Asset Intrinsic Risk Assessment

Covid-19 impact case study

Luísa Alexandra Inácio Varandas dos Santos

Instituto Superior Técnico

Lisbon, Portugal

october/2021

Abstract

In mid-March 2020, there was a unique and transversal concern to the entire public and private sector in Portugal, reducing the number of contagions by Covid-19 as much as possible. ANSR, faced with a worldwide pandemic, forcing changes "innovations" related to current routines and work modalities, promoting the reality Telework.

This new reality, Teleworking, has also resulted in a vulnerability, as a potential factor that accentuates the action of certain threats to ANSR's Information Security.

Therefore, evidence of the current circumstances was collected, during the first half of the year 2020, that could be observed, in order to ascertain the objective of this dissertation: to ascertain the intrinsic risk of ANSR's teleworking assets, in a Covid-19 pandemic context, in the light of the events of threats and vulnerabilities between January 2019 and July 2020, through the risk assessment phases of an integrated risk management model, according to ISO31000 and ISO27005 standards.

Keywords: Risk, Information Security, Vulnerabilities, Threats.

1. Introduction

In late 2019, the SARS-COV-2 virus (Covid -19) was first identified in humans in the Chinese city of Wuhan, Hubei province. Subsequently, cases were confirmed in other countries, in early 2020, the World Health Organization, identified the disease caused by the new coronavirus SARS-COV-2, as Covid-19. Because of this pandemic and the recommendations of the World Health Organization, the Organizations, worldwide, allocated almost all of their Employees, in a Teleworking modality, promoting the work performed with legal subordination, usually

outside physical installations of the Organizations, providing information and communication technologies.[1], [2]

In this context, vulnerabilities are exploited by malicious individuals, such as social engineering attacks, to Organizations Employees, often exploiting their illiteracy in the areas of Information Security or their psychosocial conditions.

We will continue the conclusions of several entities, national and international, in the field of information security, in a Covid-19 pandemic context, analyzing a Case Study, which will contribute to directly relate teleworking in a Covid-19 pandemic context, with the increase of information security threat events, by proposing a risk management model that can measure de asset intrinsic risk of the Organizations.

1.1. Brief History

The technological revolution started in the last decades of the XX century, and transformed the whole Information concept. Organizations have seen a paradigm shift in which, this asset, Information, has ceased to be something merely physical, and has become an essentially digital asset.

Information in the digital age is no longer an easily identifiable target to be protected, in which, many times, the protection of this asset, involves assessing and managing the risk of the possibility of its total or partial loss, or even, being accessed by unauthorized destinations.

At the end of the XX century, between the 80s and 90s, two models appeared for IT management services. Although these two models did not address the topic information security in their first versions, they still became references for Organizations, they are: The Information Technology Infrastructure Library (ITIL) and the Control Objectives for Information and related Technology (COBIT). Later in the first decade of the XXI century, emerges a new referential, an International Organization for Standardization (ISO) dedicated to the topic of Information Security and risk management in Information Technologies, although the beginning of the ISO standard dates back to the late 1940s. XX. [3]–[5]

1.2. Problem Definition

Information security risk assessment and monitoring, in the context of new forms of work organization

1.3. Goal

Propose and validate an information security risk management model adapted to new forms of work organization, which allows the determination of the intrinsic risk of certain vulnerabilities and threats to organizations in a pandemic context.

2. Methods

2.1. Methodology

The methodology used for the investigation, will be the Case Study, specific to a Portuguese public sector organization, allowing to determine the intrinsic risk of assets placed under Teleworking, in the Covid-19 pandemic context.

