate are in consonance. The company's efforts to provide a robust information security is perceived and followed by its employees. A limitation of this work is its application in a company with headquarters in Brazil and mechanical metal branch.

Keywords: IT security policies, prevention, response, adherence of employees.

1 INTRODUCTION

Over the years the information has become one of the most important assets for competitiveness and maintenance of organizations. Thus, the growing concern for the protection of these assets has been increasing steadily, considering the emergence of new threats, whether technological or human. For the protection of information is necessary, therefore, to take new actions to mitigate the risks that are generated by these threats.

The Center for the Study, Response and Treatment of Security Incidents in Brazil recorded 352,925 incidents related to Information Technology only in 2013, lower than the 466,029 cases reported in 2012, with more than 61% of reported incidents being attacks from the country itself. To reduce the risks related to the loss of information by companies, the center has a number of support services to users and network administrators, materials, and projects that seek to better understand the nature of the threats to Information Technology and technologies capable of better capacity in incident responses (CERT.br, 2014).

This study sought to understand the existing strategic balance between prevention and response and adherence of employees to security policies for information technology at a large company, in the segment of road equipment, located in Brazil. In order to achieve the objectives of this study, a questionnaire of 22 objective questions was applied to 40 company's employees, who identified issues relating to company's safety procedures on IT adherence, based on Siponen's et al (2014) model. Also, an interview with company's IT coordinator was made, based on Baskerville's et al (2014) model, which contained ten questions in order to determine the strategic balance between company's prevention and response related to information security issues.

However, it is necessary to consider the performance of other asset of great importance for organizations: people. Therefore, the commitment of employees to the procedures and techniques related to security of information technology is of utmost importance for the maintenance of corporate information.

2 LITERATURE REVIEW

2.1 Data and Information

From the point of view of the theory of decisions, the organization can be viewed as a structured set of information networks linking the information requirements of each decision-making process to the data sources. Although separate, these information networks are overlapped and interpreted in a complex way.

Chiavenato (2000) says that the data are the elements that are the basis for forming judgments or solve problems. A data is just an index, a record, a straightforward, open to a subjective analysis, that is, it's necessary to consider the interpretation of the person handling them. In itself, the data have little value. However, when classified, stored and interrelated, the data allow obtaining information. Thus, the isolated data are not significant and do not constitute information. The data require processing (sorting, storage and networking), so that they can gain meaning and consequently inform. Information has meaning and intentionality, aspects that differentiate it from the concept of data.

Information consists of greater value to businesses. Balloni (2002) says that currently information has a highly significant value and can represent great power to whoever possesses it, whether person, whether the company. The information is presented as a strategic resource from the perspective of competitive advantage. It has value because it is present in all activities involving people, processes, systems, financial resources, technologies and so on.

Information is a substrate of competitive intelligence and should be administered in their particular, differentiated and safeguarded. It serves as an essential resource for the definition of alternative strategies and to form a flexible organization where learning is constant.

According to Rezende and Abreu (2000), information plays important roles both in defining and implementing a strategy. It helps in the identification of threats and opportunities for the company and sets the scenario for a more effective and competitive response.

Not all information is critical or essential to deserve special care. In addition, certain information can be vital that the cost of their integrity, whatever it is, is still lower than the cost of not having it properly. Boran (1996), Wadlow (2000) and Abreu (2001) classify information on priority levels, respecting the needs of each company as well as the importance of information classes for the operations of the company:

a) public: information that can be made public without further damaging consequences for the normal operation of the company, and whose integrity is not vital;
b) internal: the free access to this type of information should be avoided, although the consequences of unauthorized use are not too serious. His integrity is important, even if not vital;
c) confidential: restricted to the boundaries of the enterprise, the disclosure or loss can lead to operational imbalance, and eventually, to financial losses before or reliability in front of the external customer;
d) secret: critical information for the activities of the company, whose integrity must be preserved at any cost and to which access must be restricted to a small number of people. The safety of this type of information is vital for the company.

Regardless of the type or relevance of the information, the management of organizational data is strategic because it allows decision-making in any institutional framework. In fact, some information is central to the organization, and its total or partial disclosure may cause repercussions whose complexity may be little or nothing manageable by the organization. It is necessary to be careful about the completeness, accuracy, timeliness, interpretation and general information value.

