



D6.6

Data breach management plan V(2)

DOCUMENT	D6.6	WORKPACKAGE	WP6
DELIVERABLE STATE	Final	PROGRAMME IDENTIFIER	H2020-SU-DS-2020
REVISION	V1.0	GRANT AGREEMENT ID	101020560
DELIVERY DATE	31/01/2024	PROJECT START DATE	01/10/2021
DISSEMINATION LEVEL	Public	DURATION	3 YEARS

© Copyright by the CyberSEAS Consortium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101020560



DISCLAIMER

This document does not represent the opinion of the European Commission, and the European Commission is not responsible for any use that might be made of its content.

This document may contain material, which is the copyright of certain CyberSEAS consortium parties, and may not be reproduced or copied without permission. All CyberSEAS consortium parties have agreed to full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the CyberSEAS consortium as a whole, nor a certain party of the CyberSEAS consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, and does not accept any liability for loss or damage suffered using this information.

ACKNOWLEDGEMENT

This document is a deliverable of CyberSEAS project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 101020560.

The opinions expressed in this document reflect only the author's view and in no way reflect the European Commission's opinions. The European Commission is not responsible for any use that may be made of the information it contains.

D6.6 Data breach management plan (V2)

PROJECT ACRONYM	CyberSEAS
PROJECT TITLE	Cyber Securing Energy dAta Services
CALL ID	H2020-SU-DS-2020
CALL NAME	Digital Security (H2020-SU-DS-2018-2019-2020) SU-DS04-2018-2020
TOPIC	Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches
TYPE OF ACTION	Innovation Action
COORDINATOR	ENGINEERING – INGEGNERIA INFORMATICA SPA (ENG) CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA (CINI), AIRBUS CYBERSECURITY GMBH (ACS), FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FRAUNHOFER), GUARDTIME OU (GT), IKERLAN S. COOP (IKE), INFORMATIKA INFORMACIJSKE STORITVE IN INZENIRING DD (INF), INSTITUT ZA KORPORATIVNE VARNOSTNE STUDIJE LJUBLJANA (ICS), RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN (RWTH), SOFTWARE IMAGINATION & VISION SRL (SIMAVI), SOFTWARE QUALITY SYSTEMS SA (SQS), STAM SRL (STAM), SYNELIXIS LYSEIS PLIROFORIKIS AUTOMATISMOU & TILEPIKOINONION ANONIMI ETAIRIA (SYN), WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE (WIN), ZIV APLICACIONES Y TECNOLOGIA SL (ZIV), COMUNE DI BERCHIDDA (BER), COMUNE DI BENETUTTI (BEN), ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA (ELES), PETROL SLOVENSKA ENERGETSKA DRUZBA DD LJUBLJANA (PET), AKADEMSKA RAZISKOVALNA MREZA SLOVENIJE (ARN), HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA DOO (HOPS), ENERIM OY (ENERIM), ELEKTRILEVI OU (ELV), COMPANIA NATIONALA DE TRANSPORT ALENERGIEI ELECTRICE TRANSELECTRICA SA (TEL), CENTRUL ROMAN AL ENERIEI (CRE), TIMELEX (TLX).
PRINCIPAL CONTRACTORS	
WORKPACKAGE	WP6
DELIVERABLE TYPE	Document, report
DISSEMINATION LEVEL	Public
DELIVERABLE STATE	FINAL
CONTRACTUAL DATE OF DELIVERY	31/01/2024
ACTUAL DATE OF DELIVERY	26/02/2024
DOCUMENT TITLE	Data breach management plan (v2)
AUTHOR(S)	ENERIM
REVIEWER(S)	WIN, RWTH
ABSTRACT	SEE EXECUTIVE SUMMARY
HISTORY	SEE DOCUMENT HISTORY
KEYWORDS	Data breach, Response plan

Document History

Version	Date	Contributor(s)	Description
V0.1	31/01/2024	ENERIM, GT, SYN, WIN, FRAUNHOFER	First draft – table of content and contributions to the content
V0.2	31/01/2024	ENERIM	Review version
V0.3	23/02/2024	PETROL, ENERIM	Final version. Review comments addressed. Added Slovenian data breach case 2. Updated document template to V2.
V1.0	26/02/2024	ENG	Final approval by coordinator

Table of Changes in Version 2

Section	Contributor	Change description and motivation
Chapter 1	ENERIM	Updated chapter to reflect version 2.
3.1.3.7	PETROL	Added new Slovenian incident case study.
4.1.2	PETROL	Added lessons learned from the new incident case study.
Chapter 5	ENERIM	New chapter discussing the model developed in Task 6.3.

Table of Contents

Document History	4
Table of Contents	6
List of Figures	8
List of Acronyms and Abbreviations	9
Executive Summary (Updated)	10
1 Introduction (Updated)	11
1.1 Objective of the report	11
1.2 Connection with other Tasks	11
1.3 Structure of the document	12
2 Background knowledge	13
2.1 Data breach	13
2.2 Existing Data breach management frameworks	13
2.2.1 Recommendations by the National Cyber Security Centre Finland	14
2.2.2 Recommendations by the German Federal Office for Information Security	17
2.2.3 Recommendations by the Hellenic Data Protection Authority	22
2.2.4 Recommendations by the Italian National Framework for Cybersecurity and Data Protection	26
2.3 Electric Power and Energy System Overview	30
3 Recent studies and documents on data breaches	33
3.1 Data breaches events on each country	33
3.1.1 Finland	33
3.1.2 Estonia	37
3.1.3 Slovenia	39
3.1.4 Italy	42
3.1.5 Greece	44
3.1.6 Germany	47
3.1.7 Croatia	52
4 Guidelines for data breach management plan	54
4.1.1 Comparison of the existing frameworks	54
4.1.2 Best and worst practices of recent data breach incidents (Updated)	56
5 Common Model for data breach management (NEW)	58
5.1 Description of Common Model and steps	59

D6.6 Data breach management plan (V2)

5.1.1	Preparation.....	59
5.1.2	Detection.....	60
5.1.3	Response.....	61
5.1.4	Recovery.....	62
5.1.5	Review.....	62
5.2	Practical example	63
5.2.1	Demonstration – Background.....	63
5.2.2	Demonstration – Preparation.....	64
5.2.3	Demonstration – Detection.....	66
5.2.4	Demonstration – Response.....	69
5.2.5	Demonstration – Recovery.....	70
5.2.6	Demonstration – Review.....	71
6	Conclusions (Updated)	73
7	References	74

List of Figures

Figure 1 Five main steps of data breach management by the Finnish national authority.....	14
Figure 2 BSI printable card for supporting employees during data breach events.....	18
Figure 3 Combined procedure for data breach management.....	55
Figure 4 A Common model of data breach management describing steps.....	59
Figure 5 Different assets created in the CVIAT.....	65
Figure 6 Assets dashboard depicting different levels of threats.....	65
Figure 7 Initial threat assessments for database and human factors.....	66
Figure 8 Re-evaluation of threat level.....	66
Figure 9 MIDA tool implementation to CIS platform.....	67
Figure 10 Example of validation results with OK results.....	68
Figure 11 Example of validation results with failure and errors.....	69
Figure 12 Response step.....	70

List of Acronyms and Abbreviations

AI	Artificial Intelligence
ARNES	Academic and Research Network of Slovenia
CER	Critical Entities Resilience
CERT	Computer Emergency Response Team
DPA	Data Protection Authority
EPES	Electric Power and Energy System
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
GSE	Gestore dei Servizi Energetici
ISMS	Information Security Management System
NIST	National Institute of Standards and Technology
NCSC-FI	National Cyber Security Centre Finland
RIKU	The Victim Support Finland
SI-CERT	Slovenian Computer Emergency Response Team
WP	Work Package

Executive Summary (Updated)

This document is an updated deliverable reporting contributions made under Task 3 in work package (WP) 6 of project CyberSEAS. The document encompasses the following content:

- 1)** Data breach management frameworks are briefly reviewed in the report where the recommendations and instructions provided by national authorities in different countries including Finland, Germany, Greece and Italy are provided. According to the instructions, management procedure of a data breach incident can be divided into a few major steps such as preparation, detection, containment, recovery and post-incident review. The report briefly reviews the main measures and activities during the steps.
- 2)** Recent data breach incidents in different European countries are reviewed. The focus is on incidents in the energy supply chain. In case we'd find no major incidents in the domain that are applicable, incidents in other main infrastructures or other major incidents are reviewed. The aim of the review is to extract best and worst practices as well as to explain the lessons learned from the incidents.
- 3)** Comparing the data gathered from the incidents and the relevant lessons learned during the studies, a list of recommendations about how to manage data breach incidents is provided.
- 4)** A Common model for data breach management is provided by combining existing frameworks into 5 discrete steps describing actions required to prepare, and to react to a data breach event. These steps are in order: preparation, detection, response, recovery, and review. Finally, a practical example of these steps are described by a demonstration done in the Finnish pilot, in which a data breach incident is simulated.

This report is the revised version of the deliverable in Task 6.3. The first version of the deliverable is the foundation of this report.

1 Introduction (Updated)

1.1 Objective of the report

The overall planning of the CyberSEAS project is depicted in the following figure. As can be seen, WP6 in the project focuses on cyber security of energy common data spaces. In the work package, there are four tasks namely cybersecurity governance for electric power and energy system (EPES) operators and other stakeholders, secure and privacy preserving data exchange among operators, orchestrated management of data breaches among supply chain operators and rules & tools for operators' coordination and reporting to computer emergency response team (CERTs) in case of incidents. The current report is dedicated to the third task which is the orchestrated management of data breaches among supply chain operators. As the title implies, the focus of the task, and thus this report, is on data breach management. To take steps in that direction, this report gathers and studies recent data breach events in energy supply chain in different European countries. In case of no major data breach event in energy supply chain in a country, other major data breach events preferably in critical infrastructures in the country are considered. The existing data breach management frameworks are studied, which provide a common framework for data breach management.

In summary, the main objectives of this report are listed below:

- Gather existing data breach management frameworks
- Gather and study recent data breach events in energy supply chain in different European countries
- List the best and worst practices from the studied data breach events and how they are managed
- Provide a common model for data breach management using 5 steps: preparation, detection, response, recovery, and review.

1.2 Connection with other Tasks

This report is a deliverable of Task 6.3. The task is highly connected to activities and studies in the other tasks in the work package. The connections are briefly described here:

- Task 6.1 focuses on cybersecurity governance of energy common data spaces. In that task, guidelines about cybersecurity governance models are developed. The governance models are general policies to ensure cybersecurity of energy common data spaces. They cover different aspects of cybersecurity and variety of actions and measures including but not limited to data breach incidents. The authors assume that the current report provides inputs to Task 6.1 where some of the guidelines and policies are allocated to data breach management.

- Task 6.2 focuses on secure and privacy preserving data exchange among operators. It is clear that managing data breach incidents in energy common data spaces require secure and privacy preserved data exchange among different players. Therefore, the authors assume that this task (i.e., Task 6.3) provides input to Task 6.2 about potential data exchanges among different players in case a data breach event occurs.
- Task 6.4 focuses on rules & tools for operators' coordination and reporting to CERTs in case on incidents. That task provides a general playbook for operators' coordination and reporting to CERTs that can handle different cyber incidents. This means that the rules in the playbook covers operators' coordination and reporting to CERTs in case of data breach incidents. So, the authors assume this task and Task 6.4 will crosspollinate each other regarding the coordination and reporting of data breach events.

1.3 Structure of the document

The rest of the report is structured in four chapters:

- Chapter 2 provides background knowledge and definitions of terms required by readers to better understand contributions and technical content of the report. The chapter contains three sections. The first section reviews different levels, players and their roles in electric power and energy system. The second section defines a data breach event. The third section reviews existing data breach management frameworks such as the recommendations and instructions made by the National Cyber Security Centre Finland to name one.
- Chapter 3 reviews different data breach incidents that have happened in different European countries in recent years. Then, the lessons learned from the incidents and how they are managed are reviewed. This review leads to a set of recommendations about the best and worst practices in managing data breach incidents.
- Chapter 4 uses the information gathered in the previous chapters and takes benefit from the studies to develop a set of guidelines for data breach management plan. The guideline helps organizations to manage potential data breach incidents in a more efficient fashion.
- Chapter 5 provides a common model for data breach management which focuses on shared knowledge and provide practical support to EPES operators.
- Chapter 6 concludes the report by highlighting the most important and relevant findings and observations.

2 Background knowledge

2.1 Data breach

An event that leads to information taken from a system without the authorization of the system owner is called data breach. In the context of CyberSEAS project, smaller or larger companies playing role in the energy supply chain may suffer a data breach event. In the event, the stolen data can be any kind of sensitive or confidential information including but not limited to consumers personal data, consumption/production data, contracts between the company and customers, end users' personal data, technical data of energy infrastructures and financial data.

A data breach event can lead to significant damage to the target company including damage to the company reputation, financial losses, and loss of customers to name a few. A data breach event can be due to hacking attacks, malware attacks, insider leak, loss or theft and unintentional disclosure.

Companies in the energy supply chain operate with a combination of human processes, technical systems, and communication networks. A typical activity of the attacker is to find a weakness in either of these: human (employees in case of companies), the system or the network. Having the weakness found, the attacker initiates an attack to the identified weakness. The attack can be done in a variety of different ways including, but not limited to, social attacks like sending phishing emails and emails with a malware attachment to name a couple. Once the attacker gains access to data, it can potentially be used for executing more damaging attacks or blackmail.

Let's consider an example of a data breach event in the energy supply chain: in December 2020, a data breach happened at People's Energy, which is Edinburgh electricity supplier. In this event, customer data was compromised. The compromised data was mainly customer personal information including names, addresses, phone numbers, email addresses, dates of birth, energy account numbers, tariff details and meter identification numbers. The number of affected customers in the event was 270000.

2.2 Existing Data breach management frameworks

In this section, information and references of the existing data breach management best practices, models and frameworks are explained.

2.2.1 Recommendations by the National Cyber Security Centre Finland

The National Cyber Security Centre Finland of the Finnish Transport and Communications Agency TRAFICOM published a report containing instructions for data breach. The purpose of the instructions is to give advice to organizations about how to manage data breach incidents. It is indicated that the instructions offer general guidance and recommended organizations to develop a more detailed incident response plan according to their technological and operational environment.

According to the instructions, data breach management can be done in five main steps namely preparation, detection, containment, recovery and post-incident review as depicted in the following figure.

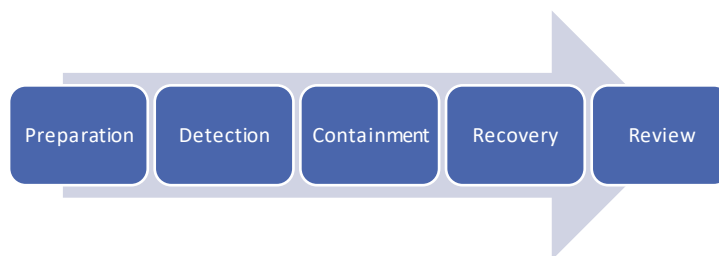


Figure 1 Five main steps of data breach management by the Finnish national authority

In the preparation step, the aim is to better protect against incidents, reduce the severity of incidents and enable a fast recovery after an incident. In this step, organizations are recommended to assess their readiness using cyber security evaluation tools and develop their incident response plan. In order for organizations to be well prepared, different measures are proposed, divided into administrative measures and technical measures.

