A Strategy for Implementing an Incident Response Plan

Alexandre Fernandes[1], Adaíl Oliveira[1,2], Leonel Santos[1,2] and Carlos Rabadão[1,2]
[1]School of Technology and Management, Polytechnic of Leiria, Portugal
[2]Computer Science and Communication Research Centre, Polytechnic of Leiria, Portugal
alexandre.fernandes@ipleiria.pt
adail.oliveira@ipleiria.pt
leonel.santos@ipleiria.pt
carlos.rabadao@ipleiria.pt
DOI: 10.34190/EWS.21.080

Abstract: With the exponential growth of the Internet, several challenges and security threats arise. Those threats are due to the lack of adequate security mechanisms, security policy flaws, increasing usage of mobile devices, mobility, and user's naivety. Although organisations try their best to deploy effective security solutions and practices, there will always be security incidents. Therefore, they must place detection methods to identify those threats and vulnerabilities. On the other hand, response activities must be established to deal with and respond to the detected incidents. An Incident Response Plan (IRP) aims to provide an organisation with an easy-to-follow guide that leads to a quick and effective incident response. The implementation of such a plan is not an easy task. To implement an IRP requires an organisation a lot of research and analysis of the existing frameworks and examples. Most frameworks explain how to set up a Computer Security Incident Response Team and how they should handle incidents, but only a few instruct how to implement a plan. The proposal of this paper is to present a practical strategy on how to implement an IRP, complementing the existing incident response frameworks, thus reducing the difficulty of creating an effective and useful plan. The study and proposal of this topic come from the research and experience developed during the implementation of an academic Security Operation Centre. The paper starts by presenting the most relevant incident response frameworks and related work. It then proposes a flexible strategy for creating an IRP that can be adjusted to any organisation's scope and objectives. During the strategy presentation, the various domains of incident response are presented. Finally, strategies for its implementation will be introduced. As the main contribution of this work, the reader will be able to understand the common structure and content of an IRP and to create their own plan.

Keywords: incident response, CSIRT, framework, cybersecurity, security operations centre

1. Introduction

As technology grows and evolves, so does cybercrime. Attackers have increasingly sophisticated tools and strategies, and most organisations simply cannot prevent or block them. With the increase of computer attacks, companies are beginning to recognise the need and criticality of protecting their organisations, information and businesses from security threats or incidents.

After the occurrence of an incident, it is the security incident response team (CSIRT) that is responsible for handling the situation. However, for the team to respond adequately to a security incident, it is necessary to have some previously defined procedures. One of the most important procedures is the IRP, which is the focus of this work. The IRP is a procedural piece that describes the actions that an organisation must take to deal with security incidents and, consequently, minimise their impact, whether from cyber-attacks, data breaches, policy violations or other security incidents. As a reference document, its content must be practical and easy to understand. However, due to the diversity of needs and organisations' limitations, it is impossible to have a single plan that suits all organisations. The creation of an IRP is a complex task, and despite the diversity of existing standards and frameworks to guide this task's execution, organisations still do not know how to structure or implement theirs.

Some of the difficulties experienced by organisations are the lack of sufficient knowledge and the diversity of standards and frameworks, which is the cause of the delay in implementing a good IRP.

As the main contribution of this work, the reader will be able to understand the typical structure and content of an IRP and to create their own plan. Past this section, this paper is organised as follows: Section 2 offers the related works, including the analysis of standards and frameworks, examples of IRP and other scientific articles. Section 3 provides and discusses the proposed strategy and its model, presenting the various model's domains. Section 4 offers paths to implementation of the discussed strategy and model. Section 5 concludes this paper and mentions future work. The study and proposal of this work come from the research and experience developed during the implementation of an academic Security Operation Centre.

2. Related work

Initially, in this section, several reference standards and frameworks related to the implementation of an incident response program were collected and analysed to understand the recommendations proposed by the main reference entities and assess whether they are easily applicable or simple to follow. Subsequently, several examples of incident response plans, proposed by entities from the most diverse activity sectors, were studied, crossing their content with the previously analysed standards and frameworks. A search was also carried out in the leading databases of scientific works.