The disclosure of confidential or secret information by the elements that participate in the organization is on a serious lack of ethics and morals, according to Sá (2001). According

to Mota and Amorim (2001), in the knowledge economy, the disclosure of organizational data or information can bring economic loss or damages.

2.2 Basic Concepts of Information security

2.2.1 Confidentiality, Integrity and Availability

According to Krutz and Vines (2001), the triad that makes up the basics of information security are: integrity, confidentiality and availability. When applied, these principles allow to adopt controls and measures related to information security, reducing, among others, the risks of leakage and unauthorized disclosure of information, financial fraud, misappropriation of information, reputation of the image of the institution:

a) integrity: principle that deals with the protection of information or information assets against unauthorized creation or modification. Loss of integrity may be related to human error, intentional or contingency actions. The loss of integrity of information can make it worthless, or even makes it dangerous. The consequence of using incorrect data can be disastrous.
b) confidentiality: principle that deals with the availability of information to authorized persons only. Controls should be implemented to ensure that access to information is always restricted to those people who actually need to have them. Many cybercrimes happen through breach of confidentiality and information theft. One can consider two distinct moments of this principle: be confidential and remain confidential. The information to be confidential must be rated to determine the necessary safety measures when it is being treated. Remain confidential means that the means used to handle information allows adequate protection.
c) availability: principle that deals with preventing that information or information resource is unavailable when requested by the customer, the regulator or even the institution itself. Applies not only to information, but also to electronic channels, a network equipment and other elements of the technological infrastructure. Not getting access to a feature desired information is called denial of service, technique very used by hackers. Intentional attacks on technology infrastructure may have intended to make them unavailable data, as well as steal information.

2.2.2 Information Security Policy

The information security policy is one of the main instruments for achieving the Management of Information Security within an organization (FERREIRA; ARAÚJO, 2006). It consists of a set of rules and standards for the protection of information and services that are important to ensure the confidentiality, integrity and availability (FERREIRA; ARAÚJO, 2006; MARTINS; SANTOS, 2005; CAMPOS, 2007). The information security policy is the document that best defines the rules and the best practices of information life cycle which according Sêmola (2003) are divided into: handling, storage, transportation and disposal of information, and the document of policy information security is the essence for the occurrence of prevention and protection of information.

The information security policy needs to establish institutional principles of how the organization will protect, control and monitor their computing resources and, consequently, the information handled by them. It is important that the policy describes who are responsible for the functions related to security and key threats, both if oriented to risks or impacts involving the process (FERREIRA; ARAÚJO, 2006).

The document of information security policy consists of guidelines, standards and procedures (NAKAMURA; GEUS, 2002). The guidelines are the elements that will guide actions within an organization and future implementations in an overall way, while the rules describe situations, environments and processes giving specific guidance to the appropriate use of information. The procedures that are used to users can actually fulfill what was defined in the policy document.

The three basic principles, according to NBR / ISO IEC 17799:2005, confidentiality, integrity and availability constitute a basic paradigm of information security and should be part of the policy document. However, before its development is important to perform risk management so that you can know the real threats and thus achieve information security management more efficient without financial waste or waste of time.

2.2.3 Risk Management

In literature there are many definitions of risk and its importance in conducting projects in any area. In the area of information security, risk management or risk analysis is critical to the decision making process, as at this stage is held scoping and prioritization of assets to be protected (LICHTENSTEIN, 1996).

The process of analyzing the risks consists in the probability that there is a loss characterized by a threat against a specific asset. When this concept is applied to information technology, it is associated with the possibility of loss of availability, integrity and confidentiality (MARTINS, 2003).

According to Campos (2007) the steps that comprise the process of risk management are: to examine the context of risk, identify risks, analyze risks, evaluate risks, treat risks, monitor and review, communicate and consult.

