Cybersecurity Incident Management in Public Organizations

Daniel Matos
daniel.matos@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

October 2018

Abstract

The inadequate preparation of organizations to deal with increasingly sophisticated cyberattacks is publicly recognized. The cybersecurity incidents should be managed in accordance with a process for cybersecurity incident management. Using the research methodology Design Science, we propose a reference process based on standards and guidelines of international good practices, with the aim of contributing to the implementation of the cybersecurity incident management process in Portuguese organizations. The proposed reference process was evaluated in practice in a public organization in Portugal.
Keywords: cibersecurity; incident management; ISO 27035; cyberattacks.

1. Introduction

This work is part of the cybersecurity area. The choice of the topic Cybersecurity Incident Management in Public Organizations took into account the numerous cases that have come to public attention related to cyberattacks targeting different organizations and states.

Public organizations are also exposed and should be able to manage and respond to cybersecurity incidents.

1.1. Problem

According to the European Commission [6], in 2016 alone, there were more than 4000 attacks per day using sequestration software, also called ransomware, with 80% of companies suffered at least one cybersecurity incident. This document further notes that, in the last four years alone, the economic impact of cybercrime has increased fivefold.

One of the public cases that occurred on May 12, 2017 was the ransomware attack which became known as WannaCry.

This incident with WannaCry, and according to the National Audit Office's (NAO) investigation report in the United Kingdom, has spread to more than 200,000 computers and has had an impact in a short space of hours in more than 100 countries. The damages caused were in the most diverse areas.

It highlights the health area in England, where the National Health Service (NHS) has been affected and has disrupted services, leading to the cancellation and postponement of numerous consultations [11].

Bearing in mind the article published in the SapoTek, it is possible to extract that threats to cybersecurity are growing, hackers are specializing and the risks increase with increasing economic impacts, (...) security breaches that are many hidden times because the organizations have not yet discovered or revealed that they were attacked [17].

Still recently, on August 4, 2018, it was known by the newspaper Diário de Notícias[1] that CUF Hospitals belonging to the José de Mello Saúde group, in Portugal, were subjected to a computer attack that prevented the use of the group's computers.

The computer virus that infected the hospital systems was named SamSam and blocked access to information. Because of this situation, access to patient records was difficult or even impossible.

These are some of the real examples that have happened and which show that cyberattacks often occur as well as some of their effects.

[1] See: https://www.dn.pt/pais/interior/hospitais-da-cuf-alvo-de-ataque-informatico-9678447.html; Access in 10-09-2018

Noting the national data contained in the RASI [18] for 2017, and for cybersecurity, the National Computer Security Incident Response Team, CERT.PT, received 1,895 notifications, of which 535 (about 28%) resulted in the opening of incidents analyzed and successfully resolved.

Of the incidents analyzed and resolved, 17% affected directly or indirectly state entities, which represents an increase of 8% compared to 2016.

Also in RASI, it is mentioned that computer crime is practiced using technology, it is a generalized increase compared to 2016. In relation to cybercrime, ransomware, data exfiltration, exploitation of system vulnerabilities, containing sensitive user data, and equipment vulnerabilities.

From the above, we ask a question that leads us to the problem: Will public organizations be sufficiently prepared to manage cybersecurity incidents?

Faced with this reality, it is urgent that organizations prepare and train to make an adequate management of incidents of cybersecurity that can affect them. These should be managed according to a process for managing cybersecurity incidents.

With the accomplishment of this work we propose a reference process [2] based on international standards and guides of good practices, with the aim of contributing to the implementation of the cybersecurity incident management process in portuguese organizations.

1.2. Research Methodology

The research methodology adopted for this work is the *Design Science* (DS) [10].

The goal of DS is to be useful in creating and evaluating artifacts to solve identified organizational problems. Artifacts can be constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implementations and prototypes of systems).

We intend with this research to create an artifact for a specific problem. This Information Technology (IT) artifact is defined as a method.

As a reference in this work, we will follow the Information Systems Research Framework, [10], which presents conceptually, according to Figure 1, the structure to understand, research in an Information System.