2.1 Standards and frameworks

We sought to understand the main objectives and what type of information they provide by taking the most popular incident management frameworks and standards. Some of the analysed documents are: (i) SANS: Creating and Managing an Incident Response Team (Proffitt, Timothy; SANS, 2007); (ii) RFC 2350: Expectations for Computer Security Incident Response (Brownlee & Guttman, 1998); (iii) CERT: Handbook for Computer Security Incident Response Teams (CSIRTs) (West-brown, Stikvoort, & Kossakowski, 1999); (iv) NIST 800-61: Computer Security Incident Handling Guide (Scarfone, Grance, & Masone, 2012); (v) ENISA: Good Practice Guide for Incident Management (ENISA, 2010); (vi) ISACA: Incident Management and Response (ISACA, 2012); and (vii) ISO/IEC 27035-2:2016: Information Security Incident Management (International Organization for Standardization, 2016). The SANS document (i) includes the definition of the different CSIRT services, policies, and standards, identifies a sequence of phases regarding incident response and ends with some important details about CSIRT members. Regarding RFC 2350 (ii), this RFC provides CSIRT teams with a way to publicly publicise their services and scope in a comprehensive, simple, and common structure between different entities, thus, allowing CSIRT constituents to know its CSIRT's policies and procedures. Created by CERT, the Handbook for CSIRTs (iii) aims to provide materials and suggestions for the creation and operation of a CSIRT and an incident handling service. The document defines a framework that includes the definition of the mission, organisation, services, CSIRT policies, among others. In addition, it also addresses several details regarding functions and interactions during the handling of incidents. NIST 800-61 (iv) has a structure similar to the previous document. This document begins by defining how to organise the security incident response through the creation of policies, plans and procedures, as well as the structure of a CSIRT. Subsequently, it presents a framework of several phases of an incident, including a checklist and recommendations. Finally, it includes some topics on coordination and information sharing. The ENISA guide (v) mainly includes practical tips for application in the incident handling process, presenting a workflow and a life cycle for incident response. Like the previous ones, this document also addresses and offers suggestions for the definition of mission, organisation, and responsibilities in this matter. Finally, the topics of communication and cooperation between other CSIRTs or authorities are addressed, together with the issues of outsourcing and presentation to management. The ISACA document (vi) also defines an incident life cycle's phases, the associated security strategies, and other governance activities. This document recommends the use of the COBIT framework (IT Governance Institute, 2007) to structure incident response processes. Finally, ISO/IEC 27035-2 (vii) presents guidelines for planning and preparing for incident response. It mainly focuses on defining and updating security policies and a security incident management plan. It also has several topics about creating a CSIRT and its relationship with other organisations or entities. It ends with recommendations on the topics of awareness, training, IRP testing and on ways to evaluate and improve the different processes.

Almost all the presented frameworks include the definition of a workflow or a life cycle of a security incident with several recommendations on how to act during any of its phases. These documents present suggestions on implementing or designing a CSIRT and what to include in an IRP. However, there are no recommendations on how it should be structured, nor what path to follow when implementing it.

2.2 Examples of published Incident Response Plans

Following the previous documents evaluation, several incident response plans from different activity sectors were identified and collected. To evaluate each plan's content, the authors considered the frameworks and standards to determine the most important topics to include in a plan. The identified topics are: Purpose and Scope; Roles and Responsibilities; IR Life Cycle; Communication Plan; Metrics; SLAs; Plan Test and Review; IR Training; Taxonomy; Incident Classification; and Playbooks. The performed analysis is systematised in Table **1**.

Table 1: Comparison of several IRPs

Incident Response Plan	Purpose and Scope	Roles and Responsibilities	IR Life Cycle	Communication Plan	Metrics	SLAs	Plan Test and Review	IR Training	Taxonomy	Incident Classification	Playbooks
University Carnegie Mellon	✓	✓	✓	±	±	×	±	±	×	×	×
Tulane University	✓	✓	✓	✓	×	×	×	×	×	✓	✓
University of Adelaide (Data breach)	✓	✓	✓	✓	×	×	×	±	×	×	✓
University of Alabama	✓	×	×	✓	±	×	×	×	×	×	✓
LGPD - PROCEMPA	×	±	✓	✓	×	×	×	×	×	×	×
Stinson Leonard Street	✓	✓	✓	✓	×	✓	±	×	✓	✓	×
Criminal Justice Information Center	✓	×	✓	±	×	×	±	✓	×	✓	✓
OSCIO EIS (Sample)	×	✓	✓	✓	×	×	±	±	×	×	×
Universidade Federal do Rio de Janeiro	✓	×	±	×	×	±	±	×	×	×	×
HU-UFJF (EBSERH)	±	✓	✓	×	✓	×	×	×	✓	✓	×
EGPr-TIC	✓	✓	✓	×	✓	×	×	×	×	✓	×
Texas Southmost College	✓	✓	✓	×	×	✓	×	±	×	✓	×
Western Oregon University (Data Breach IRP)	×	✓	×	✓	×	×	±	±	×	×	✓
JSM Marketing Services	✓	✓	✓	✓	×	×	✓	×	×	×	✓
Total (✓/ ± / ×)	10/1/3	10/1/3	11/1/2	8/2/4	2/2/10	2/1/11	1/6/7	1/5/8	2/0/12	6/0/8	6/0/8

± - Reference to the topic or information too limited; ✓ - Information present; × - Information not present

According to the table above, the most used topics are "Purpose and Scope", "Roles and Responsibilities", "IR Life Cycle", and "Communication Plan". There is some divergence in the parameters in the different plans analysed, which is probably due to: (i) the complexity and diversity of standards and frameworks; (ii) the specificities of each organisation; and (iii) the absence of systematisation of what an IRP should be. Therefore, it is understood that there is a need to design a practical IRP implementation strategy capable of contributing to this problem's resolution.