A diverse set of administrative measures can be taken into use including, but not limited to, the following:

- Development of an organization incident response plan
- Training personnel
- Monitoring the news provided by the National Cyber Security Centre Finland to be aware of emerging risks and threats
- Being familiar with the procedure for reporting incidents to the National Cyber Security Centre Finland
- Reviewing attack scenarios and devising practical measures and responsible authorities for handling them
- Practicing attack scenarios regularly
- Implementing continuous vulnerability and update management
- Identifying the components critical to the business in order to better protect them
- Granting access rights according to the needs of the users
- Establishing a responsible body inside the organization to monitor the network traffic of the organization and security events in the systems

D6.6 Data breach management plan (V2)

In addition to the above administrative measures, the following technical measures can be taken into account:

- Conducting regular and automatic backups of any critical system data in the organization
- Conducting regular testing of the functioning of the backups
- Implement security measures including but not limited to network segmentation, data encryption and access control
- Investigating suspicious activities and monitoring critical processes to detect likely attacks as early as possible
- Ensuring security of terminal devices for instance by installing anti-malware software or isolating them from the public network if possible
- Protecting against suspicious emails with harmful content
- Enabling detection and investigation of cyber threats via implementing centralized log management tools

All the above measures are recommended to be implemented by the organizations during the normal situation when there is no ongoing cyber incident. The measures aim at either protecting against cyber incidents to happen, mitigating their consequences or facilitating their detection and management.

After all the above measures are applied in the preparation step, the next step is to ensure that the organization is able to detect cyber security incidents. There is a diverse range of approaches to detect an attack since there are many ways an attacker can use to penetrate to a system. Without loss of generality, the following list provides some general ways to detect an attack. The following is a non exhaustive list of signs or evidence of a past or ongoing attack:

- A system or part of a system stops working.
- An unexpected process is observed.
- An alarm is observed.
- Notification about the attack is received from the attacker.
- Notification about the attack is received from customers, partners, etc.
- A penetration to the system is discovered while a recently found bug or vulnerability is being addressed.

It is worthwhile to mention that the National Cyber Security Centre Finland recommended organizations to report data breach incidents to them as soon as the incident is detected. This is to support the national information security situation awareness as well as to help and warn other potential victims. The National Cyber Security Centre Finland also provides confidential and free of charge advice on how to limit the damage, assess the incident and take recovery measures.

Once a data breach event is detected, containment step begins. During this step, the aim is to investigate the incident. The National Cyber Security Centre Finland provided a workflow for investigating a data breach event. Among other things, it recommends to keep a precise

D6.6 Data breach management plan (V2)

event log of all taken measures with information about the party that implemented the measure and a timestamp. During this step, documentation is crucial. It is recommended to document any potential evidence with detailed information about the body that gathered the data, what the data was and when and how the data was gathered. The documents and logs facilitate the investigation as well as cooperation with police and information security investigators.

In the containment step, some immediate measures are necessary to protect the critical data in the environment, stop the malware from spreading, prevent the attackers from gaining a foothold in the network and prepare for the next step which is recovery. The immediate measures are listed as follows:

- To stop the attack from progressing, any infected device must be isolated.
- If the organization uses outsourced IT services, the IT service provider should be contacted to limit the scope of the incident.
- To limit the consequences of the incident, partners in cooperation and interest groups that may be affected by the incident should be notified about the incident.
- If the required expertise for handling the incident is not available within the organization or from the IT service provided, getting external support is recommended.
- If there is the risk that any personal data is compromised, the incident should be reported to the Data Protection Ombudsman without undue delay.
- If there is any obligation to report the incident based on regulations or the terms of the cyber assurance, reporting the incident to the relevant authorities should be done.

In addition to the above immediate measures, identification information is collected and used to determine the extent of the attack and its impact on the organization. In addition, the actions are necessary to ensure that potential malware and backdoors are removed. Identification information includes but is not limited to the time when the incident occurred, when a login to the server occurred and when a certain command was run on the server. Collecting identification information helps to identify harmful activities and thus ensure that all infected devices and identifiers are found and cleaned.

Once the environment is cleaned, the next step which is recovery can be started. The recovery step begins from the systems which are the most critical to the business. In this step, infected systems are restored from backups. It is worthwhile to mention that the process should be done as safely as possible to ensure that the attacker cannot get back into the system. In addition, login information of all of the potentially infected IDs is changed so that the attacker can no longer use the IDs to access the systems. In order to avoid similar attacks in the future, it is recommended to make user login requirements stricter. Once the systems are restored and the IDs are changed, database can be restored from a backup copy to invalidate potential changes made by the attackers.

Finally, when the incident is over and the business is returned to normal, it is recommended to review the attack. This review can be used to update the organization incident response plan to ensure that the organization is protected against a similar incident. In this step, the

measures taken during the event are studied to see how the plans and the security level can be improved. In the study, root causes of the incident and effectiveness of the organization protection plan are examined carefully. The National Cyber Security Centre Finland recommends organizations to share their most important lessons learned from incidents to help other organizations too.

2.2.2 Recommendations by the German Federal Office for Information Security

The German Federal Office for Information Security (abbreviated BSI, for German: "Bundesamt für Sicherheit in der Informationstechnik") provides a large variety of general information and recommendations on their website. These range from high-level one-page recommendations to detailed guidelines and standards covering hundreds of pages. In the following, we present the high-level checklists for guidance in IT-emergencies, followed by a brief overview of available BSI Standards for preventive measures.

2.2.2.1 Checklists for guidance during an IT-emergency

The BSI provides two checklists on their website to guide organizations in the response to IT-security incidents, which can in part be executed simultaneously. The first checklist focuses on organizational measures, while the second one provides guidance in technical aspects. In the following, we summarize the key information in these two checklists. These checklists are not meant to replace an incident response plan. To ensure wide applicability of the checklists, the individual points are kept generic. The BSI points out that the checklists were primarily designed to guide small and mid-sized enterprises in responding to IT-emergencies under the assumption that the respective organization has neither extensively prepared nor taken advanced preventative measures to address IT-emergencies, but that individual parts of the checklists are applicable for everyone.

Organizational Checklist

The organizational checklist is available online under the following URL:

[BSI - Company - Company: Managing an incident, reporting, informing yourself, preventing it \(bund.de\)](https://www.bund.de/.../BSI-Company-Company:Managing_an_incident,_reporting,_informing_yourself,_preventing_it_(bund.de))

Since no English version is provided, we have summarized and translated the most important points:

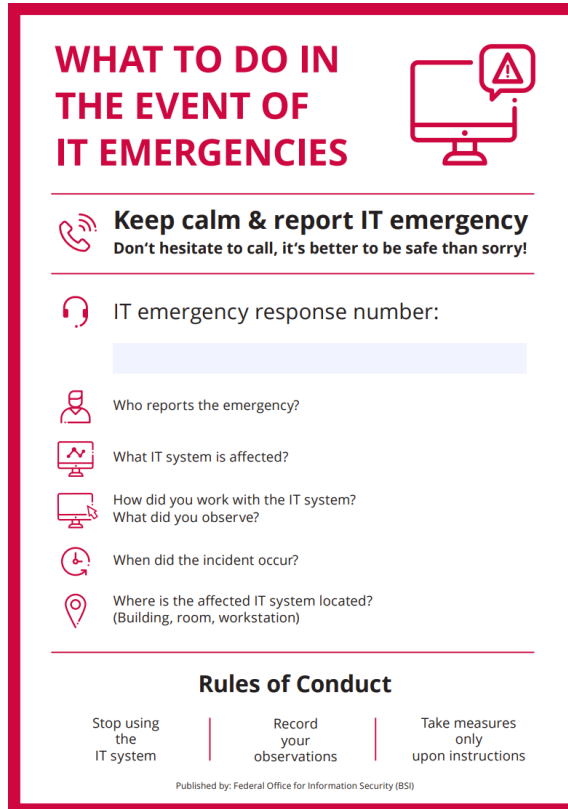
- Keep calm, do not act overhastily.
- Inform all relevant people in the organization, who are supposed to know about the incident. Explicitly but not exclusively, the IT-Security Officer, the Data Protection Officer, the IT-Department, the company management are named. Additionally, the BSI provides printable cards with the most important points for every employee to

D6.6 Data breach management plan (V2)

know. PDF versions of these cards are available for download in different languages (incl. English) under the following URL:

<https://www.allianz-fuer-cybersicherheit.de/dok/13035680>

The card is depicted in the following figure:



WHAT TO DO IN THE EVENT OF IT EMERGENCIES

Keep calm & report IT emergency
Don't hesitate to call, it's better to be safe than sorry!

IT emergency response number:

Who reports the emergency?

What IT system is affected?

How did you work with the IT system?
What did you observe?

When did the incident occur?

Where is the affected IT system located?
(Building, room, workstation)

Rules of Conduct

Stop using the IT system	Record your observations	Take measures only upon instructions
--------------------------	--------------------------	--------------------------------------

Published by: Federal Office for Information Security (BSI)

Figure 2 BSI printable card for supporting employees during data breach events

- Setup of a crisis committee and distribute roles and responsibilities. This includes the agreement of who is supposed to make relevant decisions and which actions should be carried out by whom until which point in time.
- Collect as much information as fast as you can to make informed decisions. Important points are what happened, how the incident was detected, which effects the incident can have on the organization and its services, which effects it may have on third parties or the general public, and whether the attack was targeted.
- If not done before, assign the responsibility of a Communication Manager to provide and receive information in a coordinated fashion. This also includes informing the employees of the organization, and checking to whom the incident must or should be reported. This is sensitive to local law, and for example includes reporting data breaches to data protection authorities. For organizations providing or working with critical infrastructures, additional reporting duties may apply. Further, there may be contractual obligations to report to business partners and customers. Even if not legally required, it could be considered to inform customers and the public, to report the incident (possibly anonymously) to respective government initiatives, and to report the incident to law enforcement agencies.

D6.6 Data breach management plan (V2)

- Check whether external help is required, and possibly where to find it. The BSI provides various lists of certified IT-security service providers to guide in finding suitable contacts. Under certain circumstances, the BSI might also provide guidance directly.
- After mitigating the effects of the incident, the lessons learned from the incident should be documented and used to prepare for future attacks.

Technical Checklist

Similar to the organizational checklist, the technical checklist is available online:

[BSI - Unternehmen - Unternehmen: Einen Vorfall bewältigen, melden, sich informieren, vorbeugen \(bund.de\)](https://www.bund.de/bsi/unternehmen/unternehmen-einen-vorfall-bewaeltigen-melden-sich-informieren-vorbeugen)

Since again only a German version is available, we summarized the most important points in English:

- Prevent any logins from accounts with advanced privileges to systems which have potentially been affected by the attack. Further, check whether some existing user accounts might have unnecessary privileges, and whether there has been an unauthorized elevation of account privileges in the recent past.
- Ensure to use complete and up-to-date information about your network. Identify the affected system(s) and do not only limit yourself to obvious systems. Consider that the adversary might have access to other systems, which might wait for further orders. In general, it should be assumed that all local systems were fully compromised. This includes all login data submitted to the system after the infection. In case that the Active Directory was compromised, the whole network should be considered as compromised. For isolating the affected system(s), the following steps are recommended:
 - Unplug the network cable.
 - Do not switch off the devices, if you intend to perform a technical analysis.
 - Perform a forensic investigation including the creation of a disk image, if a criminal prosecution is intended. This step could also be executed by an external IT-security service provider or law enforcement agencies.
 - Anti-virus software should only be used after the previous points have been completed. The reason for this is that such software might alter both random access and persistent memory, which in turn might impede forensic investigation efforts.
- If network monitoring and logging was not active to a sufficient degree, it should be enabled to capture ongoing attacks and/or data flows. This step should be done in coordination with the organization's Data Protection Officer and possibly the Betriebsrat (i.e., works council). The BSI suggests the following steps:
 - Activate Full-Packet-Capturing in the network. Communication between compromised internal systems and local command and control servers can be detected via the mirror port at internal, central network switches. The transition

from LAN to WAN might further reveal external command and control servers. To comprehend anomalies reported by externals, logging at firewalls is suggested.

- Set up a dedicated protocol server. Ideally, these should be operated externally to the productive/office network in “Promiscuous” mode. It should be considered that adversaries commonly take actions to corrupt logs or to prevent logging all together.
- Block all identifiable points of entry for the adversary.
- Check, whether you have clean and up-to-date backups. These backups should ideally be stored offline, since online-backups may be compromised coincidentally or intentionally. It may also be possible to find uncompromised copies of important files at branch offices, or on machines of employees who were on holidays while the attack occurred.

2.2.2.2 BSI standards

While the above mentioned checklists aim to provide general and quickly applicable guidance during an IT-emergency without assuming advanced security infrastructure in place, the BSI also provides standards which describe how to properly prepare for IT-emergencies. These standards provide significantly more details, and build on each other. In contrast to the checklists, most of them are available in both German and English languages.

The BSI provides four standards with methods, processes, procedures, approaches, and measures for different aspects of information security. They are an essential part of the “IT-Grundschutz” (IT base protection) methodology developed by the BSI, which is targeted at government agencies, companies, manufacturers, and service providers. In the following, a brief overview of the four standards is given.

BSI-Standard 200-1: Information Security Management System (ISMS)

This standard describes general methods for designing a basic information security management system (ISMS), which provides the means necessary to aid the management level of an organization in achieving a suitable level of information security. Among other topics, the standard addresses ways to manage and monitor security processes, and how to maintain the achieved level of security in the long run. It further deals with the questions of how to design suitable security objectives and strategies, how to select security safeguards, and which success factors to consider in the area of information security. It is applicable in a wide range of different environments by explicitly including computing components such as Industrial Control Systems and Internet-of-Things devices in its definition of an “IT system”. The standard is hence not restricted to office environments.

The BSI-Standard 200-1 is available in both German and English languages, and should be considered as the starting point when beginning to study the BSI standards. It is compatible

with the ISO 27001 standard and considers recommendations of other ISO standards such as ISO 27002.

The standard can be accessed through the following link:

<https://www.bsi.bund.de/dok/10027834>

BSI-Standard 200-2: “IT-Grundschutz” Methodology

Building on the BSI-Standard 200-1, which mainly considers management and design aspects, the BSI-Standard 200-2 focuses on the deployment of such an ISMS in an organization. It considers cost-effectiveness as one of its main goals, and is split into three sub-methodologies aiming at different levels of protection: The “Basic Protection” approach is aimed at ISMS beginners, but only provides limited protection. The “Standard Protection” approach aims to provide an adequate level of protection in most business environments. The “Core Protection” approach exceeds the level of protection provided by the “Standard Protection” and is intended for information and business processes, which require a higher level of protection.

The BSI-Standard 200-2 is available in both German and English languages, and should be seen as the core of the “IT-Grundschutz” methodology. It assumes that the reader is familiar with the content of BSI-Standard 200-1.

The standard can be accessed through the following link:

<https://www.bsi.bund.de/dok/10027846>

BSI-Standard 200-3: Risk Analysis based on “IT-Grundschutz”

The BSI-Standard 200-3 provides a risk analysis procedure, which consists of four steps. The first step is the identification of potential threats. In the second step, the identified risks are classified by assessing their frequency and associated damage, and by mapping risks to risk categories. As part of the third step, risk treatment is addressed by considering aspects of risk avoidance, risk reduction, risk transfer and risk acceptance. In the last step, additional safeguards identified as part of the previous steps are integrated into the security concept. This risk analysis procedure is compatible with the BSI-Standard 200-2. However, if there are special requirements or conditions for the system, the BSI suggests to consider the use of alternatives such as an adapted version of their methodology or other established risk analysis methodologies.

The BSI-Standard 200-3 is available in both German and English languages.

