Management and Marketing Research Journal
ISSN: 2997-6049 |
Volume 10 Issue 3, July-September, 2022
Journal Homepage: https://ethanpub.online/Journals/index.php/E15
Official Journal of Ethan Publication

GATEKEEPERS OF SME INFORMATION SECURITY: UNDERSTANDING PERCEIVED RISKS AND STRATEGIES

[1]João Carlos Pereira and [2]Maria Luiza Santos
[1]Student at UNINASSAU, Recife, PE, Brazil
[2]Professor at UNINASSAU, Recife, PE, Brazil

Abstract:
In our interconnected world, where information flows freely and technology is increasingly accessible, both individuals and businesses are experiencing a digital revolution. This transformation has prompted companies to reevaluate their business models, integrating information technology (IT) resources to enhance their agility and overall organizational structure. As highlighted by Lunardi, Dolci, and Maçada (2010), this shift towards IT adoption has the potential to provide a significant competitive advantage. This revolution isn't confined to large corporations; it equally affects small and medium-sized enterprises (SMEs). In Brazil, SMEs contribute significantly to the economy, accounting for 27% of GDP and 44% of formal jobs in 2011 (SEBRAE, 2015). With approximately 76% of these enterprises utilizing electronic equipment and 61% employing some form of business management system (SEBRAE, 2015), the importance of IT resources for their survival is increasingly recognized (Biagi & Roldello, 2016). Laureano and Moraes (2005) underscore the role of information as a valuable asset within organizations, requiring diligent protection and preservation. Security vulnerabilities can have far-reaching consequences, even rendering critical projects unviable (Kroll & D'Ornelas, 2009). Prates and Ospina (2004) emphasize that SMEs are particularly vulnerable due to their limited resources. This paper delves into the pivotal role of IT resources in the context of SMEs, examining their adoption, challenges, and potential impacts. It underscores the imperative for SMEs to navigate the digital landscape with caution, given the increasingly crucial role of IT in their sustainability and competitiveness.

Keywords: Information technology, SMEs, digital revolution, business agility, security vulnerabilities.

Introduction

We live in an age where people are increasingly connected, searching and sharing information, taking advantage of the ease of access to technological resources, which are increasingly democratic. This revolution has also impacted companies so that they revise their business models and incorporate more and more resources related to information technology (IT) (Lunardi, Dolci, & Maçada, 2010). In this line of thinking, Prates and Ospina (2004) affirm that IT will change the organization so that its processes become more agile, thus benefiting its entire organizational structure and management. These benefits can guarantee a competitive advantage to the company in front of its competitors.

Such a revolution is not exclusive to large companies, it also impacts small and medium-sized enterprises (SMEs). In Brazil, this group accounted for 27% of GDP in 2011, as well as being responsible for 44% of formal jobs in the same year (SEBRAE, 2015).

In a scenario where about 76% of these companies use some type of electronic equipment and some 61% of this group has some kind of system to assist in the management of the business (SEBRAE, 2015), the use of IT related resources is increasingly more common within SMEs, because there is a certain perception of the importance of IT resources for the company's survival (Biagi & Roldello, 2016). Laureano and Moraes (2005) argue about the importance of information in companies and how it has become a patrimony, so managers must ensure their protection and preservation. Security flaws can cause business impacts, rendering projects unfeasible, as Kroll and

D'Ornelas (2009, p.19) argue, "Security breaches pose major threats to the execution of corporate strategies". Prates and Ospina (2004) affirm that SMEs are the main affected, since they have limited resources.

According to Sêmola (2014) there are three layers of security being the technological, physical and human layer, and SMEs have difficulties in dealing with all layers of security. Therefore, because they are not aware of the security layers and other tools available for the implementation of a consistent information security policy, SME managers summarize their security systems in tools such as antivirus and firewalls (Sêmola, 2014).

Security failures are very much related to the individual's perceptions of the risks and vulnerabilities that threaten his or her organization, since each one interprets the environment according to the lived experiences and the knowledge acquired over time (Robbins, 2009). Due to its subjectivity, the perception can be considered a critical element for a master plan of security. In the context of SMEs, the perception of the risk associated with a lack of knowledge of the tools and layers of information security makes them even more vulnerable. Thus, the present project aims to address the use of information security tools in their respective layers of security, as well as the perception of the risk of security events in the SME scenario.