2.3 Scientific contributions

In addition to studying existing standards and frameworks and analysing existing IRPs, research for scientific papers related to this topic was also performed to find work that might assist in the practical implementation of an IRP. For this objective, a search was carried out in the leading databases for scientific works (IEEE, ACM,

others) produced in the last five years, using the terms considered most relevant, systematised in the following search key: "security AND incident AND response AND (framework OR plan OR methodology OR playbook)". As a result of this research, about eight dozen works were identified, namely in international conferences, journals, and books.

The most relevant works identified are: (i) SOTER: A Playbook for Cybersecurity Incident Management (Onwubiko & Ouazzane, 2020), that in addition to analysing the different terminologies used in the management of security incidents and providing a mapping of equivalences, proposes and discusses an incident classification and prioritisation scheme, to finally present a framework for incident response procedures according to its context, classification and time of occurrence; (ii) Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field (Al-Dhaqm, Razak, Siddique, Ikuesan, & Kebande, 2020), that proposes suitable steps for constructing and integrating the Incident Response Model that can be relied upon the database forensic investigation field; and (iii) Context for the SA NREN Computer Security Incident Response Team (Mooi & Botha, 2016), that defines the business requirements for establishing a CSIRT, within the context of SA NREN CSIRT, resulting in "strategic" framework that sets a background for the establishment processes. The remaining articles focus on other subjects not relevant to this work.

Although the scientific papers presented similar address subjects, none of the reviewed documents provides a strategy or practical model for implementing an IRP, making this article an original contribution.

3. Strategy for designing an IRP

Following the lack of a practical IRP implementation strategy, the authors understood the need to contribute to the security incident response process's systematisation, having outlined an IRP implementation strategy for this purpose. At first, the potential difficulties and concerns in implementing an IRP were analysed to identify the strategy's objectives. Not having enough knowledge to implement an IRP, the existence of many standards and frameworks, and the delay in implementing a good plan are some of the difficulties experienced by organisations. Thus, considering these difficulties, the defined strategy should be phased and progressive, adjustable to different realities, and both practical and quick to implement. These requirements led us to the definition of a practical model for an IRP design.

The related work analysis and the experience acquired during the activities in an Information Security Office identified some relevant topics to consider in an IRP. Table 2 presents the relation between the specified subjects and the standards/frameworks that contemplate them. The ticked boxes mean that the respective document provides material or recommendations on implementing the subject.

Table 2: Topics coverage on frameworks

Framework/ Standard	Purpose and Scope	Roles and Responsibilities	IR Life Cycle	Communication Plan	Metrics	SLAs	Plan Testing and Review	IR Training	Taxonomy	Incident Classification	Playbooks	Templates
SANS: CM IRT	-	X	X	-	-	-	-	X	X	X	-	-
IETF: RFC 2350	X	-	-	-	-	-	-	-	X	X	-	-
CERT:Handbook for CSIRTs	X	X	X	X	-	-	-	X	-	X	-	-
NIST 800-61	X	X	X	X	X	-	-	X	-	X	X	X
ENISA: Gd Prt Guide for IM	X	X	X	X	-	X	X	X	X	X	-	-
ISACA: IMR	X	X	X	X	X	X	-	X	-	X	-	-
ISO/IEC 27035-2:2016	X	X	-	X	X	-	X	X	X	X	-	X

After defining the objectives and selecting the most important topics to include in an IRP, a model of implementation was created. This model is divided into three domains that go from the essential components of a plan to the components of continuous evolution, ending with useful tools to improve the performance of its execution, thus including all topics referenced before. Figure 1 represents the proposed model.