The standard can be accessed through the following link:

<https://www.bsi.bund.de/dok/10027822>

BSI-Standard 100-4: Emergency Management

This standard covers procedures for managing IT-emergencies to ensure business continuity. It provides guidance for establishing an IT-emergency management process in an organization, covering its initiation, drafting, and realization, as well as recommendations on emergency and crisis management, suggestions for tests and training programs, and measures for continuous improvements of the emergency management process. The standard further includes aspects to consider in regard to outsourcing and tool-assisted emergency management.

The BSI-Standard 100-4 will be replaced by the BSI-Standard 200-4 (Business Continuity Management) in the future. As of the writing of this deliverable, there is only a community draft of the future BSI-Standard 200-4 available. Both BSI-Standard 100-4 and the community draft of BSI-Standard 200-4 are only available in German language. The BSI-Standard 100-4 assumes that the reader is familiar with the BSI-Standard 200-2.

The standard can be accessed through the following link:

<https://www.bsi.bund.de/dok/6782544>

2.2.3 Recommendations by the Hellenic Data Protection Authority

The Hellenic Data Protection Authority (HDPa) is an independent public authority that was established in 1997 and is concerned with the protection of individuals with regard to the processing of personal data and on the free movement of such data. HDPa is responsible for supervising the implementation of the General Data Protection Regulation (GDPR), Greek Laws and other regulations concerning the protection of the individual from the processing of personal data.

HDPa provides useful information about security measures in its website. These measures are divided in two categories: organizational and technical. In the following, the most important action points are presented¹.

2.2.3.1 Organizational measures

The organizational measures proposed by HDPa are available in Greek under the following URL:

https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/organotika_metra

The most important points are provided in the following:

- Designation of Security Officer: A distinct safety officer position must be defined within the organization with clearly defined responsibilities. The security officer must, at a

¹ Source: <https://www.dpa.gr/en>

D6.6 Data breach management plan (V2)

minimum, supervise and control the implementation of the security policy and security measures. It is pointed out that this role should not be related to the Data Protection Officer of the organization and, in fact, these two roles are considered to be incompatible.

- Authorizations: Organizational roles must be created for specific tasks within the organization. There must be a clear separation and assignment of duties/responsibilities to each employee, based on their role. Roles must be formally assigned. Employees must have the right to access only strictly necessary personal data, based on the responsibilities and duties assigned to them. There must be a process for the periodic review and revision of authorizations and access rights. In case of a member of staff leaving, the following measures should be taken:
 - Remove access accounts, authorizations and passwords.
 - Removing email accounts and not assigning them to another employee (not reusing them).
 - Return of any equipment provided to the employee and belonging to the organization (including computers, keys, electronic entry cards, etc.).
- Security measures concerning information processing: The employee who processes data must take the appropriate organizational and technical measures for the safe keeping and processing of personal data. Additionally, he should write an appropriate confidentiality statement.
- Data destruction procedures: Before destroying paper or electronic files containing personal data, appropriate measures should be taken to ensure the complete and permanent deletion of such data.
- Management of personal data breach incidents: The organization must have procedures for the identification, reporting, notification and immediate response to incidents of personal data security breaches within the processing system used. These procedures must include the actions necessary to investigate each incident – how to report an incident, personnel to be activated, system files to be investigated, what the incident management file will contain, etc. There should be a record of each incident in a relevant file, which will include the time it occurred, the person who reported it and to whom it was reported, assessment of the consequences and criticality of the incident, recovery/correction procedures followed, notification to the authority as well as a possible process of informing the affected people depending on the extent of the incident and its consequences for the affected people.
- Disaster recovery plan: The Disaster Recovery Plan is a document that refers to the protection, recovery and restoration measures of information systems and technological infrastructure in emergency situations, such as natural disasters, external attacks/intrusions, etc. This plan is necessary to capture the procedures and technical measures that the organization must implement to protect personal data in case of an emergency, such as natural disasters (e.g. earthquake, fire, flood) or large-scale security incidents (e.g. malware damage). As such, it complements the security plan and it is part of the wider emergency plan that an organization may have in place.

D6.6 Data breach management plan (V2)

The organization should have alternative facilities and equipment, within the framework of the disaster recovery plan, in order to maintain its operational function in case of an emergency. Additionally, this plan should be reviewed periodically to determine the effectiveness of the recovery methods. Controls must cover the entire scope, processes and data of the systems. The disaster recovery plan should include measures for the following:

- Minimize interruptions to the normal operation of systems,
- Limiting the extent of damages and disasters and avoiding their possible escalation,
- Ability to smoothly degrade,
- Training, practice and familiarization of human resources with emergency procedures,
- Ability to quickly and smoothly restore operation,
- Minimize the economic impact.

This plan must identify the possible risks and, more generally, the criteria that define the situation as extreme and force its activation. There must be clear and written procedures that place the operator in an emergency situation and allow for withdrawal of the plan.

- Personnel training: Personnel training in data protection, as well as in special security-related functions of the information system (e.g. use of strong passwords, how to identify and report security breaches, correct use of e-mails and removable storage devices) is particularly important for the correct implementation of organizational and technical security measures. On-boarding training should include, as a minimum, communication to employees of the security policy, which should be fully understood by all, as well as data breach incident management and disaster recovery procedures, if they fall within their responsibilities. Additionally, specialized training on technological developments in the field of information security should be provided to the personnel in charge of safety management.
- Protection of portable storage devices: Appropriate measures must be taken to physically secure and protect portable storage devices, such as storing them in secure locations when not in use and being supervised at all times during use.

2.2.3.2 Technical measures

The technical measures proposed by the HDPA are available in Greek under the following URL:

https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/asfaleia/asfaleiaepexergasias/tekmiriwsh_asfaleia_proswpikwn/metra_asgaleia_proswpikwn/teknika_metra

The most important points are provided in the following:

- Backups: The organization must develop a specific policy for taking and managing backups. At a minimum, the policy should include the rules/procedures for: the selection of critical resources (applications, operating systems, files, user file data, etc.)

D6.6 Data breach management plan (V2)

that need to be backed up, the frequency of creating/retrieving backups (regularly, daily or weekly, depending on the size and type of data, as well as when it changes), properly labeling them, storing them securely and properly recovering data from the backups (including periodically checking the integrity/reliability of the copies received). The above must ensure that in the event of security emergencies and loss or destruction of data for another reason (e.g. hardware failure), their availability and integrity remains. Any backup must be kept in a different space/physical location from the primary data, which has security measures commensurate with the measures adopted for the primary data. Also, measures should be taken for its safe transport.

- **Computer configuration:** All computers (both personal computers and servers) that hold or process personal data must be protected from malware. This can be achieved (in addition to the correct use by employees) with anti-virus programs, as well as with the use of firewall programs. Both the antivirus and the firewall must have the latest updates available at all times. In addition, computers (as long as they are connected to the internet) must have security updates installed on their operating system at regular intervals.

Periodic checks of installed software should be performed to detect any programs that have been installed outside of approved procedures.

If a computer is used as a server, then it should not be able to be used as a workstation by a user.

Computers used by end users must not be capable of extracting data using removable media (e.g. USB, CD/DVD) unless approved by the Security Officer (or other form of approval, through a process provided in the security policy).

No personal data should be stored on computers connected to the internet (unless it is absolutely necessary in the context of the role/responsibilities assigned to the user of the computer).

- **Log files:** In critical systems, there should be procedures for maintaining and controlling log files of all users' actions, including the actions of system administrators, as well as security events. The protection and integrity of these files must be ensured.

These files may be accessed by the security officer, system administrators and any other staff members charged with security incident management responsibilities upon written authorization.

It should be ensured that the followings are absolutely kept in the action log files, at a minimum: the identifier of the user who requested access to personal data, the date and time of the relevant request, the system through which access was requested (computer, software program, etc.), as well as whether it ultimately accessed the files it requested. Requests to print files with personal data must also be recorded, as well as changes to critical system files or user rights.

System logs should not be able to be deleted by a single person. Such deletion should be done in the presence of at least 2 people, who will have different roles (e.g. security officer or administrative manager).

- Use of encryption: The organization should implement effective encryption (choice of modern and strong encryption algorithms, appropriate key size and key management techniques, etc.) of files with personal data held on portable storage media (e.g. USB sticks), since for these cases the risk of data leakage increases.

2.2.4 Recommendations by the Italian National Framework for Cybersecurity and Data Protection

Established in 2015, the [National Cybersecurity Framework](#) provides a tool to support organizations that need strategies and processes aimed at personal data protection and cybersecurity, according to the General Data Protection Regulation (GDPR), which governs the treatment and circulation of personal data. The framework, inspired by the [Cybersecurity Framework](#) created by NIST (National Institute of Standards and Technology), inherits its three fundamental notions: Framework Core, Profile and Implementation Tier. In the following, a brief description of these key points is presented.

2.2.4.1 Essential elements

The **Framework Core** represents the structure of the life cycle of the cybersecurity management process, both from a technical and organizational points of view. The core is hierarchically structured in *function*, *category* and *sub-category*. The functions are: *IDENTIFY*, *PROTECT*, *DETECT*, *RESPOND* and *RECOVER* and are the main issues to be addressed to operate strategic cyber risk management. Therefore, for each function, the framework defines category and subcategory, the enabling activities, such as processes and technologies, to be implemented to manage it. For this purpose, the Framework Core combines every single subcategory with references to the safety practices envisaged by sector standards or general regulations in force and which are the starting point for a correct and safe implementation. The version of the presented framework incorporates a series of new elements in the core aimed at guiding the correct management of personal data, with specific reference to their security in the face of possible cyber attacks. In addition, NIST's changes to the Framework Core have been integrated, thus including elements to consider supply chain security issues and to deepen the security of authentication and identity management processes. The different *sub-categories* of the framework are many and aim to cover all the possible needs of an organization. Therefore, in most cases, a single organization is only interested in a subset of them.

Profiles represent the result of an organization selecting specific *sub-categories* of the framework. This selection is based on several factors: the risk assessment, the business context, and the applicability of the various *sub-categories* to the organization. Profiles can be used

to improve the security status by comparing a current profile (current profile) with the desired profile (target profile). The profiles can also be used to carry out a self-assessment or to communicate one's level of cyber risk management inside or outside the organization.

Implementation Tiers provide context on the level of integration of cyber risk management processes within the organization. There are four levels of evaluation, from the weakest to the strongest:

- **Partial** - An organization's cyber risk management model is partial if it does not systematically consider the cyber risk or environmental threats. Cyber risk is managed with ad hoc processes and often in a reactive manner. The level of risk awareness at the organizational level is limited. There are no processes for sharing information related to cybersecurity with external entities.
- **Informed** - An organization's cyber risk management model is informed if the organization has internal processes that account for cyber risk, but these are not organization-wide. The awareness level of cyber risk is sufficiently broad, but this is not accompanied by pervasive management processes involving all levels of the organization. The organization understands its role in the reference ecosystem, but the exchange of information related to cybersecurity events is limited and typically passive.
- **Repeatable** - An organization's cyber risk management model is repeatable if formally defined and approved and if the organization regularly updates its cybersecurity practices based on the output of the risk management process. Cyber risk management is pervasive at all organizational levels, and personnel are trained to manage the roles assigned. The organization regularly exchanges information related to cybersecurity with other actors operating in the same ecosystem.
- **Adaptive** - With an adaptive cyber risk management model, an organization adapts its cybersecurity procedures with past experiences and risk indicators. It continuously aligns with ever-evolving threats and can respond effectively to sophisticated attacks. The information exchange with other players operating in the same ecosystem is continuous and happens in real time.

The framework also introduces the *priority* and *maturity levels* that allow the creation of a flexible tool that adapts to the organization's needs and considers its maturity in dealing with cyber risk and a new tool called *contextualization prototypes*.

Priority levels allow organizations and companies to be supported in defining an implementation program to achieve a target profile that favours as a priority the interventions that most reduce the levels of risk to which they are targeted. Therefore, the goal is to identify the essential sub-categories to be implemented immediately. The priority levels assigned to the sub-categories must be determined based on two specific criteria:

- The ability to reduce cyber risk, in terms of exposure to threats, the frequency of a hazard which can occur over time and the consequent impact on Business

D6.6 Data breach management plan (V2)

Operations or Company Assets, understood as the extent of the damage resulting from the occurrence of a threat;

- The simplicity of implementation of the sub-categories, also considering the level of technological and organizational maturity typically required to carry out the specific action.

The framework has three general levels of priority: **HIGH**, interventions that significantly reduce one of the three cyber risk factors. These interventions are priorities and must be implemented regardless of the implementation complexity of the same; **MEDIUM**, interventions that make it possible to achieve a reduction of one of the critical factors of cyber risk and which are generally also simple to implement; **LOW**, interventions that make it possible to achieve a reduction of one of the three cyber risk factors but whose implementation complexity is generally considered high, for example, significant organizational changes or significant infrastructural changes. It should be noted that the sub-categories take on a specific priority in the organization context.

Maturity Levels give information about a security process maturity, the implementation maturity of a specific technology, or the number of resources used to implement a given sub-category. The maturity levels provide a benchmark against which each organization can evaluate its implementation of the sub-categories and set goals and priorities for their improvement.

Finally, the **contextualization prototypes** tool allows defining applicable templates in the contextualization phase to more easily integrate concepts related to laws, regulations or best practices into the same. It represents an essential element based on which it is possible to build a new contextualisation or which can be adopted and implemented in an existing one.

2.2.4.2 Cost of a data breach report

According to the 17th annual [Cost of a Data Breach Report](#), conducted by the Ponemon Institute and sponsored, analyzed, reported and published by IBM Security, the energy industry ranked fifth in data breach costs, surpassed only by the healthcare, financial, pharmaceutical and technology sectors. The energy sector includes oil and gas companies, alternative energy producers and suppliers and utility providers such as electric companies. Cybersecurity breaches and failures in this sector can have massive impacts.

In 2020 in Italy, according to a survey, the energy sector was among those most affected by cyberattacks, with a loss of 165 euros for each piece of information stolen. This escalation of data breaches is mainly due to the rapid changes dictated by the pandemic, explains IBM, such as the transition from "traditional" to remote work and the migration of businesses towards a "cloud-based" approach to ensure business continuity.

2.2.4.2.1 Top cybersecurity mitigations

Chris McCurdy, vice president and general manager of IBM Security, says that "although data breach costs have reached record highs over the past year, it has been found that the adoption of innovative cybersecurity technologies and approaches, such as Artificial Intelligence (AI), Security Automation and the Zero Trust approach, can help reduce the cost of incidents with returns for the future as well". Artificial Intelligence, security analytics and encryption for IBM security were the top three breach mitigation factors, demonstrating how these technologies can reduce costs per attack. For cloud-based data breaches, however, the costs incurred have been in favor of companies that have adopted a hybrid cloud strategy rather than public or private cloud solutions.

2.2.4.3 What's going on with national cybersecurity?

In Italy, the national reference legislation on data security is represented by Law 4 August 2021, n.109, containing "Urgent provisions on cybersecurity, the definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency". This legislation has transposed the **NIS** 2016/1148 Directive "On the security of networks and information systems" at the national level, with which the European Commission has laid the necessary foundations for regulating and regulating the essential aspects of information security, with reference to companies operating in critical infrastructures, on which the socio-economic fate of entire nations depend. However, the continuous evolution of increasingly specialized cyber threats has prompted the European Commission to propose a revision of the directive, providing updates on cybersecurity issues. Hence the NIS2 is presented below.

2.2.4.4 The NIS2 & CER directives

On November 10th 2022, the European Parliament, with a large majority, approved the Network and Information System Security (**NIS2**) directive². Margrethe Vestager, Executive Vice-President of the European Commission in charge of Competition, declared that with the NIS2³, "additional tools will be proposed that strengthen our collective ability to respond to cyber threats, from prevention to the detection of concrete threats that already exist." The directive will formally establish the European network of cyber crisis link organizations *EU-CyCLONe*, which will support the coordinated handling of large-scale cybersecurity incidents.