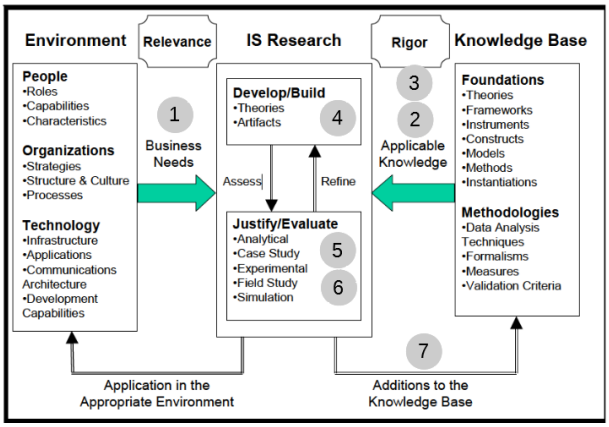

Figure 1: *Information Systems Research Framework* - Adapted [10]

In order to understand the relationship between the phases of the Information Systems Research Framework and the structure of this dissertation, which is organized in seven chapters, we introduce in the Figure 1 markers with numbers 1 to 7 and which are mapped with each of its chapters.

In section 1 we make the framing, contextualization and identification of the problem and the motivation to carry out this work. As a research method we refer to and adopt the methodology *Design Science*. Then, in the section 2 the literature review. In section 3 we present the result of interviews conducted with cybersecurity specialists.

In section 4 we present the objectives for a solution. In the section 5 we demonstrate the solution that will be subsequently evaluated. We evaluated the work developed in section 6 and finally, in section 7 we conclude the research work and perform an analysis of the work performed, presenting contributions, limitations and proposals for future work.

2. Related Work

In this section we refer to a set of related basic concepts, the applicable legal framework, international standards and reference guidelines on the subject.

2.1. Basic concepts

We present some of the basic concepts used in this work and their definition for better understanding and contextualization.

In the context of this report, and for the sake of simplicity, we will designate information security incidents due to cybersecurity incidents. When referring to incidents, it means incidents of cybersecu-

[2] We refer to a process that serves as a reference

rity.

Incident - an event with a real adverse effect on the security of networks and information systems [12] [13]. Actions taken through the use of a computer network that result in a current or potentially adverse effect on an information system and/or the information stored therein [1].

Cyberattack - an attack by information technology in cyberspace directed against one or more systems, in order to jeopardize the security of information and communication technologies (confidentiality, integrity and availability), in whole or in part [3].

2.1.1. Public Administration

The Portuguese Public Administration is a vast and complex reality [8]. Organically it is a system of organs, services and agents of the State and other public entities, which with the development of their activities, aim at the regular and continuous satisfaction of collective needs.

It comprises three large groups of entities. The Direct Administration of the State that is hierarchically subordinated to the Government, as supreme organ of the Public Administration; the indirect administration of the State that is subject to its superintendence and guardianship; and the autonomous administration that is subject to its guardianship.

2.1.2. CERT

It is a team of computer security experts whose main activity is to respond to computer security incidents requested by the user community served [2]. A dedicated IT security team helps organizations mitigate and prevent incidents as well as protect their resources. Other possible benefits are:

- Centralized coordination for computer security issues in the organization.
- Centralized and specialized management and response on computer incidents.
- Have available experts to support and help users recover from security incidents.
- Addressing legal issues and preserving evidence in case of legal action.
- Monitor developments in the field of security.
- Encourage cooperation on computer security within the user community.

2.2. Legal

The applicable legal framework includes several diplomas related to cybersecurity. We analyzed those considered more relevant.

2.2.1. NIS Directive

The Directive (EU) 2016/1148 of the European Parliament and of the Council [13], of 6 July 2016, It was the first horizontal legislative act of the EU addressing cyber security challenges and was a turning point with regard to Europe's cybersecurity resilience and cooperation capabilities. The NIS Directive has three main objectives [5]:

- improve national cyber security capabilities;
- strengthen cooperation at EU level;
- promote a culture of risk management and incident reporting among the main economic actors, including operators of essential services for the maintenance of economic and social activities and digital service providers.