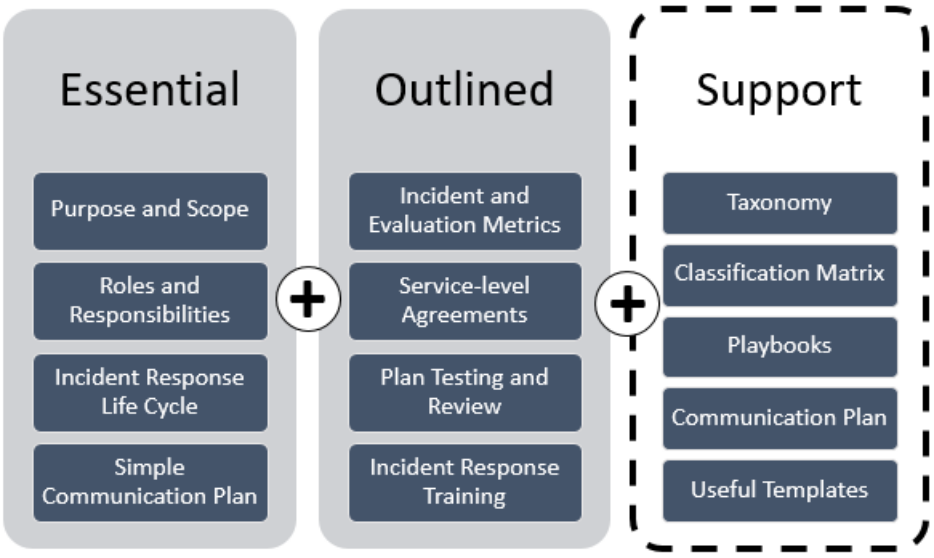

Figure 1: The proposed model for implementing an IRP

3.1 Essential

The first domain, Essential, corresponds to the initial stage of building an IRP. The topics that are considered most important to be in an IRP are part of this step, allowing the creation of a simple but useful and functional IRP. In this phase, the topics "Purpose and Scope", "Roles and Responsibilities", "Incident Response Life Cycle", and "Simple Communication Plan" will be addressed.

3.1.1 Purpose and scope

An IRP must be implemented and executed with the collaboration of key stakeholders. To understand what is reasonable to expect from the security team, it is crucial to know the community served and the services offered to the community. Furthermore, this section usually includes the mission, constituency, authority, responsibility, and services of the incident response team/process. Based on the analysed plans, some of them also place an organisation chart to locate the incident response team within the organisation (Stinson Leonard Street, LLP, 2017).

3.1.2 Roles and responsibilities

The structure and responsibilities of the incident response team must be clear. An IRP must define and present each team member's roles and tasks. In addition, it should also identify the main stakeholders and their responsibilities in the incident response service, as represented in Table 3. It is essential to highlight user participation's importance since, without their input, CSIRT services' effectiveness can be significantly reduced, particularly with reporting incidents.

Table 3: Roles and responsibilities (example)

Title/Role	Responsibility
Chief Information Officer	- Maintain and Enforce this Procedure. (…)
Security Analyst Tier 1	- Monitor systems and activity, respond to potential security events and incidents. (…)
IT Department	- Provide IT support and expertise to the CSIRT (…)
(…)	
End Users	- Detect and report security incidents to the CSIRT (…)

Besides the presented roles, it may also include the Help Desk, Physical Security, DPO, Legal Department, Human Resources, etc.

3.1.3 Incident response life cycle

The incident response life cycle is one of the key components of an IRP. It describes the organisation's step-by-step framework for identifying and responding to a security incident or threat.

Two main industry-standard (NIST and SANS) frameworks provide a few steps to the incident response life cycle. Despite their differences, there are many similarities. It is up to the organisations to choose which of them best suits their needs. It is also important to highlight that, if neither of those is considered appropriate to the organisation's reality, they can be adjusted to meet the requirements.

The IRP should focus on all phases by describing its goals, steps, and tasks. It may also be interesting to include questions, a checklist, or a flow diagram to help the reader understand the phase actions entirely.

It is common to see the available interfaces for reporting incidents or threats on the Identification or Detection phase's description since the users need to know that they should report and where to do it.

Also, independently of the chosen incident response framework, there should always be a phase where the detected event or threat is considered a security incident. When that happens, it is typically addressed by some sort of incident classification to indicate its relevance. Each team has its own way of defining severities, but it is usually assigned to a scale value (e.g., Informational, Low, Medium, and High). This triage allows the CSIRT to prioritise the incident management and even change the incident's route if considered relevant.

3.1.4 Simple communication plan

When an incident response team is confronted with a potential security breach or data loss and the organisation's reputation or business is at stake, it can be overwhelming to the team because of all the technical issues related to the investigation, containment, or recovery.

The absence of a communication plan can lead to a situation where a CSIRT does not know whom to communicate with, when, and by what channel, possibly resulting in a security incident mishandling. This episode can jeopardise the organisation and possibly result in a non-compliance fine.

As a simple communication plan, the IRP should include the main stakeholders and their notification trigger. This usually comprises internal staff, regulators, law enforcement authorities, third parties, end-users/clients, among others. When possible, each stakeholder's contacts should be presented in the document or means to consult them should be provided. A simple table with the stakeholder category and its contact information should be sufficient.