To perform risk treatment is necessary to involve the determination of the most appropriate strategies to deal with their occurrences. According to Zhi (1994) there are four strategies to respond to project risks:

a) avoid: not adopt technology or processes that offer business risks. The way to deal with these risks can generate new higher risk than the benefit he may come to bring, so it is chosen to avoid;
b) transfer: the treatment of these risks is transferred to third parties or to other sector being a viable alternative when your treatment is charged on the cost of implementing the project;
c) reduce: mechanisms or controls that have action to mitigate the risk encountered are adopted;
d) accept: to accept the risk could be a possibility if he does not offer much threat, but one must be aware that there is the risk this way, so it’s necessary the continuous monitoring so that it will not increase.

These strategies of risk treatments will be important to conduct the work, because from this definition of risk is to be taken appropriate action for the implementation of information security.

2.2.4 Methodologies of Information Security Management

With the dissemination of standards related to information security and the higher interest of companies focused on protecting their biggest asset, information, studies have been published, presenting new methodologies for implementing a safety management system of

organizations information. Below we discuss some of these studies have relevance to the methodology proposed in this article.

According to Martins and Santos (2005), the factor resulting from the implementation of a Management System of Information Security is the standardization and documentation of procedures, tools and techniques, creating indicators and records as well as the definition of a educational process of awareness within the organization and its partners. This author proposes a theoretical and conceptual methodology following the PDCA cycle of continuous improvement to assist in building a Management System of Information Security based on international standards (TECSEC, 1985, ISO 15408:1999; B7799-2: 2001) presenting managerial points on your driving.

Brooks and Warren (2006) present a methodology for development of health information security techniques based on Unified Modelling Language (UML). In this model, four steps are set out for its implementation. The first and most important is the modeling and implementation of the scenario in which the methodology is applied seeking to map the entire environmental context aided by UML techniques in order to obtain the level of security for that ideal environment.

A study by Vermeulen and Solms (2002) presents a framework and the use of a tool to guide the process of implementation of a methodology for managing information security. The tool called ISMTB (Information Security Management Toolbox), which consists of a number of questionnaires based on the standard of BS 7799-1 (1999), aids in the understanding and characterization of the process, identifies the current security level and serving to determine which security measures that will be taken from this analysis.

In these methodologies of Management Information Security proposed by Vermeulen and Solms (2002) and Martins and Santos (2005), it's recognized that the practice of risk management has an important role in the implementation of the process of safety management, however, they perform the subsequent step of risk analysis establishing the information security policy. In fact, in the globalized world we live in where time is synonymous of money, many organizations seek agility in income and end up choosing to have the policy document as a first step to implementing a security management information before performing the risk analysis stage. However, this choice is due to the fact that this stage is characterized as overly complex according to Martins (2003) and also require some time, a factor that companies do not have or want to have. However, many IT projects fail because of the inefficiency and because do not prioritize the step of risk management (BACCARINI ET AL, 2004).

2.2.5 Information Security

Currently the information is a strategic weapon in any company and is also a vital resource in organizations. Information security is a feature that aims to protect and is also a way of management. "Information security of a company ensures, in many cases, business continuity, increases stability and allows people and goods to be secure from threats and dangers" (BLUEPHOENIX, 2008).

Information is everywhere and can be stored in printed papers, electronically in files and databases, in images or videos and even in conversations between employees. But the importance of information is only recognized when it is destroyed, lost or even stolen. "The cost to protect itself against a threat should be less than the cost of recovering if the threat attain" (BLUEPHOENIX, 2008). Cost in this quote means determining the amount of losses in both money and the organization's reputation, trust and other assets that the organization maintains as its mission.

To deploy a project of information security in an organization is necessary first to establish guidelines, security mechanisms, policies and procedures, protection and authentication tools, and its cost benefit ratio. Establish the level of security is crucial. This security level must ensure that each employee can only access to permitted content, for example an accountant should only have access to information content which is part of his job and cannot access a data that is related to another department that has no relation to the functions in which he plays. What this example shows is that the information must be secure and available only to those who are authorized. " In organizational terms, the information has a vital role with regard to the management, organization and maintenance of entities The value that information represents is not measurable and may result in stops, loss of productivity, disorganization and instability" (BLUEPHOENIX, 2008).