Article 9 expressly refers to the security of information technology systems and requires the adoption of specific technical and organizational measures relating to the maintenance of a sound information security framework for the management of computer security risks.

Measures that should include mechanisms and procedures that guarantee the availability of services, as well as the protection of the authenticity, integrity and confidentiality of data [4].

2.2.2. National Cybersecurity Centre

Its mission is to ensure that the country uses cyberspace in a free, reliable and secure way, through the promotion of the continuous improvement of national cybersecurity and international cooperation, in conjunction with all competent authorities.

As well as the definition and implementation of the measures and instruments necessary for the anticipation, detection, reaction and recovery of situations which, in the face of imminent or occurrence of incidents, jeopardise the national interest, the functioning of the Public Administration, the critical infrastructure operators, essential service operators and digital service providers [1].

2.3. National Strategy for the Security of Cyberspace

Portugal has an ENCS that was approved by RCM nº. 36/2015 [15], dated June 12, and currently in effect. With a commitment to enhancing network and information security as a way to ensure the protection and defense of critical infrastructures and vital information services, and to promote the free, secure and efficient use of cyberspace by all citizens, companies and public and private entities.

The ENCS defines the framework, objectives and lines of action of the State in this matter, according to the national interest and is approved by

resolution of the Council of Ministers, on proposal of the Prime Minister, after hearing the Council of Security of Cyberspace [1]. Its general and specific orientation is translated into six axes of intervention.

2.4. Standards and guides

We have analyzed a set of national and international standards and guides, which we will mention: the Reaction Maturity Model of the CNCS; the Taxonomy; the Traffic Light Protocol - TLP; SIM3; ITIL; COBIT; SANS; and lastly, we paid special attention to the ENISA's Good Practice Guide for Incident Management, NIST's Computer Security Incident Handling Guide and finally to ISO/IEC 27035. All these documents contain important contributions to this work.

3. Interviews

Based on the analysis of the literature and legal framework identified, we elaborated a set of questions that were made, through interviews, to specialists in the area of cybersecurity. The issues were elaborated taking into account what is indicated as being the one that exists to do incident management.

The purpose of these interviews was, on the one hand, to collect the answers to the presented questions, and to extract causes that lead to the insufficient preparation of the organizations for this subject, and on the other to collect other relevant contributions for the definition of the method.

3.1. Framing

The ten experts were selected from different sectors and organizations. The selection of the interviewees sought to diversify the profiles, the entities to which they belong, the functions performed and the years of experience. It was intended that the answers obtained be diverse and comprehensive.

The structure of the interview was composed of two sections. In the first section, we interviewed the interviewees, questioning personal information about the level of education, position or function, years of experience in security/cybersecurity and the sector to which they belonged. In the second section, the incident questions were presented.

3.2. Summary

After completing the ten interviews, we extracted some important contributions that will be integrated into this work.

It has been stated that the weakest link will be the human being and that cybersecurity incidents are essentially caused by inappropriate user behavior. The path is to develop training and training plans tailored to all employees.

Cybersecurity must be transversal to the whole organization and not be in vertical silos. In this regard, time is crucial; decision-making must be swift and supported at the highest level of the organization.

Know all the assets of the organization, by different needs, to be able to take appropriate and concrete measures.

In addition to the contributions obtained there was interest in identifying some causes for the insufficient preparation of the organizations.

We indicate some of the causes identified:

- the organic readjustment in the structure of public organizations, mergers or separation of organisms;
- the lack of inventory and identification of all assets;
- the lack of human resources;
- the training and training of human resources;
- the constraints of public organizations at the level of public procurement and budget management;
- difficulties in access to training;
- lack of policies and procedures;
- the investments made to which no profit is taken.

4. Proposal

We present our proposal to solve the problem identified in section 1 and the objectives that we propose to achieve.

In accordance with the requirements of the process of constructing an artifact as referred to in DS, we have constructed a method that implements a reference process for the management of cybersecurity incidents. According to Hevner et al. [10], the methods define processes and provide guidance on how to solve problems. These guidelines may be textual and informal descriptions of best practice approaches or combinations.