3.2 Outlined

This domain corresponds to the intermediate stage of constructing an IRP, aiming to complete the IRP and give it a strategy of evolution and constant improvement. In this phase, the topics "Incident and Evaluation Metrics", "Service-level Agreements", "Plan Testing and Review" and "Incident Response Training" will be covered.

3.2.1 Incident and evaluation metrics

It is imperative to continuously monitor the incident handlers' tickets and interactions/actions during incident handling. The statistics collected through this monitoring provide insight into the CSIRT service's performance and the most recurring incidents, failures, or users. It is up to the organisation to define the metrics it intends to collect based on its objective. This measurement can be done manually or automatically.

3.2.2 Service-level Agreements (SLA)

An SLA is a contract between a service provider and the end-user that defines the provider's service level. Therefore, this section should include the CSIRT service activation criteria, the definition of expected response times, and the indication of the service hours.

By defining service activation criteria, the CSIRT can reduce the workload and thus guarantee the incident response's success. These criteria could be, for example, to only respond to SPAM incidents if they originated

from the organisation. The activation criteria, if used, can and should be adjusted as the CSIRT grows and the responsiveness increases.

Response times are usually associated with the level of criticality provided to the incident. The time set to notify or handle a high-rated incident should be much shorter than a low-rated incident. The service's workload usually varies between 8x5, 24x7, or mixed, but these are not standard. The availability of this information allows the user to know when they will be expected to receive the handling of an incident by the CSIRT.

3.2.3 Plan testing and review

Periodically reviewing and updating the plan's content is necessary to update, identify gaps, and maintain its applicability at any time. Also, testing the plan affects the document's content and helps incident handlers identify poorly executed steps and aspects that need improvement.

Testing should be carried out considering a minimum periodicity (usually annual). These tests should include practical simulations of real scenarios, and the team must ensure the fulfilment of the incident response process. It is essential that the team understands how important simulations are for the service's good performance.

3.2.4 Incident response training

It is difficult to maintain the ability to respond to incidents effectively over time without adequate and continuous training. As in the previous section, the training of incident response teams can be carried out through practical simulations. Another way is simply through continuous training, either internally or externally. The plan should include the perspectives and objectives of the CSIRT service in this context.

For stakeholders in this process, it may be pertinent to include awareness sessions so that they know what to report and how to deal with incidents to ensure a consistent and appropriate response.

3.3 Support

The Support domain corresponds to the last stage of building an IRP. The implementation and use of tools such as a taxonomy or classification matrix may not be in everyone's interest, despite accelerating and improving processes. In this phase, the topics "Taxonomy", "Classification Matrix", "Playbooks", "Communication Plan", and "Useful Templates" will be covered.

3.3.1 Taxonomy

The incident taxonomy is a classification scheme commonly used by CSIRT to better understand and categorise the security incidents in an organisation. It also allows the organisation to have a view on the trending of incidents and threats, and to better prepare/improve the incident response team performance. Creating a taxonomy is not a simple task, and therefore it is best to use an existing classification scheme. Since the organisation will probably be exchanging some information about their security incidents with other CSIRTs or regulators, it can be useful to determine if they use a shared taxonomy[1]. Table 4 presents an excerpt of an example.

Table 4: Excerpt of an example

Category	Type	Description
Malicious Code	Infected System	System infected with malware, e.g., PC, smartphone or server infected with a rootkit. Most often, this refers to a connection to a sinkholed C2 server.
	(…)	(…)
	Malware Distribution	URI used for malware distribution, e.g., a download URL included in fake invoice malware spam or exploit-kits (on websites).
Information Gathering	Sniffing	Observing and recording of network traffic (wiretapping).
	(…)	(…)

[1] E.g., in Europe there is the Reference Security Incident Taxonomy Working Group (RSIT WG) scheme.

3.3.2 Classification matrix

As seen in the incident response life cycle, assigning a severity value allows defining a prioritisation and incident handling strategy. The classification matrix introduces a simpler and faster way to assign a level of severity to incidents, which are often assessed inappropriately or inconsistently when doing this manually. This matrix determines a default severity value according to the type of incident in question. Being a default value, it can be adjusted if considered relevant. The IRP may also include the definition of criteria for this adjustment (e.g., in the event of an incident in a critical asset, the incident's criticality should rise). Table 5 presents an excerpt from an example classification matrix.

Table 5: Example of a classification matrix

Category	Type	Severity by default
Intrusions	Privileged Account Compromise	S1 (High)
	Unprivileged Account Compromise	S2 (Medium)
	Application Compromise	S1 (High)
	Burglary	S2 (Medium)
Vulnerable	Vulnerable system	S4 (Informational)
(…)		

In addition to the incident's criticality level, CSIRTs are recommended to use an information classification system in terms of sharing, the Traffic Light Protocol (TLP). Through a colour scheme (WHITE, GREEN, AMBER and RED), access to information is defined and limited, whether publicly, internally, to a limited group or only those involved.