1 The SME Scenario

SMEs have played an important role in the economy, however they face difficulties to remain competitive in the market (Balestrin & Vargas, 2003; Andrade, Almeida, & Freitas, 2014). In the most developed economies, including micro, small and medium-sized enterprises, the total number of jobs generated reaches 60% of the workforce. In less developed economies, just over 30% of formal jobs are generated by companies classified as micro, small and medium (Sarfati, 2013).

Despite the economic importance of SMEs to the national and regional economy, Santini *et al*. (2015), when dealing with micro and small enterprises, affirm that there is a high mortality rate and that several factors can influence the closure of companies, among them the oppression of large companies, market limitations, difficulties in obtaining financial resources, working capital management, high tax burden and the low ability to manage business. The low capacity of management in small and medium-sized enterprises is also a factor cited by Silva and Araújo (2016). Additionally, Silva and Araújo (2016) argue that micro and small enterprises have scarce financial resources, simplified organizational structure, centralized decision making, intuition-based decisions, and flexibility for rapid adaptation to the environment.

2 Information Securities

Information security aims to ensure the protection of information from the threats it is exposed to, thus preserving the risk business (ISO/IEC 17799, 2005). Sêmola (2014) states that managers should be aware of the possible threats to which information is subject, which can happen in four moments, which should be more careful than handling, storage, transport and disposal. The main moments that information is most at risk are:

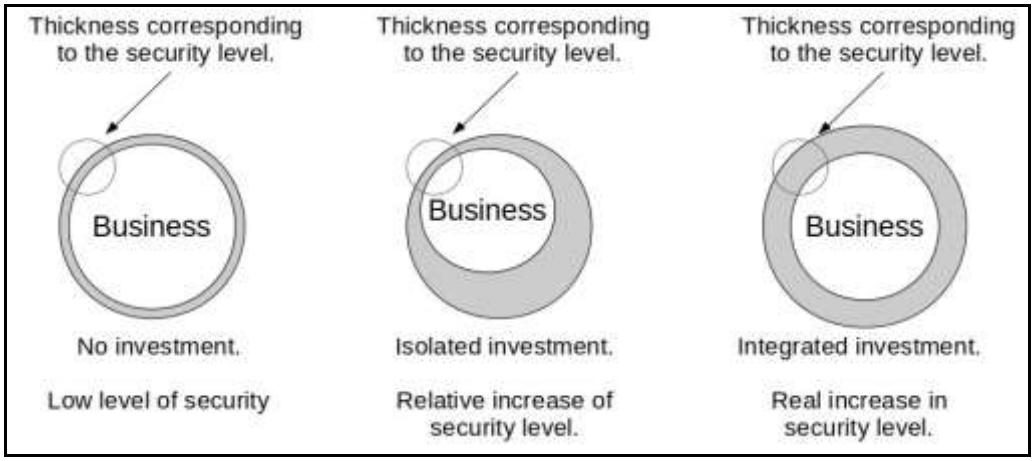
- Handling - including or creating information, care must be taken to ensure that the data is complete;
- Storage - Time when the information is stored in some type of storage device, database. It should be ensured that no data are lost or altered during this process;
- Transportation - is the moment when the information is delivered, disclosed or accessed. Attention must be paid to possible invasions and leaks;
- Disposal - Stage where the information is discarded after its use. Information must be avoided.

Adachi (2004) emphasizes that information security should also be dedicated to ensuring availability, confidentiality and integrity of information, thereby ensuring the survival of the business. Availability is the ability for information to be available to users when they access it. Confidentiality guarantees that the information will only be accessed by the one who has authorization and no one else. And, finally, integrity understands the notion that information must be preserved in the same way that it was originally made available. Information is an asset of the companies, if not the most important (Sêmola, 2014). Like other assets, it must be protected from attacks and threats. The implementation of an information security system in the organization must be accompanied by a series of requirements, one of which is a security master plan, in which tools and processes are strengthened and strengthen the security perimeter. Information security systems create a security perimeter that works as a protective barrier

Management and Marketing Research Journal
ISSN: 2997-6049 |
Volume 10 Issue 3, July-September, 2022
Journal Homepage: https://ethanpub.online/Journals/index.php/E15
Official Journal of Ethan Publication

around the organization. For Sêmola (2014) a company's security level is measured by the most vulnerable side of the barrier, the thickness of the barrier, or of the perimeter will define the level of security of the company, if it is badly sized the company will be in serious trouble, or if the investments made are very concentrated in a single threat type, neglected other areas, thereby the perimeter thickness will be defined by as shown in figure 1.`

Figure 1: Security Level Thickness (Sêmola, 2004)



3.1 Security layers

For Sêmola (2014), due to a myopic view, companies distort what is information security, being more concerned with the technological aspects, forgetting the physical and human aspects of information security, thus not obtaining the level of security. According to the same reasoning, Diniz, Porto and Adachi (2003) divide information security processes into three layers: technological, physical and human. Adachi (2004) defines that the technological layer encompasses everything that involves the software, the physical layer seeks to protect the hardware and the human layer encompasses all the human resources of the organization.