This proposal comes from the literature and related work and also from the contributions obtained from interviews with experts in the field.

4.1. Goal

The objective we propose to achieve is to contribute to the implementation of the process of managing cybersecurity incidents in Portuguese organizations. This contribution can mean an initial course, where nothing is defined and implemented, to more advanced situations where the

incident management process is already in place and can introduce improvements.

4.2. Proposal method

Incident management should be done in a methodical way and have defined a set of phases with the practices to be developed.

The proposed reference process is aligned with ISO/IEC 27035 and follows its guidelines. We justify this decision on the basis of the indications in the legal framework where it refers to *"the use of internationally accepted standards and technical specifications"* [1], and *"Adoption of standards and good security practices of cyberspace "* [15]. The ENISA guide also [9] refers to the adoption of ISO/IEC 27002, which in turn refers to ISO/IEC 27035.

We propose a reference process consisting of five phases composed of practices and objectives to be achieved in each one of them. The phases that we identified to be included in the process should be the following:

4.2.1. Planning and Preparation

Managing cybersecurity incidents to be effective and efficient requires proper planning and preparation. To this end, a set of practices should be working. For this phase the following practices should be implemented:

- Identify the objectives, stakeholders inside and outside the organization, specify the type of incidents that are addressed, what functions should be included, benefits to the organization and its departments, to formulate and produce an incident management policy cross-sectional cybersecurity throughout the organization and with the approval, commitment and support of top management;
- Align and update information security, risk management and other policies at the organization, system, service and network level;
- To implement a detailed plan for the management of cybersecurity incidents, with whom communications should be established and how information should be disseminated; This disclosure shall be made in accordance with the provisions of TLP;
- Constitute a CSIRT, with adequate training and training updated to all its elements. The establishment of an incident response capability is essential and must exist, if it is contractualized it is the responsibility of the organization to guide this capacity;
- Establish relationships and links with internal and external organizations that are directly involved in the management of events, incidents and vulnerabilities;
- Establish and implement the technical, organizational and operational mechanisms required to operationalize the CSIRT activity. Develop and implement the information systems required to support CSIRT, including a database. These mechanisms and systems are intended to prevent the occurrence of incidents or the likelihood of occurrence. (eg: *firewall*, anti-virus, ticketing system such as RT/RTIR [3] or OTRS [4]);
- Plan and develop an awareness and training program on events, incidents and vulnerability management;
- Test the incident management plan, processes and procedures.

4.2.2. Detection and Participation

This phase involves the detection, through associated information and reports on the occurrence of events and the existence of vulnerabilities, by manual or automated means. The participation of events and vulnerabilities does not mean that they are considered and classified as incidents and can be analyzed later, if necessary. For this phase the following practices should be implemented:

- Monitor and collect logs from the systems and network activity for which CSIRT is responsible;
- Detect and report the occurrence of an event or the existence of a vulnerability, either manually or automatically;
- Gather information about an event or vulnerability;
- Have information about what is happening, a situational picture of internal and external data sources, including system and network traffic, activity logs, news feeds political, social, or economic activities that may affect the activity of the incident, external trends of incidents, new attack vectors, indicators, new strategies and mitigation technologies;
- Assure that all related practices, results and decisions are duly recorded for further analysis;
- Assure that digital proofs are collected and stored securely and that their preservation is safely and continuously monitored if evidence is necessary for legal proceedings or internal disciplinary actions;
- Warrant that change tracking is followed to track events and vulnerabilities and keep the database updated;
- Scale, as needed, during the course of this phase, for further review or decisions.