3.3.3 Playbooks

Playbooks are operational procedures with practical guidelines for handling and resolving specific type/category incidents. The purpose of these documents is to guide the CSIRT and optimise and accelerate the entire process. Playbooks are often illustrated in checklists, diagrams, RACI[2] tables, among others. The chosen method should be the one that best serves the team members who will handle the incidents.

Usually, only a few playbooks are related to more critical incidents, including data breach, malware, or intrusions. However, the use of playbooks for all types of incidents may prove extremely useful for the team. Also, even within the same type of incident, it may still be pertinent to have different procedures according to the problem.

3.3.4 Communication plan

The implementation of a more detailed communication plan, in addition to the recommendations provided above, should consider three points: (i) Adapt communications to internal stakeholders and define preferred communication channels - Refers to the inclusion of entities such as management, DPO, IT department, among others. Triggers and means of contact should be defined to notify these entities, as well as what information to forward. (ii) Include practical cases that require a particular notification procedure - Situations such as data breaches may impose a different notification flow, possibly involving other entities. The definition of guidelines for these unique cases may be sorely missed in an emergency; (iii) Include notification to service providers - Providers whose service has been abused and third-party providers/services that may be useful in applying blocking measures and thus reducing the impact. It might be interesting to include some platform URLs or an indication of how to search for third party contacts (e.g., using WHOIS).

3.3.5 Useful templates

The primary purpose of templates is to assist and speed up some of the incident handlers/team's tasks. This section can include an incident form, a final incident report template, or even text scripts to use when there is a need to notify someone. In the latter case, templates should be prepared mainly for public communication (media statements) or third parties (abuse notification).

[2] Responsibility assignment matrix (Responsible, Accountable, Consulted, Informed).

4. Paths to implementation

The strategy presented includes a phased implementation model, and the application of this model may differ from entity to entity. There is no single path. Each organisation is different, and, therefore, it is necessary to assess its objectives, needs, and capabilities concerning the management of security incidents. Thus, the plan to implement should reflect the organisation's maturity in order not to be considered inadequate or have a careless or rare use. The model phases are executed sequentially, starting in the Essential domain, continuing to Outlined and ending in Support. The plan was made so that the entities can make their own path. An organisation can choose only to make a simple plan, namely in situations where investment in the incident response service is reduced or made in an ad-hoc approach by IT employees. On the other hand, an organisation that considers itself more mature may choose to perform the first two phases, either sequentially or at once. In the case of organisations already mature and consolidated, they will probably try to implement a complete IRP, going through all this model's domains.

The presented model's main utility is that, regardless of the phase in which an organisation is, it has a useful and ready-to-use plan, reducing the waiting time to start the services. Finally, although the Support domain corresponds to the third phase, it is important to mention that it can be started at any time after the first domain's consolidation. The implementation of the second phase is not mandatory, although recommended. It is also important to remember that, to achieve the plan's success, participation and support from the administration is compulsory, as well as the definition of measures to evaluate the service's success.

5. Conclusions and future work

As security threats and incidents rise, it surges a need for investing in monitoring and protecting information systems. In case of an incident, the response process must be assertive and quick to mitigate the impact and reduce costs to the organisation.

The development and use of a complete, practical, and straightforward IRP become essential for responding to security incidents. However, the implementation of such a document requires time, knowledge, and some effort to analyse the norms and frameworks. Even so, these standards, despite presenting the main ideas and including some tips, do not provide an implementation methodology.

Through the research and study of the documents of reference, related articles, and incident response plans of several organisations, it was developed a practical strategy for implementing an IRP that can be used to complement the existing standards and frameworks.

After consolidating the most important and referenced topics in the analysed documentation, a model was developed, divided into three domains: Essential, Outlined and Support. Each domain includes practical tips and examples of what and how to integrate each subject.

The adoption of the proposed model allows answering several essential questions in the process of creating an IRP that is effectively used and put into practice. These include questions such as "What is a security incident for the organisation?"; "Who are the stakeholders?"; "What is the response procedure?"; "To who communicate in a data breach incident?"; "Which of the incidents to give priority to?"; among others. Subjects that promote evaluation and progressive improvement for the process and team are also included.

The proposed strategy for implementing this plan may differ from organisation to organisation, as the model was designed to be adjustable to each one's reality. A plan with only the first domain of the consolidated model can already be considered a useful and applicable plan in several realities. If considered insufficient, the remaining domains should be explored. Through this strategy, the implementation of an IRP is phased and modular, allowing it to evolve according to organisations' needs.