In order to establish this policy, it's necessary to take into account the risks related to lack of security, the benefits and the costs of implementation of mechanisms. The risks associated with lack of security represent data that can be lost with a bug in the database, for example. Hackers can take advantage of these faults and be able to infiltrate into the organization's system. Once inside the enterprise system, they have access to all the data related to the organization and customer data. Also you need to consider the occurrence of natural factors such as fires, floods and earthquakes.

The expected benefits are to avoid leaks, fraud, commercial espionage, misuse, sabotage and many other problems that might affect the company. Security also aims to increase employee productivity through a more organized environment and enable critical applications of enterprises. The costs of implementing mechanisms vary according to what the organization intends to implement.

Wadlow (2000) states that security is not a technology. It's not possible to buy a device that will make your network secure, as well as it is not possible to purchase or create a software capable of making your computer safe. The fallacy of these promises is based on the security implications of being a state that can be achieved. This is not possible. Security is the direction in which one can travel, but never actually reaching the destination. Also says:

> Security is a process. You can repeatedly apply the procedure to the network and to the company that maintains it and, thus, improve system security. If you do not start or stop the application process, your safety is getting worse, as new threats and techniques emerge.

Security is related to the need for protection against access or manipulation, intentional or not, of confidential information by unauthorized elements, and unauthorized use of the computer or its peripheral devices. The need for protection should be defined in terms of the possible threats and risks and objectives of an organization, formalized in terms of a security policy (SOARES, 1995).

> In this globalized world, where information cross borders with astonishing speed, protection of knowledge is of vital importance for the survival of organizations. A failure, a communication containing false information or information theft or fraud can have serious consequences for the organization, such as loss of market, business and consequently financial losses (NAKAMURA, 2002).

3 METHODOLOGY

In order to achieve the objective of this research, it was used the case study method, which constitutes an ideal approach when it's necessary to get a deeper understanding of the searched object (YIN, 1994). For reasons of confidentiality, the name of the company object of this study is not cited in this article. This organization was chosen by the leadership role it plays in its segment and the economic importance it represents for the city and region.

The scientific method is defined as a set of technical and intellectual procedures aiming to attain knowledge or knowing certain reality (GIL, 1995), i.e., the method identifies trough which way the goals proposed in this research will be achieved. The research presented in this paper aims to analyze the relationship between the strategic balance between the company's prevention and response to IT security and adherence of employees to security policies in IT.

In order to collect data related to employees, it was used a quantitative approach, with applied nature and exploratory and descriptive goals, which is meant to describe specific features or functions of a given population or sample (MALHOTRA, 2001). To collect data, it was used a questionnaire of 22 objective questions, using a Likert seven-point scale, with the purpose of the adherence of employees to security policies of IT in the studied enterprise, according to the model of Siponen et al (2014). Thus, the questionnaire includes three questions related to perceived vulnerability, three questions about the effectiveness of response, two about attitude, two questions relating to self-efficacy, four questions about normative beliefs, two questions that focused on rewards, two questions on perceived severity, two related to the current agreement and finally, two questions concerning to the intention to collaboration. Figure 1 shows the objectives of each block of questions.

Figure 1 – Objectives of each block of questions

Block of Questions	**Objective**
Perceived Vulnerability	Determine the employee's perception about the level of threat that both he and the company are exposed.
Efficacy Response	Determine the employee's confidence in the measures of response to threats.
Attitude	Determine the awareness related to the importance of compliance with IT security policies
Self Efficacy	Determine the independence of the employee to take measures concerning to the IT security
Normative Beliefs	Determine the belief concerning to determine compliance with IT security policies
Rewards	Determine the level of expectation of rewards for compliance with safety standards in IT
Perceived Severity	Determine the perception of risks in IT security breaches
Current Agreement	Determine the level of cooperation policies for IT security
Intent to Collaboration	Determine the level of intent for collaboration policies for IT security

Source: Made by the authors.

The questionnaires were sent in January 2014 to 50 employees of the company, with a response time of 10 days. After this period, 40 questionnaires were returned, featuring a response rate of 80%. After the return of the questionnaires, we proceeded to the quantitative analysis using the software IBM SPSS Statistics 21, in order to verify trends in employee responses regarding the adherence of employees to security policies in IT.