² Sources: <https://www.nis-2-directive.com/>

³ NIS2 details: <https://www.cybersecurity360.it/legal/direttiva-nis2-approvata-ecco-cosa-cambia-in-materia-di-sicurezza-di-dati-reti-e-sistemi/>

The European Council also approved the **Critical Entities Resilience** (CER)⁴ directive, issuing a recommendation on cyber security. The new legislation goes hand in hand with the NIS2 to reconcile physical and cyber security. Therefore, NIS2 deals with the cyber security of critical and highly critical entities and the CER with their resilience concerning natural, voluntary, or involuntary threats, including terrorist threats.

2.3 Electric Power and Energy System Overview

An electric power and energy system consists of different elements ranging from electric power generators to the devices consuming electric energy at end user property. The elements in the system are usually categorized into four following levels:

- **Generation level:** The elements in the generation level mainly convert energy from different sources and in different forms to electric energy. Electric power generators in power plants and distributed energy resources are the main elements in the generation level. The elements can be divided into renewable and non-renewable power generators according to the source of energy. Fossil-fuel based power plants and nuclear power plants are examples of non-renewable power generators. Wind turbines and solar panels are samples of renewable power generators. In the generation level, the trend is towards renewable and distributed power generators which are expected to be locally installed very close to electricity consumption areas.
- **Transmission level:** Conventionally, power generators have been located outside of cities since they produce pollutants as well as they need water and fuel which are not necessarily available inside cities. This means that the power generated by power generators need to be transmitted to consumption areas which are cities and large industrial sites. In order to transmit electricity in long distances without significant energy loss, voltage level should be increased. This way, current level is decreased which decreases energy loss significantly. In many countries, elements in electricity networks with voltage levels higher than 115 kV form transmission level.
- **Distribution level:** In cities where electricity is consumed by the society, there is an electricity network which receives electricity from transmission network and distributes it among electricity consumers. The network and its elements form distribution level. The voltage level in distribution level cannot be the same as in transmission level mainly because land is scarce and expensive inside cities and the high voltage levels are dangerous for the society members. On the other hand, decreasing voltage to the consumption level can be translated to higher energy losses. To this end, voltage levels from a few kV to tens of kVs are usually selected for distribution level in order to make a tradeoff between energy losses and safety of the society individuals.

⁴ CER details: <https://www.cybersecurity360.it/cybersecurity-nazionale/resilienza-delle-infrastrutture-critiche-cosileuropa-concilia-sicurezza-fisica-e-cyber/>

D6.6 Data breach management plan (V2)

- **Consumption level:** In consumer territory, there are different equipments that consume electricity such as a washing machine and a dishwasher. These equipments basically transform electricity into other forms of energy according to the end user wishes. The voltage level in the consumption level is either 110 V or 220 V. Larger consumers receive a 3-phase circuit and smaller ones have 1-phase circuits. In some countries like Finland where electricity is the main energy source of end users and electricity consumption per capita is high, 3-phase circuits are implemented almost everywhere.

In electric energy supply chain, there are many players acting in the above levels to ensure that the electricity is produced, transmitted, distributed and consumed economically, safely, securely, reliably and environmentally friendly. The main players and a brief description about their roles are provided in the following:

Power producer: Electric power generators from any type are owned/operated by power producers. In addition to technical operation of the generation facilities, these players participate in electricity market to sell their electricity production too. They may participate in ancillary service markets such as flexibility market too.

Transmission system operator: Transmission system operators construct, maintain and operate electricity transmission systems. In the construction phase, transmission system operators forecast potential changes in size and location of electricity demand and supply and develop their systems accordingly. Their objective is to ensure affordability and security of electric power supply with minimum required investments. In the operation phase, they forecast near future supply and demand and operate the system to economically and reliably transmit electricity to electricity consumption points. In the maintenance phase, transmission system operators ensure that the existing system and its components are operated in an appropriate way. Needless to mention, transmission system operators are mainly focusing on technical activities rather than business. Transmission system operators have natural monopoly so their business is under regulation.

Distribution system operator: Similar to transmission system operators, distribution system operators do construction, maintenance and operation of electric circuits but their systems are mainly in urban and suburban areas and have lower voltage levels. Distribution system operators mainly focus on technical activities, and due to their natural monopoly, their business activities are under regulation.

Market operator: In energy systems, different markets are developed to ensure transparent and competitive prices for electricity. The player is responsible for operating electricity market to ensure consumers have access to affordable and secure energy. Market operators develop and maintain relevant marketplaces for energy and ancillary service markets where power producers can sell their electricity production and consumers, aggregators and electricity retailers can buy their or their customers electricity needs. The marketplaces are developed and operated in a way that most affordable electricity production considering energy system security is implemented.

Balance responsible party: In electric energy system, electricity supply and demand should always be balanced to maintain system frequency. In any energy system, market players are also balance responsible parties who plan their operations to maintain the balance between their electricity supply and demand as well as their electricity procurement and sale. The player can be a producer, consumer or even a trader of electricity.

Balancing service provider: This player provides balancing services to a transmission system operator. This player can be a producer, consumer or a trader of electricity. By providing balancing services, balancing service providers give the chance to transmission system operators to invoke the service to maintain system frequency when necessary.

Imbalance settlement responsible: The player is responsible for the settlement of the difference between the contracted and realised quantities of energy products for the balance responsible parties. This player checks the exchanged energy and the amount of energy that was supposed to be exchanged with each balance responsible party and makes an invoice according to that. The invoice value depends on the difference between the contracted and realized energy exchange as well as imbalance price.

Electricity retailer: This player sells electricity to an end user. It sells and buys electricity directly from a producer, another retailer or via participating in the energy market. The competition among electricity retailers ensure that the retail price of electricity which is paid by end users is fair.

Energy service company: This player is a party that provides different services to the other players in electric energy system. Energy data exchange, energy metering operations, asset monitoring and energy trading companies are some examples for an energy service company.

Aggregator: In energy system, there are limits for market participants. As an example, a residential electricity consumer is not eligible to participate in wholesale energy market due to set threshold. So, the end residential consumer is bound to make a supply contract with a retailer who then participates in the wholesale market. The consumers can form a coalition which is managed by an aggregator to meet the threshold for participating in the wholesale market. Then, they can procure their electricity needs as well as offer ancillary services to the energy system. It is worthwhile to mention that an aggregator does not aim for aggregating consumers, it can aggregate small power production units to enable them participate in energy market and offer ancillary services too.

In order to have an affordable, secure, and reliable energy system, the above-described players exchange relevant data and interact both with end users and each other. It is crystal clear that the data exchange and maintenance must be secure to achieve the target. This is the main incentive for the studies conducted to provide approaches for enhancing cybersecurity of the system.

3 Recent studies and documents on data breaches

3.1 Data breaches events on each country

In this chapter, the focus is on analyzing recent data breach events in different European countries and how the responsible bodies handled the incidents in order to identify the best and worst decisions and practices, especially from data breach management perspective. These data are collected from different countries to see if there is deviation or similarities between the countries.

3.1.1 Finland

In this section, the aim is to gather and analyze recent data breach events in energy sector in Finland. Since there was no public information about any major event in Finnish energy infrastructure or other critical infrastructures in recent decades, the biggest cybersecurity event has been selected to analyze here. The incident was a data breach incident to Vastaamo psychotherapy centre. The psychotherapy centre Vastaamo was a Helsinki-based private psychotherapy center founded in 2008. Vastaamo provided private mental-health services to its patients. It was a firm with twenty-five therapy centers throughout Finland where it operated as a sub-contractor for the national public health system. In the following, the incident, relevant consequences of the incident as well as the lessons learned are provided.

3.1.1.1 Incident

In September 2020, the CEO of Vastaamo notified various government authorities, including the police about a data breach incident. In October 2020, Vastaamo announced that its confidential treatment records of approximately 36000 psychotherapy patients and 400 employees had been compromised.

The leaked patient database contained psychotherapy clients' personal information, such as their full names, home addresses, email addresses, social security numbers, names of the clinics where they received treatments, and therapists' and doctors' notes from each session. The leaked information was used to extort Vastaamo and its affected clients and was published on the dark web. The extorters demanded 40 bitcoins, roughly 450000 euros at the time, or threatened to publish the records. To add pressure for their demands, the extorters published hundreds of patient records a day on a Tor message board.

As the company resisted to pay the ransom, the hacker, using the alias "ransom_man," published the therapist session notes of at least 300 patients, including politicians and police officers, using a server called Tor, a public forum. The therapist session notes contained information about adulterous relationships, suicide attempts and pedophilic thoughts. The

hacker approached victims of the security breach directly with extortion emails demanding ransoms of 200 euros paid in Bitcoin, with the amount increased to 500 euros unless paid within 24 hours in order to avoid publishing their sensitive personal data. The ransom demands were sent to roughly 30000 victims. A 10-gigabyte data file containing private notes between at least 2000 patients and their therapists had appeared on websites on dark web.

According to a technical investigation completed on October 2020, the company's security practices were found to be inadequate: the sensitive data was not encrypted and anonymized, and the system root did not have a defined password. It was found very likely that the patient records were stolen during two attacks, which started as early as 2018. The first access by intruders was in November 2018, while the security flaws continued to exist until March 2019.

It was found that the patient database of Vastaamo was very likely downloaded via an open internet port used by the MySQL database software. The technical investigation has also revealed that on November 2018, almost a gigabyte of data may have been transferred from the MySQL service of the Vastaamo patient information system to an IP address managed by a Swedish VPN provider. In the technical investigation, a database containing an extortion message has been found on the server of the patient information system, PLEASE_READ_ME_XMG, which is very likely created by an attacker on 15 March 2019. According to the extortion message, the patient database has been uploaded to the attacker's servers, and a ransom has been demanded against the recovery of the lost data.

3.1.1.2 Consequence

The cyber-attack became the biggest criminal case in Finland history. It also turned into an international scandal and a cyber-attack unprecedented in its scope due to the tactic called double extortion applied by the cyber criminals.

In December 2021, the Finnish Data Protection Authority (DPA) fined Vastaamo 608000 euros for violating the provisions of the General Data Protection Regulation (GDPR). This fine was mainly due to the fact that Vastaamo neglected its duties related to the safe processing of personal data as well as reporting a personal data breach.

Based on technical investigations, it was found that the personal data had not been appropriately protected against unauthorised and illegal processing or accidental disappearance since Vastaamo had not implemented basic measures to ensure the safe processing of personal data. It was also found that Vastaamo must have become aware that the patient data had disappeared and that it may have ended up in the possession of an external attacker already in March 2019. Vastaamo should have reported the breach both to the supervisory authority and its customers without delay.

After the incident, the company acquired a 70% stake in Vastaamo in May 2019 requested that its acquisition of the company be cancelled, and the purchase price be returned for failure to disclose hacking. CEO of the firm was relieved of his duties as the chief executive of the psychotherapy center in October 2020. To this end, Vastaamo was declared bankrupt

by the decision of the Helsinki District Court in February 2021, and its staff and services were transferred to Verve, a provider of occupational welfare services in early March 2021.

The security breach has shaken societal trust in Finland's institutions, violated sensitive systems, and damaged faith in online social networks that are supposed to be properly secured. Thousands of victims have suffered anxiety, insecurity and stress from this traumatic event. After the incident, mental health and victim support charities reported being overwhelmed with calls from distressed people fearing their intimate conversations with their therapists would be released.

All in all, the security breach served as a wake-up call for Finland's cyber security. Focus on balancing availability of information and data governance has increased along with investments in companies' computer security since the hacking incident occurred. As a result of the data breach, the Finnish Data Protection Authority (DPA) started taking the violations of the GDPR more seriously and increased enforcement activities. The outcomes of investigations of the security breach, and also any sanctions established, now serve as a reference point to any future legal assessments.

3.1.1.3 Mitigation measures

Immediately following the incident, the cabinets from the Finnish government held their regular Wednesday meeting to address cybersecurity issues, create new legislation regarding data security and identity thefts, and promise emergency support for the victims. The Deputy Data Protection Ombudsman has ordered Vastaamo to notify the victims about the personal data breach personally. More than 22600 victims of blackmail in 2020 have visited The Victim Support Finland (RIKU), an organization that provides counseling and support to victims of crimes. Various Finnish organizations have quickly established ways to help the victims, including direct dial-in numbers to churches and therapy services. Different organizations including Finnish Red Cross, Mental Health Finland, Victim Support Finland and the Evangelical Lutheran Church of Finland provided victim support services. Additionally, many companies working with social security numbers and debt collecting had taken action to help the victims whose identities have been stolen. In order to rebuild public trust in the government and authorities, the Finnish central government requested that government agencies make sure the processing and handling of personal information are secure to minimize the leakage of personal data. Additionally, ministries conducted reviews on what they can do better within their own departments and how they can assure the public about the security of their personal data. The Finland's National Bureau of Investigation introduced an unprecedented Finnish criminal code, where a person can be found guilty of the privacy violation of a data subject when they process personal data, either intentionally or through gross negligence, and cause damage or significant inconvenience to the data subject. Furthermore, the Finnish government accelerated legislation that allowed its citizens to change their personal identity codes when there is a data breach that would involve high risk of identity theft.

In addition to the above services and activities, authorities launched a website for victims of the cyber-attack, offering relevant advices such as the following items:

1. File a report of an offence with the police, if you notice that the leaked information has been disseminated or if you have received an extortion message related to the Vastaamo data system break-in. Do not respond to the extortion message or pay the extortionist. Enter all information about the sender and the time when the message was received accurately into the report of the offence. Save and store the e-mail messages, other messages and other possible evidence you have received.
2. If you notice transactions in your bank account that you have not made yourself, file a complaint with your bank. You should also file a report of an offence concerning the transactions with the police.
3. Consider getting a personal credit ban which reduces the risk of identity theft as well as credit card purchases and payday loan withdrawals by a third party. The credit ban is subject to a charge. Vastaamo will reimburse the purchase of security services by victims of the data breach.
4. Notify the Finnish Patent and Registration Office that you cannot be entered in the Trade Register as a responsible person of a company or corporation without your explicit consent.
5. Request address change protection from post office and consider prohibiting the disclosure of your information.
6. Ask for support and advice from different parties described, if necessary.
7. Prepare for the possibility that the leaked information may come up again later and think about how you will react or respond in such a situation already in advance.

3.1.1.4 Vastaamo negligence

Investigations conducted by the Deputy Data Protection Ombudsman revealed that Vastaamo has violated several articles of GDPR. The main violations are described in the following:

1. Before November 2020, Vastaamo did not process personal data in accordance with the principle of integrity and confidentiality of personal data in a manner that ensures the appropriate security of personal data
2. Vastaamo did not report the personal data breach that took place in March 2019 to data protection ombudsman
3. Vastaamo did not document the personal data breach that occurred in December 2018
4. The data protection impact assessment prepared by Vastaamo does not meet requirements by GDPR

According to the above descriptions, negligence from Vastaamo was mainly on data security and incident reporting.