The model and strategy presented in this work still need to be validated, at least in applying it to an organisation to measure its effectiveness. In this regard, it is recommended that future work will focus on the applicability of this model to different organisations and across multiple verticals, e.g., government, industry, and academia. Since this strategy or model may also not be adequate when using it against an organisation that outsources the security incident management services, it should be reviewed to increase the applicability coverage.

Acknowledgements

This work was supported by Portuguese national funds through the FCT - Foundation for Science and Technology, I.P., under the project UID/CEC/04524/2020.

References

Al-Dhaqm, A., Razak, S. A., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020). Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. *IEEE Access, 8*, 145018-145032. doi:10.1109/ACCESS.2020.3008696

Brownlee, N., & Guttman, E. (1998). *RFC2350: Expectations for Computer Security Incident Response.* USA: RFC Editor.

Criminal Justice Information Center. (2019). *Example Incident Response Plan.* Retrieved January 13, 2021, from State of Michigan: https://www.michigan.gov/documents/msp/Example_Incident_Response_Policy_666657_7.pdf

Empresa Brasileira de Serviços Hospitalares. (2018, July). *PGI – Plano de Gerenciamento de Incidentes do HU-UFJF.* Retrieved January 13, 2021, from Empresa Brasileira de Serviços Hospitalares - EBSERH: http://www2.ebserh.gov.br/documents/222346/866032/Plano+_Gerenciamento_Incidentes_ajustes_JUL_18.pdf/2e6d868a-39fa-4273-a889-7bcb2a3f3867

ENISA. (2010). *Good Practice Guide for Incident Management.* Publications Office.

International Organization for Standardization. (2016). *ISO/IEC 27035-2:2016: Information Security Incident Management.*

ISACA. (2012). Incident Management and Response.

IT Governance Institute. (2007). *CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models.* Rolling Meadows: IT Governance Institute.

JSM Marketing Services. (2017, November). *Incident Response Plan.* Retrieved January 13, 2021, from JSM Marketing: https://jsm-marketing.com/wp-content/uploads/2018/03/JSM_Incident-Response-Plan-2018.pdf

Mooi, R., & Botha, R. A. (2016). Context for the SA NREN Computer Security Incident Response Team. *2016 IST-Africa Week Conference*, (pp. 1-9). doi:10.1109/ISTAFRICA.2016.7530662

Onwubiko, C., & Ouazzane, K. (2020). SOTER: A Playbook for Cybersecurity Incident Management. *IEEE Transactions on Engineering Management*, 1-21. doi:10.1109/TEM.2020.2979832

OSCIO Enterprise Information Services. (2016). *Information Security Incident Response Plan (SAMPLE).* Retrieved January 13, 2021, from State of Oregon: https://www.oregon.gov/das/oscio/documents/incidentresponseplantemplate.pdf

Pessoa, João; EGPr-TIC. (2016). *Processo de Gerenciamento de Incidentes.* Retrieved January 13, 2021, from Tribunal Regional do Trabalho 13ª Região - Paraíba: https://www.trt13.jus.br/institucional/governanca/publicacoes/trt-13/setic/escritorio-de-processos/processo-de-gerenciamento-do-incidentes/Processo%20de%20Gerenciamento%20de%20Incidentes.pdf

PROCEMPA. (2020, August). *Plano de Resposta a Incidentes de Segurança e Privacidade.* Retrieved January 13, 2021, from Prefeitura de Porto Alegre: https://prefeitura.poa.br/sites/default/files/usu_doc/sites/procempa/Plano%20de%20Resposta%20a%20Incidentes.pdf

Proffitt, Timothy; SANS. (2007). Creating and Managing an Incident Response Team for a Large Company. *SANS.edu Graduate Student Research*.

Scarfone, K. A., Grance, T., & Masone, K. (2012). *SP 800-61 Rev. 2. Computer Security Incident Handling Guide.* Gaithersburg, MD, USA: National Institute of Standards & Technology.

Stinson Leonard Street, LLP. (2017, October). *Security Incident Response Plan [Sample].* Retrieved January 13, 2021, from Carolinas Credit Union League: https://www.carolinasleague.org/resource/collection/B728697E-626E-4B25-8C68-28A43CF6536F/3%20B%20Pirnie%20Handout%20Sample%20Incident%20Response%20Pl.pdf

Texas Southmost College. (2018). *IT Security Incident Response.* Retrieved January 13, 2021, from Texas Southmost College: http://archive.tsc.edu/images/helpdesk/TSC_-_IT_3.6_IT_Security_Incident_Response.pdf

Tulane University. (2020). *Computer Incident Response Plan.* Retrieved January 13, 2021, from Tulane University | Information Technology: https://it.tulane.edu/computer-incident-response-plan