[3] See: https://bestpractical.com/rtir/; accessed 10-10-2018
[4] See: https://community.otrs.com/; accessed 10-10-2018

4.2.3. Analysis and Evaluation

At this stage, the information associated with the occurrence of events and the decision to classify an event as a cybersecurity incident are evaluated. Once an event has been detected and reported, the following practices should be implemented:

- Distribute responsibility for incident management practices, through an appropriate hierarchical chain, to people who will carry out assessment, decision making and actions involving people who may or may not be related to cybersecurity, if necessary;
- Provide procedures that each notified person must follow, including reviewing and correcting reports, to evaluate damages and notify relevant persons. Individual actions depend on the type and severity of the incident;
- Use guidelines to document an event and the subsequent actions for an incident if the event is classified as an incident;
- Gather information that may include testing, measurements, and other data about detecting an event. Type and amount of information collected will depend on the event that occurred;
- Conduct an assessment to determine if the event is a possible incident or a false alarm. A false positive is the indication of an event that has been detected and reported and is not a real threat or has no consequence. In the case of an incident, it must be classified according to an incident class and incident type according to the taxonomy in use of RNCSIRT. If necessary, CSIRT can review the assessment to ensure that the incident has been properly declared;
- Assure that all parties involved, in particular the CSIRT, record all practices, results and decisions for further review;
- Assure change tracking log is maintained in order to track the incidents and updates you are receiving in an incident report, thereby keeping database updated.

4.2.4. Response and Documentation

This phase involves responding to incidents according to the actions determined in the analysis and evaluation phase. Depending on the decisions, responses can be made immediately or in a short time, and in some cases a security investigation may be required. Once an incident has been confirmed and the responses determined, the following practices should be implemented:

- Distribute responsibility for incident management practices through an appropriate hierarchical chain to people who have to make decisions and actions involving people who may or may not be related to cybersecurity as needed;
- Provide procedures that each person involved should follow, including reviewing and amending reports, reassessing damages, and notifying relevant people. Individual actions depend on the type and severity of the incident;
- Use guidelines to thoroughly document an incident and subsequent actions;
- Investigate incidents according to their classification. Sorting can be changed if necessary. Research may include different types of analysis to provide a deeper understanding of incidents;
- Determine if the incident is under control and, if so, execute the required response. If the incident is not under control or will have a serious impact on the organization's activity, conduct crisis response practices through escalation to the crisis management function;
- Assign internal resources and identify external resources in order to respond to an incident;
- Scale as needed throughout the phase for future evaluations or decisions;
- Assure that all parties involved, in particular the CSIRT, record all practices for further review;
- Assure that digital proofs are collected and stored securely and continuously preserved if necessary for legal proceedings or for internal disciplinary action;
- Assure that change tracking log is maintained in order to track the incidents and updates you are receiving in an incident report, thereby keeping your database updated;
- Communicate the existence of the incident and share relevant details (eg: information on threats, attacks and vulnerabilities) with other individuals or internal and external organizations, in accordance with the organization's standards and communication plans and CSIRT. It may be important to notify asset owners (determined during impact analysis) and internal and external organizations (eg: other CSIRTs, National Authorities - CNCS, PJ, Internet service providers and other organizations in a community) that could assist in the management and resolution of the incident. Sharing information can also benefit other organizations, as the same threats and attacks often affect multiple organizations. Information sharing should be done in accordance with the TLP;
- Evaluate whether after an incident recovery, an after-incident analysis should be started, depending on the nature and severity. This includes investigation of incident information,

other relevant sources, such as personnel involved and reporting of research findings;
- Prepare a final report after the incident has been resolved and closed, from which all interested parties should be notified.

4.2.5. Lessons Learned

The lessons learned phase occurs when incidents and vulnerabilities are resolved. Learning about how incidents and vulnerabilities have been addressed should be removed. Lessons learned should translate into improvements or changes to be made and incorporated into planning and preparation. To this end, the following practices should be implemented:

- Recognize the lessons learned from incidents and vulnerabilities, and analyze exactly what happened and at what times;
- Identify and optimize the implementation of security controls as well as the cyber-security policy. Contributions for the implementation of new controls or updates of others already in place may arise from one or several reported incidents or vulnerabilities. The changes that have to be made have to be inserted into the organization's strategy to know what investments are needed;
- Review and improve risk assessment and management in the organization;
- Check the efficiency of processes, procedures, reports and organizational structure in responding, evaluating and recovering from incidents and dealing with vulnerabilities. Based on the lessons learned, identify and refine the incident management plan and its documentation;
- Communicate and share evaluation results within a community, if the organization want;
- Verify that information about an incident, related attack vectors, and vulnerabilities can be shared with other organizations in a partnered community to prevent the same incidents from spreading to those organizations. This information sharing should be done in accordance with the TLP;
- Periodically evaluate the performance and effectiveness of CSIRT. The maturity evaluation can be done according to the SIM3 model.