This research can also be classified as a qualitative and exploratory study. The qualitative study concerns to the purpose of understanding more thoroughly the study, without

the need for statistical fact, using a selection of small and not representative samples. According to Minayo (1996), the qualitative research encompasses the world of meanings of actions and human relationships, a task that would not be possible through the use of equations and statistical formulas. According to Gil (1995), the goal of an exploratory research is to enable greater familiarity with the problem, making it more explicit, and, in most cases, this involves a literature search, interviews with people who have had practical experience with the topic researched and analyzed case studies that promote understanding. To Vergara (2006), the aim of the exploratory study is to contribute to the familiarity of the researchers on the subject investigated.

Therefore, it was conducted a structured interview with the coordinator of IT, based in the model described by Baskerville et tal (2014), which contained ten questions in order to determine the company's strategic balance between prevention and response to IT security. The questions were about security measures, security management, security risks, and response to security breaches. The interview took place in the company, and lasted approximately two hours. Figure 2 shows the data collection techniques used in this research and their purposes.

Figure 2 – Technics of data collect used in the research

Step	**Technique**	**Finality**
I	Literature Review	Identify authors in the literature that discuss the importance of resources for competitive advantage, as well as methods for resource assessment.
		Support the completion of fieldwork.
II	Structured Interview	Identify the perception of the IT management of the studied company on IT security.
	Questionnaire	Identify the perception of the studied company employees on IT security.

Source: Made by the authors.

4 DESCRIPTION OF THE ENVIRONMENT RESEARCH

Considered the second largest exporter in the Americas, Brazil has 1300 road equipment companies, employing more than 83,000 people with revenues in 2013 of approximately R$ 9.3 billion (SIMEFRE, 2014). The production of trailers and semi-trailers in Brazil, in 2013, reached 174,400 units, with 5,400 intended for export (SIMEFRE, 2014). Companies of Rio Grande do Sul produce over 50% of the national total in this segment with 20,324 posts of work (SDPI, 2012).

The first industries of the towed vehicle industry emerged in the early '50s. This sector brings together more than a thousand small, medium and large companies, predominantly family enterprises, responsible for the manufacture of road equipment with various configurations and profiles. From the beginning, the industries of road equipment industry had to manufacture their products observing the characteristics of the Brazilian road network, which includes unpaved roads or in non-ideal conditions of trafficability (SDPI, 2012).

The growth of the primary sector, industry, trade and services impact the development of towed vehicles sector. The road equipment industry develops products and complementary accessories to the truck, giving them a role in cargo transportation. This industry produces towed vehicles, trailers, semi-trailers and superstructures, and accessories such as buckets and truck bodies on chassis, auxiliary axles and fifth wheel. The versatility of this industry allows you to have all varieties of equipment, both in the aspect of dimensions, such as specifications of the most sophisticated, quality, durability, etc. (SDPI, 2012).

Brazil is among the largest producers of auto vehicles and reached a production of 3.4 million vehicles in 2011. Consequently, Brazil is also one of the largest markets for towed vehicles (SDPI, 2012). The share of road, rail and water transport in the Brazilian modal loads is significantly different from that found in other countries of continental dimensions. In Brazil there is a large concentration of freight transportation in road transportation. Typically, countries with large territorial extension use more intensively the railroad (SDPI, 2012).

Exports of towed vehicles still represent very little turnover in the companies. This fact is due to the characteristics of each market, that requires customization because of the peculiarities of the laws of each country and the logistical difficulties associated with transportation of implements. An alternative to solve the problem of characteristics that each market demand is the realization of exports through the CKD system. The main export markets for Brazilian companies of implements are countries from Mercosul, Africa and the Middle East (SDPI, 2012).

The company studied is part of a conglomerate of 11 companies, active in automotive spare parts, services and implements rail-road sectors. The company's net revenue was R$ 3.9 billion in the period between January and November 2013 and the company has 4127 employees (RANDON, 2013).