Universidade Federal do Rio de Janeiro – UFRJ. (2018). *Plano de Gestão de Incidentes de Segurança da Informação.* Retrieved January 13, 2021, from Diretoria de Segurança da Informação e Governança - UFRJ: https://www.security.ufrj.br/wp-content/uploads/2019/02/Plano-de-gest%c3%a3o-de-incidentes-SegTIC.pdf

University Carnegie Mellon. (2020, September). *Computer Security Incident Response Plan.* Retrieved January 13, 2021, from University Carnegie Mellon: https://www.cmu.edu/iso/governance/procedures/IRPlan.html

University of Adelaide. (2018). *Data Breach Response Plan.* Retrieved January 13, 2021, from The University of Adelaide: https://www.adelaide.edu.au/policies/62/?dsn=policy.document;field=data;id=8225;m=view

University of Alabama. (2016). *IT Practice Procedure Security Incident Response Plan.* Retrieved December 18, 2020, from The University of Alabama: https://oit.ua.edu/services/security/report/

West-brown, M., Stikvoort, D., & Kossakowski, K.-P. (1999). Handbook for Computer Security Incident Response Teams (CSIRTs).

Western Oregon University. (2009). *Data Security Breach Incident Response Plan.* Retrieved January 13, 2021, from Western Oregon University: https://wou.edu/ucs/files/2015/11/WOU_Incident_Resp_Plan.pdf

Captain Carl Poole received a master's degree in space systems with specialties in space vehicle design and space control modelling and simulation from the Air Force Institute of Technology March 2021. His research topics include the examination of space-based ballistic missile defense architectures for employed kinetic weapon concepts.

Lucas Potter is a Biomedical Engineering PhD Student and member of the SAMPE
(Systems Analysis of Metabolic Physiology) Lab at Old Dominion University. His doctoral research is focused on cellular respiration in those with compromised metabolism. Past research endeavors include human factors research, specifically human factors analysis of performance in virtual reality, modeling of physiology, and materials engineering.

Seyedali Pourmoafi I have spent most of my time learning and build up my knowledge around Computer Science subject ever since I lay hands on my first self-build computer at my early childhood self-studying desire and researching on the internet led me to learn very fast in childhood. I am extremely curious about Astronomy and Computer science. I decided to study Mathematics in high school and Computer Science at the university. I had my first degree in Computer Science software engineering before I moved to the UK. Then I decided to start with an Undergraduate degree and choosing an entirely new degree and specialism which leads to being graduated in information technology with a Web specialism degree. Then after having a short discussion with a member of the faculty, I decided to follow the new direction by choosing M.Sc. in networking, now I am finishing up my Ph.D. study in Cybersecurity.

Jakub Pražák is a Ph.D. candidate of International Relations at the Charles University's Faculty of Social Studies and a project assistant at the Prague Security Studies Institute. His main research areas are weaponization of outer space and dual-use technology.

Carlos Rabadão is Coordinator Professor at Polytechnic Institute of Leiria. He received his PhD degree in Computer Engineering from University of Coimbra in 2007. He has published more than 50 papers at conference proceedings and refereed journals. His major research interests include Cybersecurity, Information Security Management Systems and Intrusion Detection Systems for IoT.

Jyri Rajamäki is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology, and a PhD in mathematical information technology from University of Jyväskylä.

Dr Trishana Ramluckan is the group research manager for Educor Holdings. In 2020 she completed post-doctoral research in International Cyber Law at the School of Law, UKZN. Her areas of research include the intersections of IT with law and governance. She is a member of the IFIP working group on ICT Uses in Peace and War and is an Academic Advocate for ISACA.

Dr Harri Ruoslahti is a Senior lecturer of Security and risk management at Laurea University of Applied Sciences, a researcher in related projects, and Laurea's point of contact in ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations).

Karo Saharinen (M.Eng) is working as a Senior Lecturer in IT and handling the responsibility of degree programme coordinator of the master's degree programme in IT, Cyber Security at JAMK University of Applied Sciences. He is currently working on his PhD related to Cyber Security Education.

Leonel Santos is Assistant Professor at Polytechnic Institute of Leiria. He received his PhD degree in Computer Science from University of Trás-os-Montes e Alto Douro in 2020 and is a researcher at Computer Science and Communication Research Centre. His major research interests include Cybersecurity, Information and Networks Security, IoT, Intrusion Detection Systems and Computer Forensics.

Janine Schmoldt studied International Relations at the University of Erfurt, Germany. Afterwards, she completed her Master at the Vrije Universiteit Amsterdam where she studied Law and Politics of International Security. She is currently a PhD student at the University of Erfurt.