The practices of the incident management process are iterative. The organization shall make improvements or corrections where those needs are identified over time.

Based on the analysis of incident and vulnerability data reported and responses to incidents, changes should be proposed, both to safety elements and to measures to be taken and implemented, as well as to the incident management process itself.

5. Demonstration

We have chosen a public organization, the fictitious name DemoPub, which provides services in the area of cybersecurity, characterized by having a CSIRT constituted and mature in response to incidents. It already has the process of management of incidents of cybersecurity implemented and expressed interest in that its process be evaluated by comparison with the solution presented here.

5.1. Goal

The purpose of this demonstration was to evaluate if the process of incident management, implemented and in use by DemoPub, could be improved, taking into account the proposed reference process and based on the work developed in this dissertation.

5.2. Self-evaluation

We started the demonstration with the framework and the presentation of the solution to the person responsible for the CSIRT and one of its technicians. We describe the structure and the desired one with the phases to be carried out, corresponding practices and what was expected to be achieved in each of them.

We started by verifying that they had documents that establish their operation and that they are in agreement with the one considered in the practices of the phase of Planning and Preparation.

They have a written manual where their entire incident management process is defined with the policies described and applied, procedures to be adopted and that support their activity.

We have compiled comparative tables, for each of the phases and compare what "Consist" and "Not Consist" in each of the corresponding practices and in each of the process.

We performed a complete iteration of the proposed reference process simultaneously with the execution and management of an incident.

In the Response and Documentation phase, and in the comparative results we indicate a practice that is not foreseen in the DemoPub process.

We have completed the demonstration and have verified that the incident management process that DemoPub has implemented is already at a high level of achievement compared to the proposed reference process.

6. Evaluation

We began by evaluating the results of the interviews with ten cybersecurity specialists, then we

present the results obtained from the demonstration, which we carried out with an organization, and we also evaluated whether the artifact we produce meets the requirements of the research methodology used.

6.1. Interview evaluation

The interviews that were carried out had the objective of gathering contributions for this dissertation. By evaluating the obtained answers we obtained and extracted contributions and from them we were able to validate that the management of cybersecurity incidents has to be done in a methodical and structured way.

That has to be seen in a holistic and transversal way to the whole organization.

With the contributions obtained from the interviewees and the content of their answers, it was possible to validate several common points in the phases of the solution that we presented.

6.2. Demonstration evaluation

The demonstration took the form of a self-evaluation carried out in a public organization.

Through this self-assessment, an organization's cybersecurity incident management process was compared to our process. We evaluated the process in all its phases, and carried out the respective practices, checking each individually.

In the end, a practice was identified that our process identifies how to perform and the DemoPub process does not contemplate.

It identifies at this point an improvement that must be implemented and recognized as an asset. It was found that a final report of each incident was missing and it was not contemplated.

Despite the referral process we submitted to be high level, we found that the goal was achieved as can be derived from this demonstration.

In this regard, we note that the benchmarking process for cybersecurity incident management brings benefits and contributed to improving the implementation of an already existing process.

6.3. Artifact evaluation

It is mentioned in the DS research methodology that it is necessary to apply rigorous practices in the evaluation of the artifacts drawn.

For this, we propose to evaluate the artifact according to *Prat et al.* [14], in which it proposes a hierarchy of evaluation criteria for information system artifacts, organized according to the dimensions of a system and which are: the objective, the context, the structure, the activity and the evolution.

For each of these dimensions, a set of criteria was defined, detailed in subcriteria. We have selected three criteria to evaluate our artifact.