The Case Study methodology will reside in a qualitative perspective, it will be oriented towards the analysis of a restricted group of data, and assessment of the intrinsic risk through the application of a risk

management model, on these data, based on events observed in a context (Covid-19 pandemic) between January 2019 and July 2020, of a certain organization, which will allow relating the events observed with the pandemic state and other scientific studies carried out, so that the phenomenon can be understood. For the characterization of the Case Study, we will specifically address the adaptation and use of the following phases represented in Figure 1:

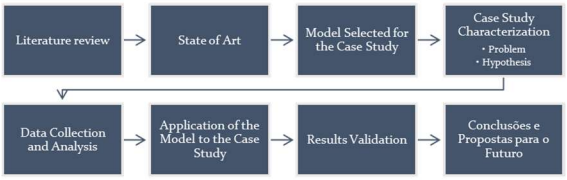

Figure 1 – Case Study Methodology Phases

2.2. Framework Applied

Within this methodology, we are going to propose the application of a framework for risk management model, based on the main standards ISO 31000 and ISO 27005, represented in Figure 2. We will demonstrate the determination of intrinsic risk assets placed in telework in any Organization, by a particular Case Study.[6], [7]

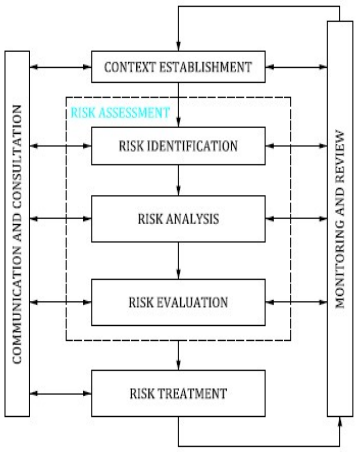

Figure 2 - Integrated Process for implementing the Information Security Risk Management Model by the ISO31000 in conjunction with the ISO27005 [7]

2.2.1. Characterization of the Case Study

For the Case Study, we collected data of information security incidents, from a Portuguese Public Organization, from January 2019 to July 2020.

In the data collection and analysis phase, it was decided to analyze homogeneous periods, january 2019 to july 2019 and january 2020 to july 2020. This decision allowed the investigation to analyze two scenarios, regarding telework and the number of security incidents occurred, before and after the covid-1 pandemic.

Two samples of data were collected, one related with security incidents, and the other related with employees of the organization. In Table 1 we can see the number of registered security incidents in the homogeneous periods, and in Table 2 we can check the classification made for the assets identified in telework class 1 (ATIVO I) class 2 (ATIVO II) class 3 (ATIVO III).

Incidentes Registados	Ano		
Mês	2019	2020	Total Geral
JANEIRO	13	82	95
FEVEREIRO	16	34	50
MARÇO	29	82	111
ABRIL	16	58	74
MAIO	31	32	63
JUNHO	57	107	164
JULHO	16	155	171
Total Geral	**178**	**550**	**728**

Table 1 number of registered security incidents in the homologated periods january 2019 to july 2019 and january 2020 to july 2020

CLASSES ATIVOS	PERFIL RESPONSABILIDADE	TIPO VINCULO	ÁREA	Qtds
ATIVO I	A.PRESIDÊNCIA	COLABORADOR ANSR	ALTA DIREÇÃO	4
ATIVO II	B.DIRIGENTE	COLABORADOR ANSR	ALTA DIREÇÃO	8
ATIVO III	C. + D. TÉCNICO	COLABORADOR ANSR E PRESTADOR SERVIÇO	RECURSOS HUMANOS, FINANCEIRA E CONTRATUAL, TÉCNICA, ADMINISTRATIVA.	166

Table 2 classification made for the assets identified in telework

the classification of assets by classes, was intended to distinguish levels of responsibility (presidency, directors and technicians) for a posteriori definition of the impact levels, for the valuation of assets.

2.2.2. Framework application

For the case study we focus on the application of the framework of Figure 2, specifically in the definition of the scope for the framework, and in the risk assessement.

2.2.2.1. Scope definition

For the definition of the scope, we considered factors of the Organization such as: The Organization's Identity; its Strategic Objectives; Mission and Values and the Organization's Structure.