5 DISCUSSION OF RESULTS

Regarding the vision of the studied company on the relationship of the strategic balance between the company's prevention and response to IT security, through an interview with the IT coordinator, the concerns and reasons related to information security has three great motivators. The first is prevention, because through it one seeks to preserve business continuity, avoiding data loss, theft of information assets and prevent fraud. Prevention is achieved through pro and control policies and monitoring tools, procedures, access restrictions, standards, risk management and information security policies. The second motivator is regulation, which aims to ensure proper use of the systems, the correct user access and comply with best market practices, such as policies for information security and identity management, laws and codes of conduct and ethics. The third motivator are the development trends of the business and new ways of using technology, such as the use of mobile devices.

The current focus of security management of enterprise information is to give an appropriate response to security attacks, however there are a number of preventive actions against future attacks. According to the manager, the security risks were always present, but only recently the company has seen the risk of management practices. From this management is possible to prepare the company structure to adequately predict the security risks. The IT sector has created two divisions of the company to effectively address the issue of information security, with one party related to application (Security Infrastructure - Infrastructure related) and one related to the study and modeling of information security part (Information Security - related to Planning and Control).

Concerning to measurement of security risk, the company believes that once identified, the risks can be measured. This measurement can be given as to the impact it may have on the business to affect the company's image; may hurt economically when strategic information is leaked, such as those relating to product development. The security risk may also be related to internal company user, measuring the offense according to the severity of the incident. For example, the use of pirated software or viewing and distribution of pornographic content, are considered very serious offenses. To address these risks, the company uses its Business Continuity Plan and train users on IT policies.

According to the company, the security risks are persistent due to the new technologies developed, employee's turnover and increasingly fierce competition, which makes the company look for technological update, permanently empowerment of professionals dedicated to information security and identification of providers qualified services with the capacity to meet the demands of the functional areas according to safety standards set by the security Information. The threats are constant and the company will always be exposed to information security risks, what the company can do is stay aware of the risks and be prepared to deal with them.

When security measures are compromised, the subject is treated with the urgency and confidentiality required, being involved the analysts, service providers (eg, Microsoft, TIVIT) and specialists to treat the problem and restore the security. The reasons for the breach of security are evaluated and an analysis of the environment is taken in order to identify the risk factors and vulnerabilities. Then an action plan is developed to ensure that the incident does not happen again.

For the company, the focus of information security changes over time, driven by a crisis (when an incident occurs). In those moments, infrastructure investments are easier to justify. Other factors that cause the changes are changes in legislation, technological advances and the specific business needs that arise. Each time a change is needed, they happen through projects that are approved in the Information Technology Committee.

To contrast with the vision and the activities that the company makes with respect to IT security, the survey revealed the adherence of employees to security policies in IT. The results of this survey are summarized in Figure 3.

Figure 3 - the adherence of employees to security policies in IT

Employees' adherence to information security policies responses							
Likert Scale	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Actual compliance							
I recommend others to comply with information security policies	10%	8%	0%	10%	13%	20%	40%
I assist others in complying with information security policies	5%	13%	3%	20%	10%	28%	23%
Intention to comply							
I intend to comply with information security policies.	3%	3%	5%	3%	8%	28%	53%
I intent to assist others in complying with information security policies.	3%	3%	3%	18%	8%	35%	33%
Attitude							
I feel that compliance to information security policies is a positive thing.	0%	0%	10%	5%	15%	33%	38%
I feel that compliance to information security policies is important.	0%	3%	8%	0%	15%	28%	48%
Self-efficacy							
I can use information security measures if I can call for help if I get stuck	13%	3%	5%	25%	15%	18%	23%
I can use information security measures if someone tells me what to do as I go along.	13%	8%	0%	28%	18%	25%	10%