We chose the criteria: context - consistency with people - easy to use; context - consistency with the organization - utility; and structure - level of detail. We considered the most adequate to our research and referred to as relevant criteria by Hevner et al., [10].

Context - consistency with people - easy to use: the solution provides a clear objectivity of what is intended. The fact that it is written in the Portuguese language becomes easier to perceive and use.

Context - consistency with the organization - utility: the solution was created for organizations. It answers a problem that has been identified and demonstrated in practice, so its usefulness is justified.

Structure - level of detail: the solution presents a level of detail considered adequate and systematized, comprehensive and high level.

Since the artefact is supported and aligned with an international standard, we can consider it as valid to achieve the proposed objective. An organization that adopts and makes alignment with the ISO/IEC 27035 standard is prepared in the future to achieve ISO/IEC 27001 certification.

In summary, and at the end of this evaluation we can conclude that the artifact reaches the goal we propose and contributes to the implementation of the cybersecurity incident management process in Portuguese organizations.

7. Conclusions

We now present the conclusions drawn from the realization of this dissertation, presenting the contributions and indicating the limitations encountered and also proposals for future work development. The purpose of this research was to define a method, also known as a reference process, for the management of cybersecurity incidents.

From the results of the evaluation we conclude that the artifact created contributes to solve the problem of insufficient preparation of Portuguese organizations to manage incidents of cybersecurity, thus fulfilling the objective that we propose.

The management of cybersecurity incidents must be carried out due to the need to guarantee the security of the information, according to D. Santos [16]. Without such a guarantee and security, essential functions in society can be called into question.

The assets of any organization are people, data, and processes. If any of the three are compromised the rest will be affected. We highlight the importance of inventorying all assets, their adequate protection and defense.

The management of cybersecurity incidents is not only a technical issue and must be addressed in a preventive and not only reactive way. It should also be seen as part of a global and integral process of the organization. To be seen as a journey that is built with capacity and maturity and that adds value, involving the organization as a whole and having the commitment and its support by the top management.

We can conclude that there are some public organizations where their maturity level is recognized in the management of cybersecurity incidents and have an incident management process already implemented and documented. On the other hand, we identified by the interviews, that there are organizations that are starting their process and others that have nothing defined to manage incidents.

In response to the issue we raised in the problem, we concluded that Portuguese organizations, public and private, are not yet sufficiently prepared to manage such incidents. It is necessary to go through a long journey of adaptation and transformation. Organizations should qualify in this area [7].

We conclude that the weakest link will be the human being and that incidents of cybersecurity are essentially caused by inappropriate user behavior. The path is to develop training and training plans tailored to all employees.

We can conclude that the adoption of a recognized international standard, as in this case ISO/IEC 27035, has advantages in terms of harmonization and interoperability.

The possibility given to us to carry out the demonstration of our solution in practice allowed us to verify the incident management and response, and with that to understand its processing and the previous work that needs to be done.

7.1. Contributions

As a contribution, we would like to point out that the guidelines in ISO/IEC 27035 should be followed in order to manage incidents of cybersecurity. In addition, the adoption of this standard, which complements other standards, allows certification in the future under ISO/IEC 27001.

We present, as a contribution, some of the causes identified for the insufficient preparation of the organizations, in which we refer: the organic readjustment in the structure of public organizations, mergers or separation of organisms; lack of inventory and identification of all assets; lack of human resources, training and capacity building; the constraints of public organizations at the level of public procurement and budget management; difficulties in access to training; the absence of policies and procedures; the investments made to which no profit is taken.

Also as a contribution, it is mentioned that at the end of the Research Methodology of Design Science there should be addition of contributions to Knowlegde Base, and our contribution is the research work that was developed in this dissertation.

7.2. Limitations

The artifact produced translates a high-level method that lacks further detail in future developments.

Implementing this solution in an organization that is initiating the implementation of the cybersecurity incident management process can be time-consuming for the requirements it needs.

The number of items that ISO/IEC 27035 presents is extensive and each organization needs to adapt to its reality and dimension.