2.2.2.2. Risk assessement

For the Risk assessement, we considered risk identification, risk analysis and risk evaluation, of the assets within he defined scope. In the ***risk identification*** phase, we refine and distinguish the primary and secondary assets, after that we propose an ***impact matrix*** to value assets considering: the class of assets, a scale of impact levels in case these assets are attacked, guidelines for impact analysis (financial, image, legal, etc.). Then we evaluate for each asset class the application of the ***impact matrix***, considering various scenarios that could affect negatively the availability, integrity, confidentiality, authenticity and legitimacy of the Organization's information. According to the defined impact scale, the following asset impact valuations were obtained:

- class 1 - 5;
- class 2 - 5;
- class 3 - 4.

In the risk analysis phase, we identify the vulnerabilities and threats to which the assets may be subject, considering the sample of data collected for the case study. After that, we defined a scale of probability of occurring those vulnerabilities and threats, taking into account the number of such events that occurred in a given period. the following scenarios were captured:

a) before the pandemic
   - Low threat and Low vulnerability

b) after the pandemic
   - Hih hreat and Hih vulnerability

In the ***risk evaluation*** phase intrinsic risk was calculated. through the application of an intrinsic risk matrix, considering the impact value of the assets class, the value of vulnerabilities and threats of that assets. After the value of the intrinsic risk of each asset class, was obtained, a simple average was performed and the global intrinsic risk of the assets was obtained, and the following scenarios were found in a risk scale defined:

c) before the pandemic
   - Medium intrinsic risk

d) after the pandemic
   Hih intrinsic risk

3. Results and discussion

Through the application of the integrated Information Security risk management model, by the ISO31000 and ISO27005 standards, it was possible to apply techniques that measure intrinsic risk, from which we highlight the following results, for the homologated period January to July 2019 and 2020:

- ✓ 728 information security incidents were investigated at ANSR;
- ✓ 178 ANSR assets were identified;
- ✓ Of these 178 assets, they were aggregated by asset classes (class 1, class 2 and class 3);
- ✓ the following threats values were found:
    - Before Pandemic January Low threat.(2019 to July 2019 (178 events over a 7-month period);
    - During the Pandemic January 2020 to July 2020 High threat (550 events over a 7-month period).
- ✓ the following vulnerabilities values were found:
    - Before the Pandemic January 2019 to July 2019 Low Vulnerability (there were 23 active teleworkers 12.92% of assets);
    - During the Pandemic January 2020 to July 2020 High Vulnerability (178 teleworking assets 100% of assets).
- ✓ the intrinsic risk was determined for assets in the scope in the following scenarios:
    - Before the Pandemic January 2019 to July 2019 Medium Intrinsic risk;
    - During the Pandemic January 2020 to July 2020 High Intrinsic risk.

The model proposed for information security risk management, allows the determination of the intrinsic risk of vulnerabilities and threats, of ANSR assets, in the context of telework, were we could observe the risk of ***HIGH level*** with the value 7 on a scale of 0 to 7. Therefore, with the model proposed it's possible to assess and monitor information security risk, in the context of new forms of work organization.

4. Conclusion

In an Organizational context, insider threats are often evidenced. These threats can be exploited and enhanced through Social Engineering techniques, often derived from vulnerabilities in the psychosocial nature of the Employees, including stress, anxiety, depression, fatalistic worldview. All these vulnerabilities, associated with a certain motivation, such as professional dissatisfaction and seeking revenge against the Organization,

are desirable targets for attacks via Social Engineering. [8]

The pandemic Covid-19, increased all the vulnerabilities identified above, by increasing the levels of stress, anxiety, depression, not only due to the situation of fear experienced, but also due to changes in work circumstances, such as the use of the telework.