3.1.1.5 Lessons learned

In accordance with lessons learned from the Vastaamo incident, a party who works with personal data needs to do the followings in normal condition to avoid data breach:

1. Relevant solutions such as data encryption and anonymization and access control and limit must be applied to ensure security of sensitive data. It is worthwhile to point that in Vastaamo incident, the sensitive data was not encrypted and anonymized, and the system root did not have a defined password.
2. Relevant activities must be documented to enable supervisory authorities to verify compliance with regulations. In case of Vastaamo incident, due to incomplete documentation, Vastaamo has not been able to demonstrate that relevant security measures were fully in place at the time of the data breach.
3. Incident contingency plans must be prepared to assist the party in planning and determining who in the organization has operational responsibility for managing the security breach and whether the incident will be reported up the hierarchy, and if so, how. In case of Vastaamo incident, there were two relevant documents by Vastaamo company namely "Psychotherapy Centre Vastaamo Oy's operations in data breach situations" and "Information security incident management and register". It was however unclear whether the first document was in use at the time of the personal data breach. The second document was prepared in March 2019 which means the document was not yet in use at the time of the data breach.

According to GDPR, there are three main activities must be done in a timely manner when a personal data breach happens:

1. In the event of a personal data breach, the controller shall, without undue delay and, where possible, within 72 hours of its discovery, notify the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification is not made within 72 hours, the controller shall provide the supervisory authority with a reasoned explanation.
2. According to GDPR, where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subjects without undue delay.
3. According to GDPR, the controller must document any personal data breach, including the facts surrounding the personal data breach, its effects and the corrective actions taken.

3.1.2 Estonia

There have not been any significant cyber incidents related to the energy sector in Estonia. However, there was recently an incident where someone stole 300 000 digital ID photos from a government website. This section describes different aspects of the incident.

3.1.2.1 Incident

On 21 July, CERT-EE detected that 286,438 document photos had been illegally downloaded from the database of identity documents. They had been downloaded in masse from 9,000 Estonian and foreign IP addresses since 12 July. This was caused by a security vulnerability in the photo transfer service (so-called photo service) that is used when a person wants to download their document photo.

You can download your document photo directly from the state portal or through the DigiDoc application. In both cases, the person must first authenticate themselves. Once the request has been made, the system requests the photo from the service that mediates it, the so-called photo service, which RIA manages. The photo service requests the photo over the X-tee from the database of identity documents, which belongs to the Police and Border Guard Board, and sends it back to the person. Upon detection of the attack, RIA temporarily closed this function for DigiDoc.

How was the attacker able to download anything?

DigiDoc makes requests over a public URL. By manipulating this, the attacker managed to give the photo service the impression that the request comes from an authenticated user who wants to download their document photo. However, behind the request was an attacker who turned directly to the photo service using forged or self-created certificates. To create a fake certificate, the attacker had to have the person's personal identification code and name.

The photo service should have recognized that SK ID Solutions did not issue the certificates used by the attacker – that they were forged. Due to the security vulnerability, the service did not do this. Although the attacker had marked SK ID Solutions as the issuer of the fake certificates, "looking into" them would have shown that they came from elsewhere.

As a result of the attack, the criminal did not have access to the database of identity documents but managed to download document photos from it.

3.1.2.2 Consequence

Reportedly, the security vulnerability in the photo transfer service occurred in November 2018. The service interruption was probably related to the exchange of ID-card certificates – changes were made in the information systems to support authentication with new certificates. CERT-EE analyzed logs starting from 30 June 2018 and found no other anomalies. This leads to the conclusion that the security vulnerability of the photo transfer service had not been abused before (i.e., before July 2021).

The police detained the suspect a few days after the incident was discovered and confiscated the downloaded data. Preliminary information suggested that the photos were simply stored on the attacker's computer. The proceedings conducted by the Office of the Prosecutor General are still ongoing.

It is rare for attackers behind cyber incidents to be caught so quickly. They are often located abroad, and their traces are difficult – if not impossible – to detect. In this case, they managed to do so thanks to quick and efficient cooperation between the police, CERT-EE, and the Prosecutor's Office.

3.1.2.3 Mitigation

A few days after the discovery, the security vulnerability was patched, and RIA reopened the photo service for DigiDoc so that people could download their document photos again.

3.1.2.4 Lessons learned

RIA analyzed and improved its workflows to prevent future incidents caused by such security vulnerabilities. In addition, the case inspired RIA to create a national bug bounty programme to motivate good hackers. This means that hackers who have discovered security vulnerabilities in state systems may receive a reward from the state in the future. However, the compensation is only paid if the hacker follows the established rules and conditions. The rewards programme is currently being worked on.

3.1.3 Slovenia

3.1.3.1 Case 1

3.1.3.2 Incident

In February 2017, the Slovenian tech forum brought to public attention SQL injection type vulnerabilities on the website of AJPES, the Agency of the Republic of Slovenia for Public Legal Records and Related Services, that manages among other things the Slovenian Business Register.

The news was picked up by major Slovenian news outlets. The Slovenian Information Commissioner launched an inspection procedure against AJPES.

Also, SI-CERT, Slovenian Computer Emergency Response Team, spoke out.

SI-CERT operates within the framework of the ARNES (Academic and Research Network of Slovenia) public institute. SI-CERT/ARNES is a partner of the CyberSEAS project.

SI-CERT announced that it was willing to take on the role of coordinator for the disclosure of vulnerabilities related to the AJPES website, so all notifications of additional vulnerabilities related to the website should be forwarded to them and any ethical hacking activity should be also coordinated with them.

More information about the incident can be found in [1]- [2].

3.1.3.3 Consequence

At the time of the public disclosure of the incident it was not known whether the vulnerability had effectively been exploited by malicious agents.

Investigations into the general cyber security posture of the AJ PES website and services lead to the discovery and disclosure of another weakness, namely that a document signing service did not sign the actual document but only an identifier. This did not protect against tampering with the document itself.

3.1.3.4 Mitigation measures

AJ PES took immediate action with its external contractor partner to mitigate the problem.

Given they were not given time to take mitigation actions before the vulnerabilities were disclosed, AJ PES also felt obliged to inform law enforcement agencies and file a complaint.

3.1.3.5 Official report findings

The investigation was carried out by the Slovenian Information Commissioner Office with the support of SI-CERT which carried a subsequent analysis of several gigabytes of logs of the affected portal in order to determine whether a data leak took place in the time frame between when vulnerability was introduced (via a regular upgrade where the contractor developing the software failed to turn on SQL-injection protections) and the disclosure. No indicators of such a data leak were found, while many probes for data were present that were linked to the announced vulnerability.

3.1.3.6 Lessons learned

A consensus grew that this incident had shown that the various actors in Slovenia, ethical hackers, technical forums and media, had not followed guidelines of the responsible vulnerability disclosure process. Even in the absence of the official Coordinated Vulnerability Disclosure policy, the common industry-standard should be observed. SI-CERT advocated at multiple instances that such a process should be followed and give vendors and developers enough time to patch the vulnerability before its disclosure.

Slovenian Information Commissioner Office and SI-CERT decided to sign an agreement on cooperation and information exchange that defined the SOP for future joint investigations.

3.1.3.7 Case 2 (NEW)

3.1.3.7.1 Incident

In the night from 24.11.2023 to 25.11.2023 The HSE Group suffered a major cyber-attack. The group is the largest producer and seller of electricity from domestic sources on the wholesale market in Slovenia and the largest Slovenian producer of electricity from renewable sources. According to public sources, unusual activities were detected by internal HSE logging systems

D6.6 Data breach management plan (V2)

a few days before, but it was believed that the attack was limited and under control. However, later activities show that the attack has spread and intensified.

HSE took quick action and promptly informed relevant authorities (law enforcement, SI-CERT, Slovenian Government Information Security Office (URSIV), government and other relevant stakeholders).

According to statement from URSIV, it can be assumed that this was a targeted attack. Attackers gained access months before activities were detected to gain as much information about the IT system and its vulnerabilities as possible, before launching an attack. Later investigation showed that an attack was a typical third-party supply chain attack, which originated from a compromised external contractor partner.

3.1.3.7.2 Consequence

According to public sources, credentials of the external contractor partner were stolen and then used to gain access to HSE resources. "Infostealer" malware was used to compromise and encrypt systems and data in the business part of the IT system. Consequently, business operations were impacted for several weeks after the incident.

According to HSE, the industrial part of the IT system was not affected by the attack, therefore the power plants and production of electricity was not interrupted or endangered in any way.

3.1.3.7.3 Mitigation measures

HSE took immediate action with internal and external professional teams in the field of information security and other key experts to ensure business continuity as soon as possible.

There is no official statement from HSE whether extortion ransom was requested and/or payment was made.

On 25.11.2023 URSIV informed all operators of essential services under NIS directive about the attack with a list of recommended measures to mitigate cyber-attacks, such as geofencing, incident response procedures review, access control review, MFA, endpoint protection and security log review, vulnerability and patch management review, disaster recovery review, BCP review, etc.

SI-CERT also provided all operators of essential services under NIS directive with a list of Indicators of compromise (IOC) to help with technical mitigation measures.

3.1.3.7.4 Official report findings

The investigation was carried out by the Slovenian Government Information Security Office (URSIV) with the support of SI-CERT and HSE staff. The findings were not publicly disclosed.

3.1.3.7.5 Lessons learned

An attack has shown the seriousness of third-party supply chain attacks. Many other HSE partners were at risk and had to take additional security measures. Based on this and similar

cyber-attacks and professional opinions, the main weak points in such cases can be summarised as follows (sorted by criticality):

- insufficient management of external contractors,
- insufficient privilege access management,
- poor network visibility,
- insufficient network access control,
- lack of identity management.

The new Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) puts increased focus also on securing supply chain with stricter requirements for contractors and service providers.

3.1.4 Italy

In this section, we gather and analyze recent data breach events in Italy.

According to the European Union Agency for Cybersecurity (ENISA) report, Italy is the fourth country among the most affected by data breaches, especially by ransomware attacks. It has been estimated that the single stolen data is worth 143\$ in Italy, against the global average of 164\$. In the following, some of the most notable cyber-incidents related to data breach in Italy are reported.

3.1.4.1 Incident

In recent years, major cyber-incidents led to leak and exposure of sensitive data within Italian companies.

In August 2021, the Italian telecommunications company TIM Group was hit by unauthorized access to their technical assistance systems, leading to the compromise of the company's database.

In October 2021, a data breach event affected San Carlo, a leading Italian manufacturer of snack foods. The company announced that technicians noticed an intrusion in their computer system and immediately activated the security measures to isolate and retain the threat.

In its latest Threat Landscape report, the ENISA also reported 33 incidents concerning energy systems. The energy sector has been among the most targeted, due to the strong reliance of Critical Infrastructures on energy distribution, and the strategic value of such systems.

In April 2022, the Italian multinational manufacturer and distributor of electricity and gas Enel was victim of a massive data breach. In August 2022, Italy's energy agency Gestore dei Servizi Energetici (GSE) was also targeted by ransomware.

3.1.4.2 Consequence

The data breach at TIM affected personal data, including login credentials of an unknown number of current and former users to the company's customer area MyTim.

The attack targeting San Carlo was ransomware, claimed by the cyber-criminal group Conti. Major consequences were the leak and exposure of sensitive information, including financial data, personal documents (passports, national IDs), and contracts.

Enel's customers faced significant consequences due to the data breach: the attack, which has been associated with the activity of the cyber-criminal group Industrial Spy, led to the loss and exposure of 745 GB of sensitive data, including customer's personal information.

The breach at GSE caused the compromise of their server, making employees unable to access internal data or their own email accounts. The BlackCat ransomware group took credit for the attack and claimed to have stolen more than 700 GB of data from the agency.

3.1.4.3 Mitigation measures

With compliance to the General Data Protection Regulation (GDPR), the companies informed the competent authorities and analyzed the stolen and tampered data.

To limit the consequences of the attack, TIM revoked the passwords of an unknown number of customers, inviting them to change the login credentials of the MyTim restricted area. The company also warned the users to pay attention to possible phishing attempts.

San Carlo refused to pay the ransom and managed to quickly recover and face minimal consequences thanks to an efficient Disaster Recovery plan and data backups.

The Enel attack didn't lead to the exposure of financial information, therefore the company decided to just alert the competent authorities.

GSE decided to make their websites and portals unavailable, and some market functions were suspended as a precaution.

3.1.4.4 Lessons learned

The recent cyber-incidents have been a wake-up call for Italian companies, especially Critical Infrastructure operators.

After the attack, GSE recommended to "raise the levels of protection of digital infrastructure of energy operators". The situation has been so concerning that Mario Draghi, Italian Prime Minister at the time of the incidents, decided to urgently hold a cybersecurity emergency meeting with the Interministerial Committee for Cybersecurity and other top government officials.

The San Carlo experience taught a lesson regarding the crucial importance of following good practices for cyber-security, such as frequent data backups and an efficient Disaster

Recover plan, which have helped the company recover from the attack with minimum consequences.

Regular Risk Assessment should also be conducted: a cyber-security strategy is mandatory for any organization, but it needs to be supported by frequent vulnerability assessments and audits to ensure that the current policies are sufficiently robust. Furthermore, it is recommended to raise employees' awareness, due to the huge role played by the workforce in preventing data breaches. Without proper training, employees are likely to represent among the most significant vulnerabilities in the system.

3.1.5 Greece

In this section, a data breach event in the energy sector in Greece is analyzed. DESFA, the company that suffered the data breach in August 2022 is responsible for the operation, management, exploitation and development of Greece's National Natural Gas System and its interconnections. Another incident that is analyzed is a data breach that occurred at COSMOTE, Greece's largest telecommunication company, in September 2020. COSMOTE which is a member of OTE group of companies, provides fixed and mobile telephony services, broadband services, pays TV and integrated information and communications technology solutions.

3.1.5.1 DESFA incident

On 20th of August 2022, Greece's largest natural gas distributor DESFA announced that part of its IT infrastructure was cyberattacked by cybercriminals who attempted to gain illegal access to electronic files. According to a public statement made by the company, the IT department prevented hackers attempt to penetrate its network.

3.1.5.2 Consequence of the attack on DESFA

However, there was a network breach since the attackers managed to gain access and leak documents and other data. Hackers used a ransomware and managed to bypass all the security measures. Ragnar Locker, that was the hacker team behind the attack, managed to steal 360 gigabytes of confidential data. Subsequently, they demanded a sum of money in order not to leak the data. They also said they had contacted the company to inform them of the vulnerability that led to the breach, but they had received no response. DESFA refused to pay them and hackers leaked DESFA files on the dark web. The records included engineering designs, budget and revenue documents, past revenue spreadsheets, copies of non-disclosure agreements with customers and partners etc.

According to the FBI, Ragnar Locker is behind 52 cyberattacks in critical U.S. infrastructure entities related among others to energy and the construction sector from April 2020 until January 2022.

3.1.5.3 Mitigation measures against the attack on DESFA

Once the cyberattack was noticed, the company informed all competent authorities and organizations like the Ministry of Digital Governance, the Data Protection Authority, the Electronic Crime Prosecution of the Hellenic Police, the Hellenic National Defense General Staff as well as the Ministry of Environment & Energy and the Energy Regulatory Authority and worked with them to resolve the issue and minimize any potential impact. To protect its customers and partners, DESFA has proactively disabled most of its IT services, with the systems gradually re-operating. It is worth mentioning that in contrast to other attacks by Ragnar Locker, the national system of natural gas continued to function smoothly and was not at all affected by the cyberattack.

More information about the incident can be found in [3], [4], [5], [6], [7], [8].

3.1.5.4 COSMOTE incident

In 2020, telecommunication company Cosmote, which is part of OTE group of companies with annual turnover of €3.258 billion, reported to the Hellenic DPA that suffered a data breach due to a cyberattack. The breach was detected through an automated notification message, that a server's data storage disk has exceeded its capacity limit.