Employees' adherence to information security policies responses							
Likert Scale	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Normative Beliefs							
Upper management is of the opinion that I should comply to information security policies.	3%	3%	3%	13%	13%	28%	40%
My superiors are of the opinion that I should comply to information security policies.	0%	3%	3%	15%	15%	28%	38%
My close coworkers are of the opinion that I should comply to information security policies.	5%	8%	8%	10%	15%	30%	25%
My organization's IT/information security personnel are of the opinion that I should comply to information security policies.	5%	5%	3%	8%	13%	30%	38%
Rewards							
If I comply with information security policies I will get appreciation.	58%	18%	10%	8%	3%	0%	5%
If I comply with information security policies I will get acknowledgment from my superior.	55%	20%	13%	3%	3%	3%	5%
Perceived Severity							
An information security breach in my organization would be a serious problem for me.	8%	8%	0%	13%	13%	20%	40%
An information security breach in my organization would be a serious problem for my organization.	3%	3%	3%	5%	3%	20%	65%
Perceived Vulnerability							
I could be subjected to a serious information security threat.	10%	10%	8%	23%	10%	15%	25%
My organization could be subjected to a serious information security threat.	5%	10%	3%	18%	15%	33%	18%
More and more serious information security threats are being faced by my organization.	8%	5%	3%	20%	10%	20%	35%
Response Efficacy							
The information security personnel in our organization keep IS security breaches down.	8%	0%	8%	10%	20%	30%	25%
Complying with information security policies in our organization keep IS security breaches down.	5%	3%	3%	5%	23%	30%	33%
Having information security policies in our organization keep IS security breaches down.	5%	0%	3%	5%	20%	40%	28%

Source: Made by the authors.

The responses provided by the employees whose answered the questionnaire in a 7-point Likert Scale, reveal that, talking about actual compliance, 60% of the employees recommend others to comply with information security policies and 51% assist others in complying with information security policies and 81% of them intend to comply with information security policies, while 68% intent to assist others in complying with information security policies. In one hand, 71% of the respondents think that compliance to information security policies is a positive thing, in the other hand, 76% believe that compliance to information security policies is important. Speaking about self-efficacy, 41% of the respondents can use information security measures if they can call for help if stuck and 35% can use information security measures if someone tells them what to do as they go along. About the normative beliefs, 68% of the employees believe that upper management is of the opinion that they should comply to information security policies, 66% think that their superiors are of the opinion that they should comply to information security policies, 55% said that their close coworkers are of the opinion that they should comply to information security policies and finally, 68% of them consider that their organization's IT/information security personnel are of the opinion that they should comply to information security policies.

When asked about rewards to follow organization's IT/information security policies, 75% of the employees said that they comply with information security policies they will not get appreciation and 75% think that they comply with information security policies they will not get acknowledgments from their superior. When asked if they believe that an information security breach in their organization would be a serious problem for them, 60% agreed, while 85% believed that an information security breach in their organization would be a serious problem for their organization.

Talking about perceived vulnerability on their company, 40% answered that they could be subjected to a serious information security threat, 51% of them think that their organization could be subjected to a serious information security threat and 55% responded that more and more serious information security threats are being faced by their organization. Finally, 55% of the employees said that the information security personnel in their organization keep IS security breaches down, 63% think that complying with information security policies in their organization keep IS security breaches down and 68% believe that having information security policies in their organization keep IS security breaches down.

6 CONCLUSIONS

Regarding the vision of the studied company on the relationship of the strategic balance between prevention and response, the company has their policies to prevent data loss, regulation to teach and to propagate the correct way to use its IT resources to its workforce and works with the newest IT tendencies, such as mobile devices. With the exposure to new threats every day, the company can respond effectively, through its two information security divisions. The company understands that its information security team must be always updating themselves in order to handle to the risks involved and to be fast to respond when the security measures are compromised. The information security of the company changes when a crises appears or when the legislation changes.

If in one hand, the company feels confident with there is policies, in the other hand, as shown by the questionnaire applied, the company's employees want and help others to comply with company's security policies, although they don't expect any rewards to comply with these policies. The employees believe that comply with information security is a positive thing and they are able to solve problems related to information security if guided by the IT personnel. They perceive that, as it is the case for their company, they are also exposed to serious threats. They believe that the company's countermeasures related to these threats have

been successful. Finally, the employees believe that they must follow the information security rules as well as co-workers, upper management and information security personnel.

With these aspects given, we can conclude that the company's policies and the employees' intention to cooperate are in consonance. The company's efforts to provide a robust information security is perceived and followed by its employees. This fact can help the company to protect its data from stealing, for example. Managers who understand the incident-centered model and whose environment reflects increasing sophistication in attacks will recognize the need to place additional emphasis on activities in the organization's response paradigm.