In a recent study (May / 2020), from the University of Coimbra, in collaboration with other international Universities, the psychosocial impact of Covid-19 in Portugal is demonstrated, in the two phases of confinement, in which most Organizations have chosen to place their Employees in Telework, the growth of anxiety, stress and depression factors was evidenced. The confinement to housing, and consequent social isolation, generated impacts at the level of undifferentiation between the place of leisure and the place of work (telework), which, among other aspects, generated a situation of great social stress for the great part of the active population.[9]

The National Cybersecurity Center, reports a possible increase information security incidents, related to the current pandemic state and the isolation of people working at a distance, in the Cybersecurity in Portugal-Society Report, of the Cybersecurity Observatory, published in December of the current year.[10]

Several national and international entities have found the link between the Covid-19 pandemic and the new ways of working, with the increase in events of security incidents. The present case study intended to contribute to these findings, proposing a risk management model that would allow to determine the intrinsic risk of teleworking assets, that is, the risk of certain assets without security controls adequate to the current reality of new forms of work.

Thus, accompanied by studies by national and international entities, on the impact of covid-19 on the increase in threats, given the current context of telework, in the present case study, it was found that there was indeed an increase in the intrinsic risk of 2019 for 2020, in the same period analyzed, from Medium Risk to High Risk, coupled with this fact, it was also concluded by the data analysis that, as represented in **figure 21**, it was observed that in 2019 the greatest occurrence of information security incidents (about 82%) occurred within the working period (9:00 am to 18:00 pm), already in 2020 the occurrence of these incidents occurs in an almost balanced way inside and outside the work period, that is, 49.64% during working hours and 50.36% outside working hours.

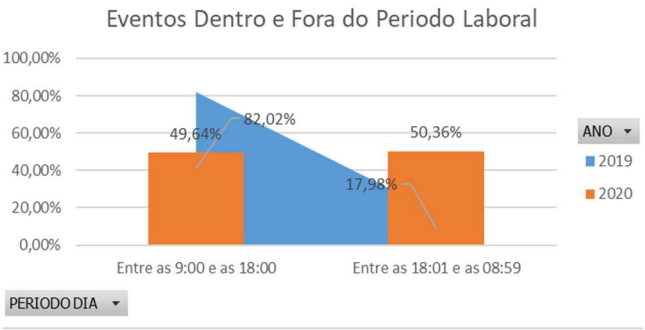

Figure 3 - security Incidents in and ou of the work period in the homologated periods january 2019 to july 2019 and january 2020 to july 2020

5. Future work

In a future perspective, it would be interesting to assess psychosocial factors of employees of organizations, inserted in the context of occupational medicine, in a forecast of risk analysis of the same. This is a delicate situation, as it is verified that privacy issues may be at stake. However, Organizations can promote encryption of data collected for risk assessment or promote anonymization of private data.

6. References

[1] Portuguese National Health Service, "'COVID-19,' (in Portuguese)," 2020. [Online]. Available: https://www.sns24.gov.pt/tema/doencas-infecciosas/covid-19/#sec-0.

[2] E. R. Diario, "Labor Code Law No. 7/2009 (in Portuguese)," 2009. [Online]. Available: https://dre.pt/legislacao-consolidada/-/lc/75194475/201707240900/73439934/diploma/indice.

[3] ISO, "ISO 'About Us' (in Portuguese)," 2020. [Online]. Available: https://www.iso.org/about-us.html.

[4] ISACA, "COBIT 5.0. 2012. Main Framework Version 2.0," 2012.

[5] M. H. Gallacher Liz, *Liz Gallacher, Helen Morris-ITIL Foundation Exam Study Guide-Sybex (2012)*. 2012.

[6] ISO/IEC, "ISO/IEC 31000:2018 - Risk Management - Principles and guidelines," 2018.

[7] ISO/IEC, "ISO/IEC 27005: 2018 - Information technology — Security techniques — Information security risk management," 2018.

[8] M. T. Whitty, "Developing a conceptual model for insider threat," *J. Manag. Organ.*, no. 2018, 2018.

[9] and L. S. A. P. Relvas, A. Portugal, S. Major, "Preliminary Results on the Psychosocial Impact of COVID-19 in Portugal (in Portuguese)," 2020.

[10] National Cybersecurity Center, "Cibersegurança em portugal (in Portuguese)," 2020.