3.1.1 Physical Layer

It refers to the environment where the computers and the computers are installed, in addition to encompassing the entire communications network. Wadlow (2000) warns that this layer is very poorly understood, even having its importance for network security. Adachi (2004) lists that the main threats of the physical layer are:

- Accidental shutdown of production equipment;
- Lack of energy;
- Improper access to the system; Theft of equipment.

3.1.2 Logical Layer

The logical layer encompasses software, from applications to the most basic programs. According to the guide GASSP (1999), computer programs are one of the main elements in the information system and therefore one of the most threatened. The layer is responsible for three of four information security events and where information is most vulnerable. The main threats are unauthorized modification, improper storage and disposal, and malware such as viruses and Trojans.

3.1.3 Human Layer

This is the most fragile layer because it is in it that are targeted to major attacks (Adachi, 2004). It is formed by all individuals involved in the processes of the organization. GASSP (1999) points out that the lack of training of employees and the lack of knowledge of the possible impacts that can be caused to information systems, if used improperly, are the major sources of risks. In this same line of thinking, GASSP (1999) concludes that an environment should be created where there is an awareness of all levels for the issue of information security, as well as providing adequate training.

Management and Marketing Research Journal
ISSN: 2997-6049 |
Volume 10 Issue 3, July-September, 2022
Journal Homepage: https://ethanpub.online/Journals/index.php/E15
Official Journal of Ethan Publication

2.2 Tools and Layers of Information Security

The information security standard, ABNT NBR ISO/IEC 27002, states that its application is not necessary in an integral way, since each organization must know its limits and so it is not necessary to implement rules that would only bring more bureaucracy to the organization. The standard addresses the three layers of security, bringing a series of recommendations for success in implementing the tools and which tools you use in each layer. Table 1 shows the main points covered in the standard for each of the layers.

Table 1: Security layers and their guidelines (ABNT NBR ISO/IEC 27002, 2005)

Layer	Type of control	Purpose
Physical	Room and Facility Security Perimeter	Defines that barriers are used that prevent unauthorized persons from entering the areas that contain the information
	Protection against external threats and the environment	Defines actions to be taken against natural or man-made disasters
	Facilities and equipment protection	Defines which equipment should be placed in secure places protected from improper access and environmental risks
Human	Selection	It stipulates that all candidates be analyzed through their histories, being it supplier, outsourced or official.
	Awareness, SI education	It defines that all are trained and have in mind the importance of SI.
	Disciplinary proceedings	Define quais ações são tomadas contra quem violar as normas de segurança
Logical	Validation of data	It defines that the data must be kept in its natural state protected that any kind of unauthorized change.
	Software security	Defines that protection measures are applied in the installation, in the source code of the software.

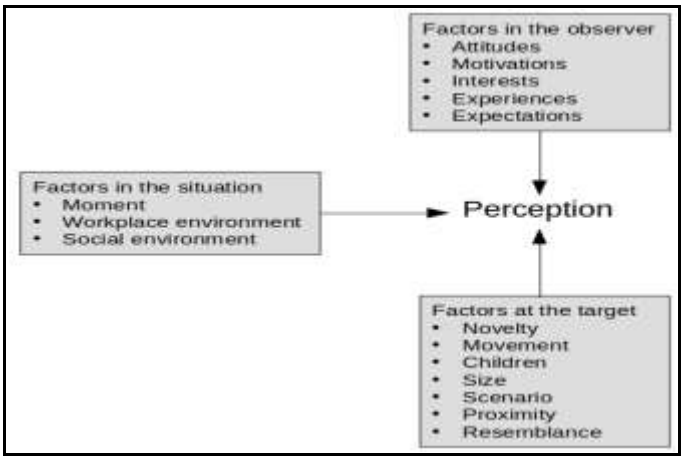
The standards also bring a number of possible events that may occur, these events may or may not be considered a vulnerability to the organization, depending on how managers will evaluate such vulnerabilities.