A limitation of this work is its application in a company with headquarters in Brazil and mechanical metal branch. Its replication in other countries and in other branches of activity would be interesting in order to check up similarities and differences, indicating the generalizability of the findings contained in this work. Another significant limitation is the fact that the questionnaire given to employees may have loopholes to misinterpretation, leading to possible distortions in its result. The models used could also be applied in a supply chain, serving as a basis for improvements in measures of information security, guiding employee behavior.

REFERENCES

BACCARINI, D. et al. Management of risks in information technology projects. **Industrial Management & Data Systems**, [S.l], v. 104, n.4, p. 286, 2004.

BASKERVILLE, R. et tal. Incident-centered information security: Managing a strategic balance between prevention and response. **Information & Management**, [S.l], v. 51, p. 138–151, 2014.

BLUEPHOENIX. **Boas práticas de segurança**. Disponível em: <www.bluephoenix.pt>. Access 20 January 2014.

BROOKS, W.; WARREN, M. A Metodology of Health information Security Evaluation. **Health Care and Informatics Review Online,** 2006. Disponível em <http://www.hinz.org.nz/journal/2006/09/a-methodology-of-health-information-security-evaluation/940>. Access 01 February 2014.

CAMPOS, A. **Sistema de Segurança da informação:** controlando os riscos. 2. ed. Florianópolis: Visual Books, 2007.

CERT.BR. **Estatísticas dos incidentes reportados ao CERT.br**. Disponível em: http://www.cert.br/stats/incidentes/. Access 28 February 2014.

FERREIRA, F. N. F.; ARAÚJO, M. T. **Política de Segurança da Informação:** Guia Prático para Implementação e Elaboração. Rio de Janeiro: Editora Ciência Moderna, 2006.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos.** Rio de Janeiro: Berkeley Brasil, 2002.

MALHOTRA, Naresh K. **Pesquisa de marketing:** uma orientação aplicada. 3.ed. Porto Alegre: Bookman, 2001.

MARTINS, A. B.; SANTOS, C.A.S. Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **Revista de Gestão e Tecnologia e Sistema de Informação**, [S.l.], v. 2, n. 2, p.121-136, 2005.

MARTINS. J. C. C. **Gestão de Segurança da Informação**. Rio de Janeiro: Brasport, 2003.

RANDON. **Comunicado Randon,** 2014. Disponível em: <ri.randon.com.br/randon/web/conteudo_pt.asp?idioma=0&tipo=12949&conta=28&id=185934>. Access 20 February 2014.

SECRETARIA DE DESENVOLVIMENTO E PROMOÇÃO DO INVESTIMENTO. **Programa Setorial Automotivo e Implementos Rodoviários 2012-2014 da Secretaria de Desenvolvimento e Promoção do Investimento (SDPI),** 2014. Disponível em: <http://www.sdpi.rs.gov.br/upload/20120328150854programa_setorial___automotivo_e_implementos_rodoviarios.pdf>. Access 20 February 2014.

SÊMOLA, M. **Gestão da Segurança da Informação:** Uma visão executiva. São Paulo: Editora Campus, 2003.

SINDICATO INTERESTADUAL DA INDÚSTRIA DE MATERIAIS E EQUIPAMENTOS FERROVIÁRIOS E RODOVIÁRIOS –SIMEFRE. **Indústria de implementos produz 4,92% a mais que em 2012**, 2013. Disponível em: http://www.simefre.org.br/Data/Release-Implementos.pdf. Access :18 February, 2014.

SIPONEN, M. et al. Employees adherence to information security policies: an exploratory field study. **Information & Management**, [S.l], v. 51, p. 217–224, 2014.

SOARES, L. F. G. et al. **Redes de computadores**: das LANs, MANs e WANs as redes ATM. 2. ed. Rio de Janeiro: Campus, 1995.

VERMEULEN, C.; SOLMS, R.V. The information security management toolbox: taking the pain out of security management. **Information Management & Computer Security**, [S.l], v.10, n.3, p. 119-125, 2002.

WADLOW, A. T. **Projeto e Gerenciamento de Redes Seguras**. São Paulo: Campus, 2000.

ZHI, H. Risk management for overseas construction projects. **International Journal of Project Management**, [S.l], v. 13, n. 3, p. 231-237, 1994.