3.1.5.5 Consequence of the attack on COSMOTE

After investigation, a 30 GB file was found stored on this server that included information of about 4,792,869 customers' calls from 1/9/2020 until 5/9/2020 and contained the following data: phone numbers, base station coordinates, IMEI, IMSI, timestamp, duration of the call, provider indicator, subscription plan, age, gender and average revenue per user. Additionally, 30GB of data was transmitted from the server to an external IP in Lithuania. The hacker managed to gain administrative access, using the password of an OTE administrator, which had come into the hacker's possession in the past, after a password leak incident. Subsequently, the hacker retrieved the data from the server and stored them in the file. Apart from that file, another four significant data transfers had been made from COSMOTE server to the same Lithuanian IP. It was not possible to identify what type of data was transmitted through this traffic.

For that data breach, COSMOTE was fined €6.000.000 and OTE was fined €3.250.000. The Hellenic DPA accused the two companies of wrong doing due to the implementation of the process of anonymizing the disputed files as well as insufficient security measures for the protection of personal data. It was also found, on behalf of OTE, a violation due to insufficient security measures in relation to the infrastructures used in the context of the incident.

More information about the incident can be found in [9], [10], [11].

3.1.5.6 Lessons learned

In recent years, there has been a continuous increase in cyberattacks. For this reason, companies and especially critical infrastructures should develop adequate protection mechanisms and train the entire staff, even those who do not deal directly with information systems. This is very important because in many cases the malwares are installed unintentionally by the users through attachments or links. In case of an attack, it is very important that the company does not try to hide the fact but cooperates with the competent authorities so that the incident is dealt with quickly and effectively.

3.1.5.7 Other incidents

The following information is available in Greek at a Wikipedia page [12].

According to the data of the Personal Data Protection Authority, the incidents of breach that have been notified from 25/5/2018 to 24/5/2021 in the context of the obligation of the General Data Protection Regulation (GDPR) are 418. Accordingly, the notifications of data breach in the context of the obligation arising from the electronic communications legislation is 94.

During the period 2008-2010, an incident of breach of personal data of a large number of OTE subscribers took place. Although, it is not established when it occurred, it appears to have occurred at least once, possibly in four different periods. The data concerns over 8,000,000 old or existing subscribers. The data was found after an investigation by the Electronic Crime Prosecution Directorate in 2013, as part of its investigation into the company InfoCredit SA. A fine of 60,000 euros was imposed by the Personal Data Protection Authority for the breach.

In April 2009, four computers were stolen from a unit of the Institute of Children's Health containing sensitive personal health data of 2,050 children.

In 2011, a hacker stole and published online the personal data of 8,500 users from the Greek Sony BMG website.

In August 2013, the Personal Data Protection Authority imposed a fine of 150,000 euros on the General Secretariat of Information Systems, judging that it violated its obligation to take appropriate security measures, which led to a particularly serious incident of personal data breach, i.e. the leakage of data concerning almost all taxpayers in Greece. The leaked personal (tax) data related to at least the years from 2000 to 2012 and included, among other things, tax data, property owners data, data from vehicle registration fees.

In 2013, the Personal Data Protection Authority imposed a fine of 75,000 euros on HSBC bank with its decision no. 109/2013, as in the period 2007-2011, it bought customer lists with personal data from two advertising companies, based on specific criteria.

3.1.6 Germany

This section presents recent data breaches affecting companies involved in the energy distribution in Germany. Since reliable information about the incidents (e.g., by involved authorities) is scarce, the majority of the presented information comes from the affected companies directly (e.g., via their website) or by news reports covering the data breaches. In the following, the TWL data breach in 2020 and the ENTEGA / Count+Care data breach in 2022 are discussed. For both incidents, we will use the term “attacker” (singular) without ruling out that the attack was a coordinated effort of different individuals, as the malicious actor(s) in both incidents have not yet been identified.

3.1.6.1 TWL data breach (2020)

TWL (short for German: “Technische Werke Ludwigshafen am Rhein AG”) is a municipal utility company located in Ludwigshafen, Germany. Among other provided services, it supplies the city of Ludwigshafen with electricity, natural gas, district heat, and drinking water. In 2020, it fell victim to an attack in which personal information of customers, business partners, and employees was attained by the attacker.

3.1.6.1.1 Incident

The attack occurred in the middle of February 2020. The date of detection, as claimed by TWL, was 20.04.2020 [13], [14], [15]. According to different reports, the attacker has gained access to the TWL network via a malicious email attachment, containing the ransomware “Clop” [16]- [17]. During the attack, more than 500 GB of personal information have been captured by the attacker, including names, addresses, mail addresses, telephone numbers, contractual details, and bank connection information for customers, business partners, and employees of TWL and some of its subsidiaries. Roughly 150,000 customers and 1,300 employees were affected by the data breach. The encryption of data on TWL systems via the ransomware as well as unauthorized access to the distributed control system was successfully prevented [15].

On 30.04.2020, the attackers threatened to publish the data on the Darknet, unless a ransom is paid by TWL. The demanded ransom was reported to be in the tens of millions of Euros [13].

On 04.05.2020, TWL published the first press release about the incident [18]. As the reason to why the incident has not been made public directly after discovery, TWL vaguely referred to the forensic investigation, work on their cyber defense system, and investigative tactical reasons. News reports about the incident have been published on various large websites [19], [20], [21].

On 11.05.2020, the attacker started contacting TWL customers affected by the data breach directly via email, alleging TWL of misconduct and lacking cooperation. These emails have been interpreted as an attempt to increase public pressure on TWL to pay the ransom [16].

After TWL further refused to pay the ransom, the attacker reportedly published 18,471 email addresses and 36,411 sensitive customer records on the Darkweb [16].

On 14.05.2020, TWL started to provide information about the potential risks and suggested mitigation measures to customers affected by the data breach.

3.1.6.1.2 Mitigation measures

TWL has reported the incident to the responsible data protection authority of the state Rhineland-Palatinate ("Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz") within the intended 72-hour period after the claimed date of detection. It further directly reported the incident to the respective law enforcement agencies ("Dezernat der Kriminalpolizei" and "Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz") and the Federal Office for Information Security ("Bundesamt für Sicherheit in der Informationstechnik", BSI) [15].

TWL further informed their customers via email, and additionally sent out around 100,000 letters of mostly equivalent content via mail [22]. Additionally, TWL set up a FAQ page about the incident, which, however, only seems to be available in German language. It is available under the following URL: <https://www.twl.de/das-ist-tw/ueber-uns/hackerangriff-faq/>

As part of the FAQ, TWL also provided their customer service contact email address and telephone number. To contact the data protection officer of TWL, these contact details should be used. Despite the warning of high demand and the potential associated delay in response, no separate email address was provided to deal with requests specific to this data breach.

TWL warned their customers about being at an increased risk of identity theft and phishing attempts, as well as a potential increase in spam emails. As mitigation measures, TWL suggested their customers to regularly check for suspicious transfers made from their bank account, to change passwords for all services used to communicate with TWL, and to directly delete emails by unknown senders. TWL further warns that links and attachments in such emails should not be opened under any circumstances [13].

3.1.6.1.3 Consequences

The 2020 activity report for data protection matters in the state of Rhineland-Palatinate devoted a section to this incident [15]. The report was published by the state authority for data protection of the state Rhineland-Palatinate (German: "Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz") in March 2022, roughly two years after the incident.

The report points out that, even though the malicious email attachment was opened by a TWL employee against internal company guidelines, the attack was only possible in the first place, because TWL allowed every employee to execute macros, independently of whether this is required for their work. The report further documents that data of past customers had not been appropriately deleted and locked, resulting in the high number of affected

D6.6 Data breach management plan (V2)

customers. The authority concludes that the investigation into the incident revealed company-wide deficits concerning data protection.

While the investigation by the data protection authority had been concluded in 2020, respective supervisory actions and sentences for TWL were not yet determined [15]. Respective actions were announced for 2021. The activity report for 2021, however, has not yet been published at the time of writing this deliverable.

TWL claims to have invested more than 10 million Euros over a period of 2 years following the incident to improve their IT-structures, as well as their IT-security and data protection measures. In combination with the effects of the Corona pandemic, the data breach was mentioned as a key reason of why TWL made a net income of minus 4.3 million Euros in 2020, compared to a net income of 12.3 million Euros the year before. Even when considering all subsidiaries of TWL, the net income of 2020 was still in the negative range with minus 1.5 million Euros [23].

One and a half years after the incident, the investigation was still ongoing and no attacker was identified [24]. Since then, no further news reports about the incident have been published. According to the current version of the FAQ (last checked: 18.11.2022), the criminal investigation is still ongoing [13].

3.1.6.1.4 Lessons learned

We derive the following relevant points from this specific incident:

- There must be a plan in place to appropriately deal with data of past customers. This plan must also be followed in practice.
- Ransomware attacks should always be also seen as potential data breaches.
- Attackers do also reach out to customers, whose data was affected. In this case, the attacker's intention was not to demand a ransom directly from the customers, but to increase public pressure on the organization, in which the data breach occurred.
- IT-system privileges of employees should be restricted, if they pose a security threat and are not required for day-to-day work. Relying on just IT guidelines is insufficient.
- The respective authorities should be informed as fast as possible after the data breach. This includes data protection authorities in the context of the GDPR, as well as law enforcement authorities and information security authorities.
- The investigation processes after a data breach are lengthy and require a long time.
- Data breaches are expensive.

3.1.6.2 ENTEGA data breach (2022)

An incident similar to the 2020 data breach at TWL occurred in 2022, targeting the IT-service subsidiary Count+Care of the German utility company ENTEGA. The data breach was more widely reported on, since Count+Care also provided services to other critical infrastructure providers, located in different cities.

3.1.6.2.1 Incident

The incident occurred on 12.06.2022. ENTEGA informed the public via Twitter on the same day that a cyberattack occurred, claiming that neither critical infrastructure nor customer data has been affected by the attack [25]. The claim of no customer data being affected later turned out to be wrong [26]. The Tweet further announced that neither the company website nor the email accounts of employees were available. First news reports were published the same day by major German online media such as Heise Online [27], Spiegel Online [28], and FAZ [29].

On 13.06.2022, it became known that also other companies using the services of Count+Care were affected by the attack. In addition to ENTEGA, which is a municipal supplier of electricity, gas, district heat, and water in Darmstadt, also the following companies were affected [30]:

- Stadtwerke Mainz: Municipal supplier for electricity, gas, and water, as well as provider for public transport in Mainz.
- Frankfurter Entsorgungs- und Service GmbH (FES): Public company responsible for waste disposal in Frankfurt. FES further provides waste disposal services to other municipalities in Germany.

In addition, other companies were reported to be affected by the incident, such as Bauverein AG, HEAG mobilio, the HEAG-Holding, and Mainzplus Citymarketing.

On 14.06.2022, it was announced that the attack was caused by ransomware and that the attacker demanded a ransom [31]- [32]. While the demanded ransom was initially kept secret [33], it was later reported to be 15 million Euros [34]- [35]. The attacker threatened that access to the IT-system would remain impossible and that captured data would be published on the Darkweb, unless the ransom is paid. ENTEGA claims that they had no reason to believe that the attacker actually captured data as part of the attack [36]. In this incident, the ransomware was able to make data of the targeted system unavailable. Like the 2020 TWL incident, the ransomware gained initial entry via a malicious email attachment.

On 07.07.2022, it was reported that ENTEGA refused to pay the ransom and that they were able to get their IT-systems running again [34]. ENTEGA further continued to assure that no customer data was affected by the attack at any time.

On 20.07.2022, ENTEGA reported that the attacker has published personal data of customers, employees, and business partners of ENTEGA and its subsidiaries on the Darkweb [26]. This data contained names, addresses, consumption data, data related to payments, and (for some customers) bank connection information [35], [36], [37]. The number of affected individuals has not been published. Different media reports, however, mention it to be in the realm of hundreds of thousands [35], [37].

News reports about the publication of customers data and suggestions how customers could mitigate the effects were published by different media (e.g., [38]). However, following these

reports, not much further information about the data breach was made available as of the writing of this deliverable.

3.1.6.2.2 Mitigation measures

According to ENTEGA, the respective data protection and security authorities were contacted directly after the incident was discovered, and external IT-specialists were assigned to investigate the incident.

Similar to TWL in 2020, ENTEGA set up a FAQ site about the incident, which only seems to be available in German language: <https://www.entega.de/hackerangriff/>

According to this FAQ, ENTEGA contacted customers with an increased risk of negative consequences (e.g., due to the publication of their banking information) individually in written form. ENTEGA further suggested affected customers to delete emails of unknown senders, and to not open any links or attachments in such emails under any circumstances. Other suggested mitigation measures include changing the passwords to all services, which are connected to the online services of ENTEGA, as well as to all services which use the same passwords. ENTEGA reset all passwords to their customer portal. Further, customers should regularly check their bank accounts for suspicious transactions.

To inform the public about potential risks for customers affected by the data breach, ENTEGA named an increased risk of receiving spam and phishing emails, emails which aim to distribute malware, and identity theft. ENTEGA further warns about malicious callers claiming to be ENTEGA employees. To address latter, ENTEGA announced that they will not call customers, unless a customer has initiated contact via phone first, and that ENTEGA will under no circumstances ask for personal access information and/or passwords via telephone, mail, or email.

A free-of-charge telephone hotline was made available on the FAQ for affected customers.

3.1.6.2.3 Consequences

On 14.06.2022, two days after the incident, it was reported that the attack had an influence on public transport in Mainz. Specifically, Stadtwerke Mainz announced that irregularities could occur, causing individual connections to be canceled or delayed. Further, ticket terminals in trams were unavailable. While service for the mobile app could be provided, the website of Stadtwerke Mainz (including ticket sale via the website) was unavailable [39].

As of the writing of this deliverable, the attacker is still unknown and the investigation is still ongoing. There are hence also no reports from authorities like the state authority for data protection yet. Because this incident occurred rather recently, the ultimate consequences for the affected companies and individuals are not known yet.

3.1.6.2.4 Lessons learned

Like the TWL incident, the attack on Count+Care showed that a ransomware attack should always be treated as a potential data breach. In this incident specifically, customers were assured for more than a month after the attack that no customer data has been captured by the attacker, which later proved to be wrong. Further, the incident was caused by a malicious email attachment in both cases.

In contrast to the TWL FAQ, the one provided by ENTEGA addressed the potential threat vector of malicious telephone calls. In both incidents, telephone numbers were among the data captured by the attacker.

Another difference between these two incidents is that ENTEGA informed the public about the data breach directly after the claimed time of detection, while TWL let several days pass before providing their first public statement.

3.1.7 Croatia

In this section, we gather and analyze a recent data breach event in Croatia.

3.1.7.1 Incident

A security incident described as "a cyber-attack" has crippled some business operations at INA Group, Croatia's biggest oil company, and its largest petrol station chain. The attack took place on February 14, at 22:00, the company said. Multiple sources have confirmed that the cyber-attack was a ransomware infection that infected and then encrypted some of the company's backend servers. The incident did not impact the company's ability to provide petrol fuel to its customers, nor its ability to handle payments. It did, however, impact its ability to issue invoices, register loyalty card use, issue new mobile vouchers, issue new electronic vignettes, and allow customers to pay gas utility bills (INA is also a natural gas provider in Croatia). The [INA Group](#), which is part of the MOL Group and lists the Croatian government as its biggest shareholder, publicly disclosed the incident over the weekend [40].

3.1.7.2 Consequence

The ransomware incident has been caused by an infection with the CLOP ransomware strain. Hours before INA reported being infected, a Sophos malware analyst reported a new malware command-and-control server going live and being involved in CLOP-related operations [41].

The use of the CLOP ransomware in the attack against INA also fits the bill when it comes to CLOP's regular modus operandi. According to BleepingComputer, a tech news site specialized in ransomware news and research, the operators of the CLOP ransomware [switched tactics in March 2019](#) from targeting end-users to targeting companies. The CLOP ransomware is now what security researchers call "big-game ransomware," which is a term

referring to criminal groups that specifically target companies to infect their networks, encrypt data, and ask for extremely large ransom demands.