3 Risk Perceptions

The human being interacts with the world in a different way, because his behavior is based on his perception of the situations faced (Robbins, 2009). Faced with such a statement, perception can influence in a negative way, since he as an observer may end up distorting the fact and shaping in his own way, according to his personal characteristics and interests. Robbins (2009) defines that there are three groups of factors that will influence the perception of the individual, being factors of the observer, the situation and the target. Figure 2 lists all the factors in their respective groups.

Management and Marketing Research Journal
ISSN: 2997-6049 |
Volume 10 Issue 3, July-September, 2022
Journal Homepage: https://ethanpub.online/Journals/index.php/E15
Official Journal of Ethan Publication

Figure 2: Factors influencing the perception of risk. (Slovic, 1987)



We are exposed daily to various types of risks and we react differently to the same risk. Our ability to interact and assess the danger is different for everyone, as Minayo and Miranda (2002) state. Slovic (1987) concludes that risk assessment is different according to the perception of each individual, and since perception is a subjective theme, it ends up influencing decision making.

The preparation of risk assessment is a very common practice for some companies in specific segments, such as construction companies, industries in general and health, areas considered unhealthy or dangerous. This evaluation is made by specialists from each sector, in addition to the existence of national and international laws and regulations.

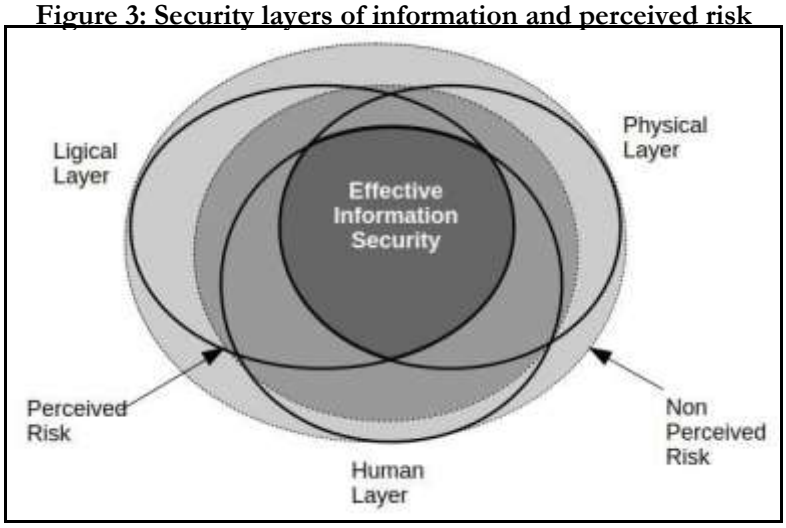
When it comes to the issue of information security, even with the existence of regulatory standards, the subject is very neglected. Especially in the context of SMEs, because usually the decision makers in SMEs are lay people. Even in cases where the IT manager is the decision maker, it is only done by him without the participation of other important organizational actors. Slovic (1987) argues that laymen and specialists have different perceptions when they observe the same risk. With such a statement, associated with the reality of SMEs, letting the planning of information security on the command of laypersons or of a single person can become a big problem, given the different perceptions of risk of the agents involved.

Sêmola (2014) highlights the importance of perception for the area of information security, it is a central element in the planning phase of the security master plan, since it is from the perception of those involved that the investment decisions will be planned and taken in the security area. Thus, perception is an element of the monitoring phase, since an assessment of safety processes and tools must be continuously done. It is important to keep in mind that it is essential for the coherent, secure, mature development of information security.

Using the concept of risk perception (Robbins, 2009; Slovic, 1987) and information security layers (Sêmola, 2014), it is possible to identify that there are areas of information security that are not covered only by the fact that managers do not perceive the risk involved in the information. Even in areas where risk is perceived, mitigation actions are not taken because the assessment of this risk is not done correctly (Slovic, 1987). Thus, figure 3 summarizes the perception of risks, the evaluation of these and the layers of information security.

Management and Marketing Research Journal
ISSN: 2997-6049 |
Volume 10 Issue 3, July-September, 2022
Journal Homepage: https://ethanpub.online/Journals/index.php/E15
Official Journal of Ethan Publication

Figure 3: Security layers of information and perceived risk



4 Final Considerations

Threats are possible breaches in the security barrier, which can be exploited by malicious agents, in order to harm a person or a company. All threats arise through some type of vulnerability that the organization has, exploiting this vulnerability may or may not cause a security flaw (Sêmola, 2014). Thus, the first step in the application of information security tools that will combat threats is their proper identification.