7.3. Future work

As future work we propose the development of the method regarding the procedures and guidelines necessary to each of its phases and the design of workflows.

Still as future work, we propose the development of reports for the participation of incidents to the portuguese authorities.

As a final proposal we understand that it would be interesting to implement the solution in its completeness in an organization and to follow it from beginning to end.

Finally, it should be noted that we follow and comply with the guidelines presented in the research methodology and we give this research work concluded.

References

[1] Assembleia da República. Lei n.º 46/2018 - Regime Jurídico de Segurança do Ciberespaço, Agosto 2018.

[2] H. Bronk, M. Thorbruegge, and M. Hakkaja. A step-by-step approach on how to set up a csirt. https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport/CSIRT_setting_up_guide_ENISA.pdf. Accessed in 12-08-2018.

[3] Centro Nacional de Cibersegurança. Glossário. https://www.cncs.gov.pt/recursos/glossario/. Accessed in 23-09-2018.

[4] Comissão Europeia. Anexo da Comunicação da Comissão ao Parlamento Europeu e ao Conselho. https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017DC0476&qid=1538255134349&from=EN. Accessed em 02-01-2018.

[5] Comissão Europeia. COM(2017) 476 - COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO. https://ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-476-F1-PT-MAIN-PART-1.PDF. Accessed in 02-01-2018.

[6] Comissão Europeia. Estado da União 2017 – Cibersegurança: Comissão reforça a resposta da UE aos ciberataques. http://europa.eu/rapid/press-release_IP-17-3193_pt.pdf, Maio 2017. Accessed in 02-01-2018.

[7] Computerworld. Preparar os trabalhadores para a cibersegurança. https://static.computerworld.com.pt/media/2018/01/CW_janeiro_2018-preparar-os-trabalhadores-para-a-cibersegurança.pdf, Janeiro 2018. Accessed in 12-08-2018.

[8] Direção-geral da Administração e do Emprego Público. Organização da administração do estado. https://www.dgaep.gov.pt/index.cfm?OBJID=a5de6f93-bfb3-4bfc-87a2-4a7292719839&men=i. Accessed in 19-08-2018.

[9] ENISA. Good Practice Guide for Incident Management. https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management. Accessed in 15-12-2017.

[10] A. R. Hevner, S. T. March, J. Park, and S. Ram. Design science in information systems research. *MIS Q.*, 28(1):75–105, Mar. 2004.

[11] A. Morse. Investigation: WannaCry cyber attack and the NHS. Report HC 414 SESSION 2017–2019, National Audit Office, Apr. 2017. Accessed in 24-12-2017.

[12] National Initiative for Cybersecurity Careers and Studies. Glossary. https://niccs.us-cert.gov/about-niccs/glossary. Accessed in 23-09-2018.

[13] Parlamento Europeu e Conselho da União Europeia. Diretiva (UE) 2016/1148, de 6 de julho, Julho 2016.

[14] N. Prat, I. Wattiau, and J. Akoka. Artifact Evaluation in Information Systems Design Science Research - A Holistic View. *PACIS 2014 Proceedings. 23*, 2014.

[15] Presidência do Conselho de Ministros. Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho - Estratégia Nacional de Segurança do Ciberespaço. http://data.dre.pt/eli/resolconsmin/36/2015/06/12/p/dre/pt/html. Accessed in 02-09-2018.

[16] D. Santos. A Cibersegurança em Portugal: a ação política nacional em matéria de cibersegurança. Master's thesis, ISCTE-IUL, 2014.

[17] SapoTek. Cibersegurança: Cooperação entre diferentes entidades é obrigatória para enfrentar os riscos crescentes. https://tek.sapo.pt/noticias/computadores/artigos/ciberseguranca-cooperacao-entre-diferentes-entidades-e-obrigatoria-para-enfrentar-os-riscos-crescentes, Junho 2017. Accessed in 09-08-2018.

[18] Sistema de Segurança Interna. Relatório Anual de Segurança Interna 2017. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=9f0d7743-7d45-40f3-8cf2-e448600f3af6. Accessed in 06-06-2018.