3.1.7.3 Mitigation measures

To prevent the damage that such a virus can cause to the system, CERT recommends taking several preventive measures, such as regularly updating the operating system and installed applications, being careful when opening unknown emails or messages with suspicious content, and a special warning is highlighted in red: The most effective way to defend against ransomware is the periodic creation of backup copies of data (backup) on separate servers, and in the case when backup copies of files are stored on an external (external) disk, that disk must be disconnected (separated) from the computer system immediately after the files are stored on it, as a malicious virus it would not detect and "lock" that disk either.

3.1.7.4 Lessons learned

Make sure the software on all servers is up to date with the latest security patches. We need to use tools that can automatically roll out patches as well as identify known vulnerabilities. Separating data from Internet-facing systems is also a good practice. We need to architect systems so we can put another layer of security that is hard to break through—maybe a different level of authentication—between the servers that run things and data [42].

Six key lessons learned:

1. Invest in secure systems (password security, team education)
2. Do what's right, even if it's unpopular
3. Bring in specialists
4. Have a back-up plan
5. Communicate early and often
6. Make friends with the media

4 Guidelines for data breach management plan

In this chapter, we draw together all the analysis and learnings from the previous chapters and try to establish guidelines for data breach management plan and best practices. The existing frameworks and best practices of the recent data breach incidents are briefly compared to see if there is a working pattern or best practises to follow and document as a common management plan for the chapter 5.

4.1.1 Comparison of the existing frameworks

In chapter 2, four existing frameworks for data breach management in different countries including Finland, Germany, Greece and Italy have been reviewed. Here in the section, the four frameworks are briefly compared. The following items are the main conclusions drawn by comparing the national frameworks:

- Usually, national authorities have high-level recommendations as well as detailed guidelines and standards. The high-level recommendations include more general rules which are applicable to almost every company and any type of incident. The detailed guidelines and standards usually focus on some aspects of data security and might be applicable to some specific sectors.
- The national authorities focus on both organizational and technical measures. The organizational measures mainly focus on relevant roles and responsibilities and non-technical recommendations like keeping calm when facing an incident. The technical measures cover main technical activities enhancing data security in an organization such as maintaining backups and controlling logfiles.
- The Finnish and the Italian authorities provided frameworks with different steps for data breach incident management. The two frameworks and a combination of them are provided in the following figure:

D6.6 Data breach management plan (V2)

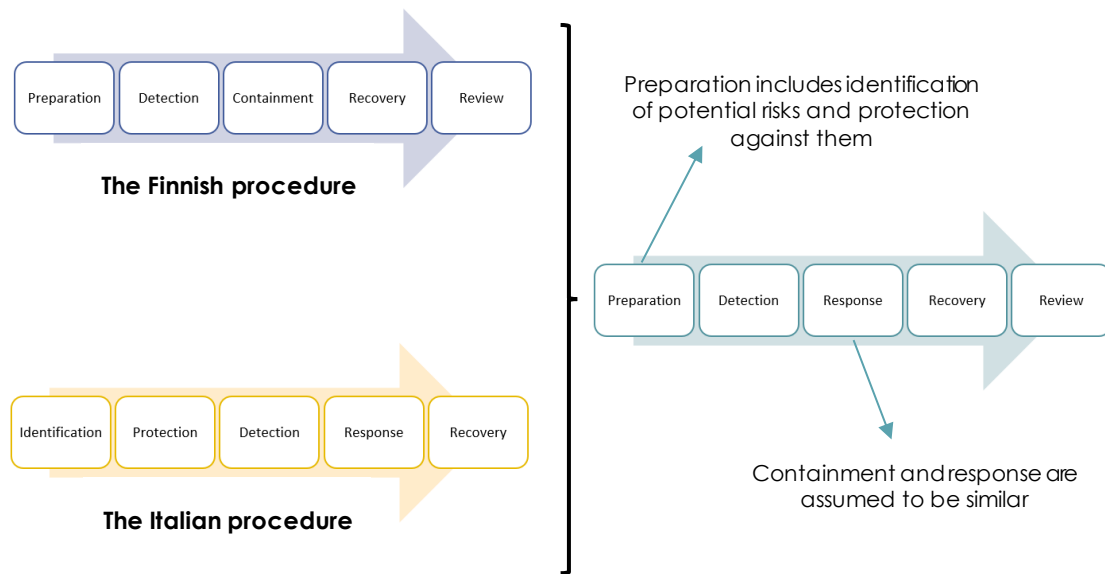


Figure 3 Combined procedure for data breach management

The German authority provides a printable card with the most important points for every employee to know. The card can be filled for each employee before the incident. The employee can consider the card as a guideline to follow during an incident.

- The German authority provides four detailed standards as follows:
 - Information Security Management System which describes general methods for designing a basic information security management system
 - "IT-Grundschutz" Methodology which focuses on the deployment of an information security management system in an organization
 - Risk Analysis based on "IT-Grundschutz" which provides a risk analysis procedure from identification of potential threats to the emerging integration of additional safeguards into the security concept
 - Emergency Management which covers procedures for managing IT-emergencies to ensure business continuity
- The Italian authority provides a framework for enhancing risk management procedure in organizations. The framework helps organizations in defining an implementation program to achieve their security goals. In the framework, evaluating risk management level of an organization is followed by assessing priority and maturity of different measures. In prioritizing the measures, effectiveness of the measure and simplicity of its implementation are considered. In assessing maturity of a measure, maturity of the related technologies as well as the amount of resources have been spent on the implementation of the measure are considered.

4.1.2 Best and worst practices of recent data breach incidents (Updated)

In chapter 3, several data breach incidents recently happened in different European countries have been reviewed. The best and worst decisions and practices drawn from analyzing the data-breach incidents studied in the above are listed here:

The list below was updated after reviewing the incidents for this revised version of the deliverable.

- In some cases, occurrence of the incident led to reviewing relevant activities and rules aiming at enhancing data security
- In most of the incidents, the affected organization provided relevant and timely advices for individuals whose personal data is compromised to limit consequences of the incident
- In most of the incidents, the affected organization filed a report as soon as the incident was noticed. This can help in finding the attacker, limiting the consequences and returning to the normal service as early as possible. Hiding an incident may lead to significantly more severe consequences both for the organization and the individuals whose information is compromised
- In most of the incidents, the affected organization received support from government and other organizations to reduce the consequences
- Effective victim support services like free-of-charge hotlines for FAQs can alleviate consequences of the incidents
- All software packages on all servers should be up to date with the latest security patches to enhance data security
- In case of an incident, the respective authorities including data protection authorities, law enforcement authorities and information security authorities should be informed as fast as possible
- IT-system privileges of employees should be restricted if possible prevent their security threat
- In many cases, attackers try to reach out to affected customers either to demand a ransom directly or to increase public pressure on the organization
- An appropriate plan for dealing with past customer data or unnecessary data is needed to limit consequences of a data leak
- Automated notification messages like exceeding the capacity limit of server data storage disk should be given thorough
- It is likely that an attacker use the information and data leaked during an incident to initiate another incident. So, it is very important to ensure security holes are cleared and compromised credentials are reset after recovery from a data leak incident
- It is important to raise employees' awareness of potential risks and also incident management procedures since they play a huge role in preventing data breaches and limiting their consequences

D6.6 Data breach management plan (V2)

- Regular risk assessment should be conducted to ensure that cyber-security strategy is up to date and organization changes (which can lead to new risk factors) and new potential threats are considered
- Frequent data backups and efficient disaster recovery plans are necessary to maintain cyber-security and ensure data security. The plans are to assist the party in planning and determining who in the organization has operational responsibility for managing the security breach and whether the incident will be reported up the hierarchy, and if so, how
- Data encryption and anonymization in addition to access control and limit must be applied to ensure security of sensitive data
- Relevant activities must be documented to enable supervisory authorities to verify compliance with regulations
- More focus should be given to securing supply chain with stricter requirements for contractors and service providers

5 Common Model for data breach management (NEW)

In Chapter 4, a common five-step procedure was suggested by combining lessons learned from the existing frameworks. This chapter provides description of common model for data breach management for EPES operators. A brief description of the 5 steps (preparation, detection, response, recovery, review) included in the Common model for Data breach management is provided in Section 5.1, which are then demonstrated as in a practical example in Section 5.2. This is the outcome of the research done in Task 6.3.

EPES operates in the cyber-physical world, whereas digital action can have physical reactions. Therefore, understanding the nature of this cyber-physical realm is relevant to all participating in EPES operations. However, this common model described here can be valid and useful for other industries as well – not just for EPES operators. As mentioned, cyber-physical nature requires more careful planning in cybersecurity and understanding of cross-linkages between systems and hardware. A breach in the system can cause actual damage to hardware by unlawful actions. Take for example a breach in the TSO datahub, where customer contracts and metering data are held. An attacker could potentially connect to the electricity meter of unexpected customer and disconnect them from the power grid. This action could lead to serious damage to the end customer. In preparation for breach incident, EPES operator should be aware of different scenarios affecting the physical world.

5.1 Description of Common Model and steps

This section and sub-sections describe five steps of the common model for data breach management. Figure 4 depicts the common model and different actions suggested in each step. Each action is explained in more detail below.

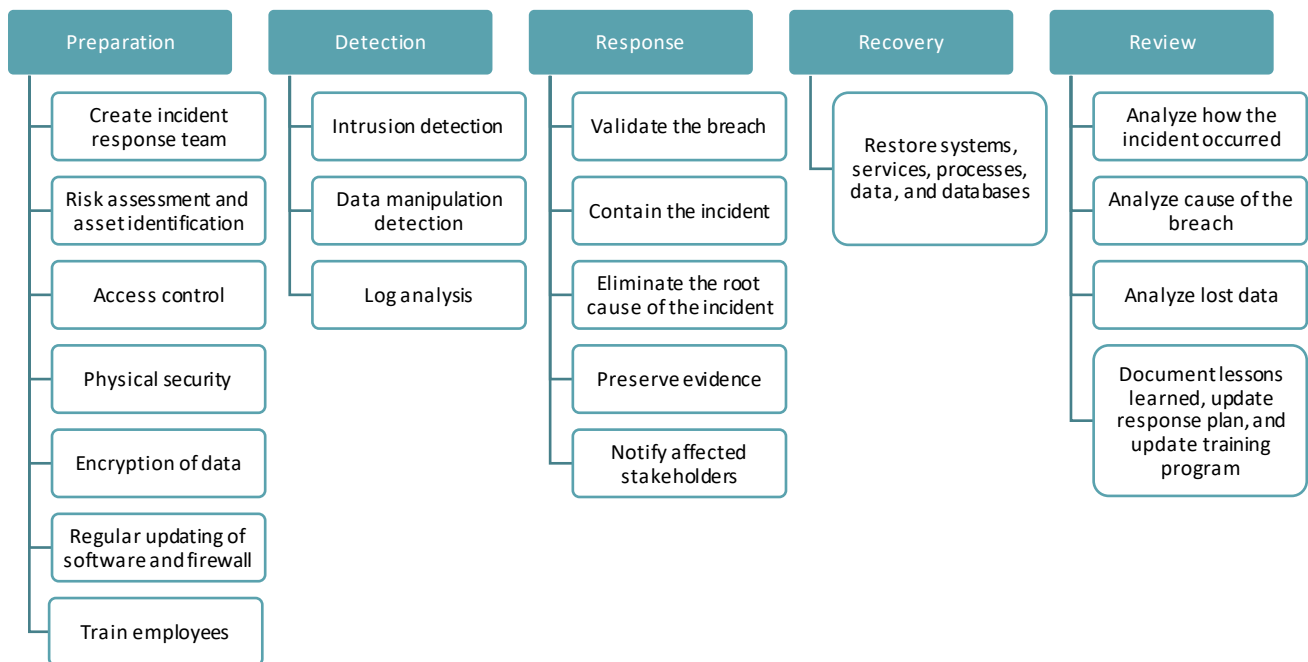


Figure 4 A Common model of data breach management describing steps

5.1.1 Preparation

Preparing for the incident is the first step in defence. Hacking is the most obvious cybersecurity threat, which can be further described by different attack methods, such as phishing, malware, data poisoning and manipulation, DDoS, and social engineering. Any attack regarding its method can lead to data breaches, which can be categorized as follows: confidentiality breach (private information is disclosed without owner's consent), integrity breach (unauthorized data manipulation), and availability breach (loss of access to the data).

The most concise approach for preparation is to develop a **response plan**. The response plan should include procedures for containing the breach, notifying affected parties, and restoring systems. This includes identifying the types of data and assets that are at risk and assessing the potential impact of a breach. The response plan should address all the steps included in the common model of data breach management.

The preparation step includes the following actions:

D6.6 Data breach management plan (V2)

1) Create an incident response team

The response team should comprise all necessary stakeholders from different departments, such as IT, legal, communications, and management.

2) Risk assessment and asset identification

Identify the potential risks and vulnerabilities of the system. Identify assets such as software and hardware and identify where sensitive information resides. In EPES domain, pay attention to cyber-physical assets. Prepare for different types of attacks and analyze weaknesses to different attacks.

3) Access control

Restrict access to the system to authorized personnel only.

4) Physical security

Protect computers and other assets by restricting physical access. In EPES, this is also mandatory by safety standards not to let outsiders have access to electrical equipment in restricted areas.

5) Encryption of data

Use encryption to protect data. Use a virtual private network (VPN) in data transmissions.

6) Regular updating of software and firewall

Software updates often include security patches that address known vulnerabilities, while firewalls help to prevent unauthorized access to the system.

7) Train employees

Have a regular employee training program for cybersecurity threats and have a response plan ready.

5.1.2 Detection

This step involves identifying the type of breach, the extent of the damage, and the data involved. Detection can be done through various methods, such as intrusion detection systems, log analysis, and network monitoring. It is essential to have a system in place that can detect a breach as soon as possible to minimize the damage.

The detection step includes the following actions:

1) Intrusion detection

Use an Intrusion detection system (IDS) to monitor incoming and outgoing network traffic for any unauthorized access or malicious activity.

2) Data manipulation detection

Data analysis tools help identify patterns and anomalies in data that may indicate unlawful manipulation.

3) Log analysis

Most modern software includes logging to track user access and events. Therefore, logs keep track of incidents, which can be detected and audited with log analysis tools.

5.1.3 Response

Response step includes containing the breach, preserving evidence, and notifying affected parties including individuals, regulators, and other stakeholders. It is crucial to have a clear and concise response plan in place to ensure that the response is effective.

The response step includes the following actions:

1) Validate the breach

Validate whether the breach has occurred, and it is not just a false flag. Refer to the last step and validate events from the system log.

2) Contain the incident

In case of an incident, first priority is to block malicious traffic and isolate the system affected by disconnecting the network connection, thus preventing any spread of contamination.

3) Eliminate the root cause of the incident

Identify the origin of the incident to prevent any further attacks.

4) Preserve evidence

Unlawful data breaches are criminal acts, for which perpetrators should be prosecuted accordingly. Evidence is necessary not just for criminal cases, but for understanding the attack and the vulnerability exploited.

5) Notify affected stakeholders

Depending on the breach and its severity, different stakeholders have to be notified. For a minor breach – not affecting customers, internal stakeholders need to be informed of actions. If customer data is compromised, the breach is much more critical, and customers must be informed. In communications with customers, it is necessary to be transparent about the incident and provide a corrective plan. In some cases, the national Computer Emergency Response Team (CERT) must be informed, and incident be reported. Find out more about reporting to CERT in CyberSEAS deliverable D6.7 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents.