Because risk assessment is a personal process (Robbins, 2009), the outcome of this evaluation can be skewed. Slovic (1987) argues that this distorted view of the risks faced may be associated with personal, situational or object factors being evaluated, which corroborates with the subjectivity of the assessment.

In SMEs, this distortion in evaluation tends to be even greater because of the limitations of resources and specialized personnel (Sêmola, 2014). Proper training not only of the IT staff, but also of other organizational actors, can make the organization's shared risk perception better able to prepare for possible security events that will occur. Another important point is knowing how to identify information security events. At various moments, events that are information security are not treated as being security, disguising the numbers of events and distorting the perception of the managers, since they do not associate these occurrences with information security.

Finally, correctly using the information security tools so that possible events can be mitigated is a central factor for the success of implementing an information security policy, even in simpler contexts such as small businesses.

References

Adachi, T. (2004). *Gestão de segurança em internet banking: estudo de casos brasileiros* (Doctoral dissertation).

Andrade, M. A. R., ALMEIDA, P., & FREITAS, L. (2014). Internacionalização como estratégia competitiva para pequenas e médias empresas do Brasil: uma revisão bibliográfica. Simpósio de Excelência em Gestão e Tecnologia, 11.

Balestrin, A., & Vargas, L. M. (2003). Redes horizontais de cooperação como estrutura favorável ao desenvolvimento das PMEs. XXVII Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração. Anais, Atibaia: ANPAD.

Biagi, B., & Rodello, I. A. (2017). Beneficios da Utilização Adequada de um Sistema de Informação em uma Microempresa. *Revista de Exatas e TECnológicas*, *6*(1), 19-29.

DINIZ, E. H., PORTO, R., & ADACHI, T. (2003). Internet Banking sob a ótica da funcionalidade, confiabilidade e usabilidade. *Conselho Latino Americano de Escolas de Administração*, *38*, 01-15.

GASSP - Generally Accepted System Security Principles (1999). Version 2.0. Information Systems Security 8, 3.

ISO, A. N. (2005). IEC 17799-Tecnologia da informação: código de prática para a gestão da segurança da informação. *Rio de Janeiro: ABNT*.

Kroll, J., & Dornellas, M. C. (2009). Aplicação da Metodologia de Avaliação de Riscos para o Gerenciamento Estratégico da Segurança da Informação. *XLI Simpósio Brasileiro de Pesquisa Operacional*.

Laureano, M. A., & Moraes, P. E. S. (2005). Segurança como estratégia de gestão da informação. *Revista Economia & Tecnologia*, *8*(3), 38-44.

Lunardi, G. L., Dolci, P. C., & Maçada, A. C. G. (2010). Adoção de tecnologia de informação e seu impacto no desempenho organizacional: um estudo realizado com micro e pequenas empresas. *Revista de Administração*, *45*(1), 5-17.

Minayo, M. C. D. S., & Miranda, A. C. D. (2002). *Saúde e ambiente sustentável: estreitando nós*. Editora Fiocruz.

Prates, G. A., & Ospina, M. T. (2004). Tecnologia da informação em pequenas empresas: fatores de êxito, restrições e benefícios. *Revista de Administração Contemporânea*, *8*(2), 9-26.

Robbins, S. P. (2009). *Fundamentos do comportamento organizacional*. Pearson educación.

Santini, S., de Vasconcellos Favarin, E., Nogueira, M. A., de Oliveira, M. L., & Ruppenthal, J. E. (2015). Fatores de mortalidade em micro e pequenas empresas: um estudo na região central do Rio Grande do Sul. Revista Eletrônica de Estratégia & Negócios, 8(1), 145-169.

Sarfati, G. (2013). Estágios de desenvolvimento econômico e políticas públicas de empreendedorismo e de micro, pequenas e médias empresas (MPMEs) em perspectiva comparada: os casos do Brasil, do Canadá, do Chile, da Irlanda e da Itália. Revista de Administração Pública-RAP, 47(1).

SEBRAE, DIESSE (2015). Anuário do Trabalho na Micro e Pequena Empresa 2014. São Paulo.

Sêmola, M. (2014). *Gestão da segurança da informação* (Vol. 2). Elsevier Brasil.

Silva, H. C., & Araújo, M. A. Emerging Strategies and Hypercompetitive Environments to Micro and Small Companies of Information Technology.

Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285.

Wadlow, T. A. (2000). *The process of network security: designing and managing a safe network*. Addison-Wesley Professional.