5.1.4 Recovery

Recovery step involves restoring systems, processes, data, and services to their pre-breach state. It is essential to have a backup plan in place to ensure that data can be recovered in case of a breach or any other reason.

The recovery step includes the following action:

1) **Restore systems, services, processes, data, and databases**

Restore systems affected and data from backups that are not infected. As always, it is advisable to have backups as often as possible. In EPES, hardware equipment can also be infected or damaged, which might lead to replacement or repair, thus understanding cyber-physicality is required.

5.1.5 Review

Review step involves reviewing the incident and taking corrective actions. Review includes analyzing the cause of the breach, identifying areas for improvement, and updating the response plan. It is essential to learn from the incident to prevent future breaches and attacks.

The review step includes the following actions:

1) **Analyze how the incident occurred**

Begin with: what happened, when it happened, and how it happened.

2) **Analyze the cause of the breach**

Analyze what was the root cause: lack of security procedures, exposed firewall, lack of anti-virus etc.

3) **Analyze lost data**

Analyze the data stolen or destroyed. How important and how valuable was the data for the company and for customers.

4) **Document lessons learned, update response plan, and update training program**

Finally, without lessons learned, your organization is exposed to similar and also to other types of incidents. Update your response plan, strategies, and security controls. Update information security and training programs accordingly.

Documenting response and recovery steps is crucial in incident handling procedures to mitigate similar types of incidents. Updates in response plans, strategies, and security controls can be documented as cybersecurity playbooks. The playbooks can include all the steps from preparation to recovery. The need for standardized documentation is evidenced by the development of response modelling and standardized specifications such as the Collaborative Automated Course of Action Operations (CACAO) [43] playbooks.

Response modelling can be done with the aid of BPMN [44] provides a structured and efficient approach to formulate the steps. BPMN serves as a graphical language for business process representation across various domains. The key features of BPMN include its graph-based representation of workflows, which simplifies complex processes and aids in visual analysis towards structuring the playbooks instead of unstructured text guidelines. The human- and machine-readability of playbooks not only facilitates understanding and communication of workflows but also supports automated workflow management. In cybersecurity, BPMN is widely used for creating repeatable procedures for detecting, responding to, and recovering from incidents. This standardization enables better coordination and effectiveness in incident response.

CACAO specification, with its latest version released in November 2023, further emphasizes the importance of standardized response documentation. CACAO playbooks, which can be either executable or templates, offer structured steps for handling security incidents. These playbooks, categorized into detection, mitigation, and remediation, are crucial in the incident management lifecycle. The CACAO specification details the playbook structure, emphasizing the importance of metadata, workflow steps, and data models for efficient execution and automation. Furthermore, the integration of the SAPPAN playbook management tool [45] demonstrates the importance of having a knowledge repository and sharing functionality to communicate the lessons learned between organizations. This tool simplifies the process of capturing, managing, sanitizing, and sharing playbooks. This highlights the collaborative and dynamic nature of incident response in the modern cybersecurity landscape.

5.2 Practical example

As part of the tool's validation, a demonstration in the Finnish pilot was conducted, which included project partners Enerim, Synelixis, and Guardtime. This demonstration is described here as a reference and as a practical example of, how a company can use different tools and the common model framework to address data breach vulnerability and incident.

In the demonstration Enerim provided the background story and the demonstration setup, where a data breach incident was simulated. Synelixis developed and provided assistance with the use of CVIAT threat assessment tool and Guardtime developed MIDA tool to be used in the demonstration. This demonstration provides an example of how five steps of the common model framework were conducted: preparation using the CVIAT tool, detection using the MIDA tool, incident response and reporting to the national CERT, recovery step, and review of the incident.

5.2.1 Demonstration – Background

The background of the demonstration is as follows. Briefly, Enerim is a Customer Information System (CIS) technology supplier and a service provider to utilities and energy retailers. As an

EPES operator, Enerim is aware of the important role of cybersecurity in daily operations and its effect on the power grid and end users. Enerim's CIS provides contractual information to the utilities and generates invoices for the end customers of energy or electricity users. The value chain from the meter to the invoice requires many steps involving data handling by different systems and operations including the Datahub (common dataspace for energy) of Fingrid. Enerim has prepared a **response plan** for data breaches and has decided to incorporate Synelixis provided Common Vulnerability Assessment Tool (CVIAT).

5.2.2 Demonstration – Preparation

As part of the preparation, Enerim has decided to investigate different threats and vulnerabilities of different assets. For this, Synelixis CVIAT threat assessment tool is incorporated enabling the creation of assets, the correlation of assets with potential vulnerabilities, the assessment and reassessment, e.g. after the implementation of relevant mitigation measures that decreases the security exposure, of vulnerabilities. See more about the CVIAT in CyberSEAS deliverable D5.8 Proactive security for energy operators (v2). Additionally, the CVIAT enhances data transferability, interoperability, and standardization for cyber threat intelligence, among its functionalities, by supporting the export (and import) of cyber threat data into the STIX format, a widely adopted standard in this domain. In this manner, widely utilised elements are modelled as STIX objects, like Organisation, Infrastructure/Asset, Vulnerability, Score, together with the relevant relationships between them. This feature facilitates collaboration and information sharing within the cybersecurity community (either within a specific organization or among different organizations/authorities), with the contribution to the implementation and maintenance of more secure systems.

For demonstration purposes, Enerim analyzed a few possible threats and created assets in CVIAT accordingly. In Figure 5, assets are illustrated in the form of a network graph of STIX objects, representing the Organisation (gray color), the assets (light blue) and their respective vulnerabilities (red (High), orange (Medium) and yellow (Low)). Additionally, Figure 6 depicts the CVIAT Dashboard, which provides a summarised overview of the vulnerable assets, together with analytical information.

D6.6 Data breach management plan (V2)

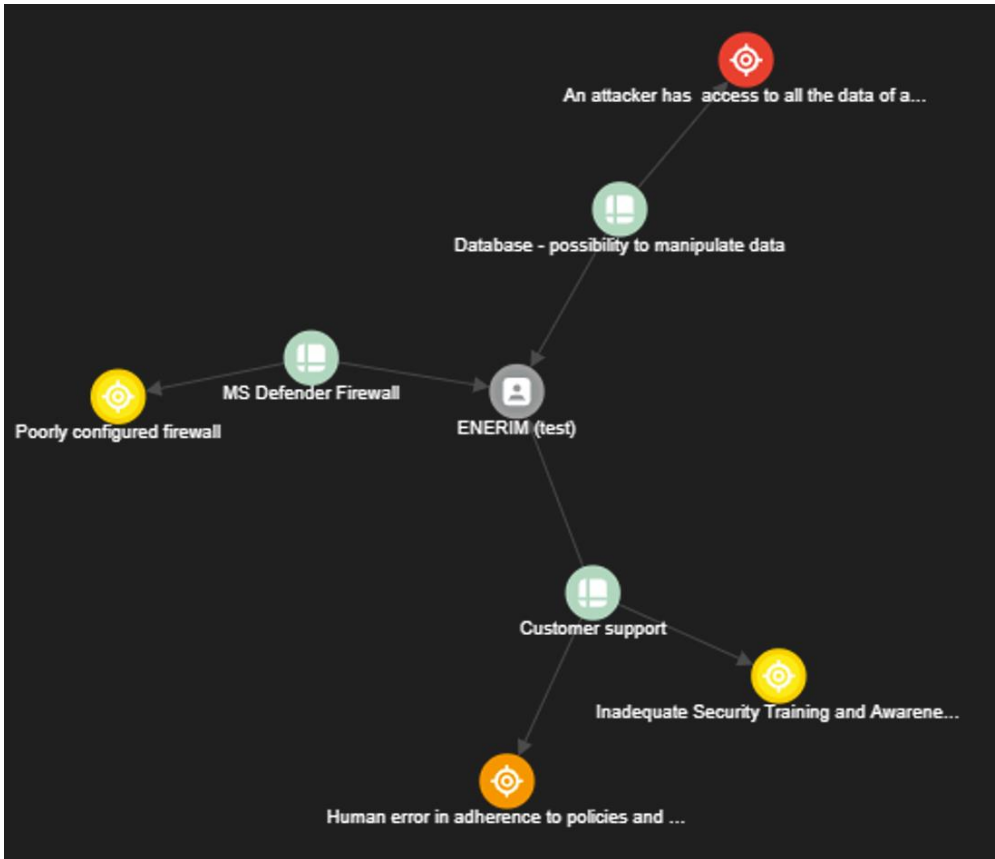


Figure 5 Different assets created in the CVIAT

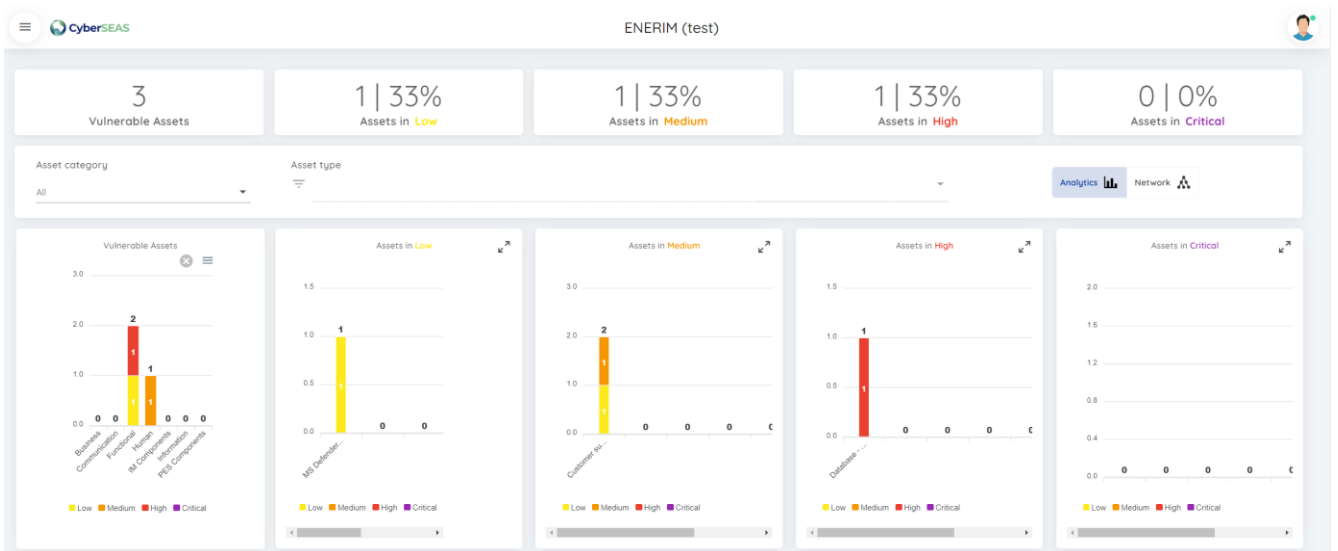


Figure 6 Assets dashboard depicting different levels of threats

Figure 7 shows the initial threat assessments for database and human factors. This reflects the score of those two vulnerabilities (5.3 and 2.4), as initially assessed, without considering any CyberSEAS mitigation actions.

D6.6 Data breach management plan (V2)

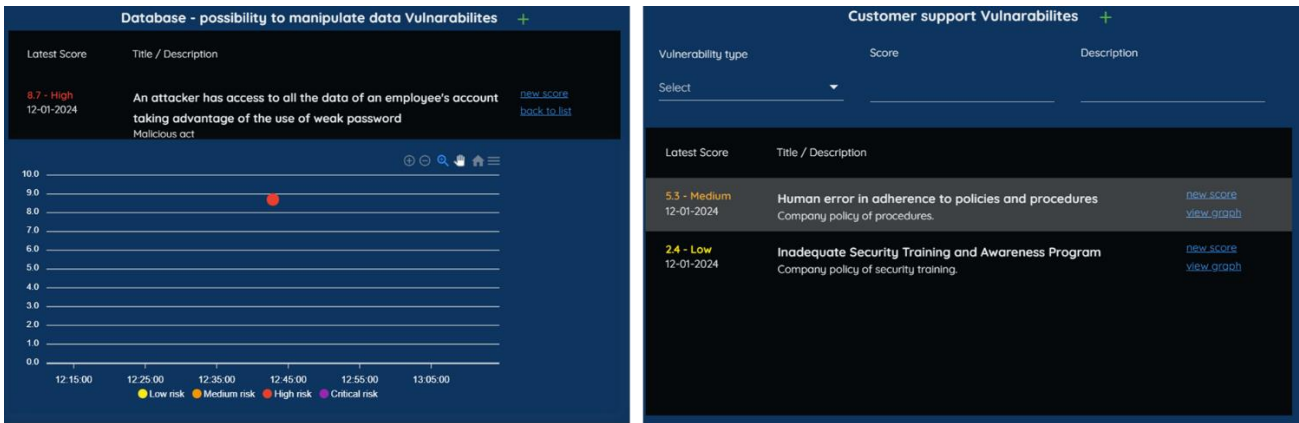


Figure 7 Initial threat assessments for database and human factors

As a result of High and Medium threat assessments, Enerim decided mitigation actions for employee training and also decided to acquire Guardtime's MIDA tool for metering data validation process. After implementing MIDA tool, as mitigation action, Enerim's cybersecurity officer reassessed the severity of the previously identified vulnerabilities, suggesting to lower the threat level accordingly, shown in Figure 8, as a consequence of the implemented mitigations.

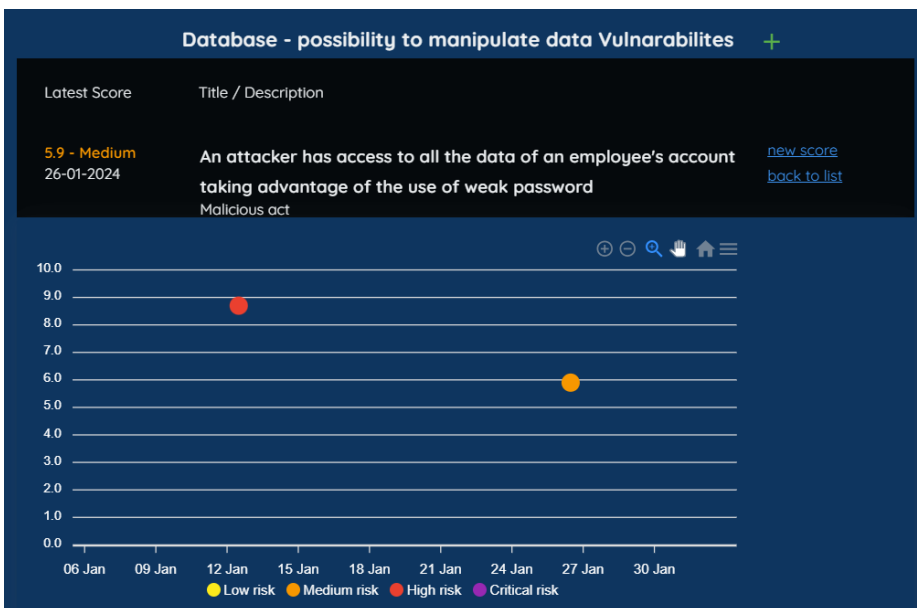


Figure 8 Re-evaluation of threat level

5.2.3 Demonstration – Detection

Guardtime's MIDA tool is designed to monitor Enerim's database integrity. With the limitations and requirements (no direct communication with either EDM or CIS databases during the PoC) that the use-cases have, the tool is being adapted to accept metering from two

D6.6 Data breach management plan (V2)

different inputs in order to either sign or to validate the CIS database integrity, as shown on Figure 9.

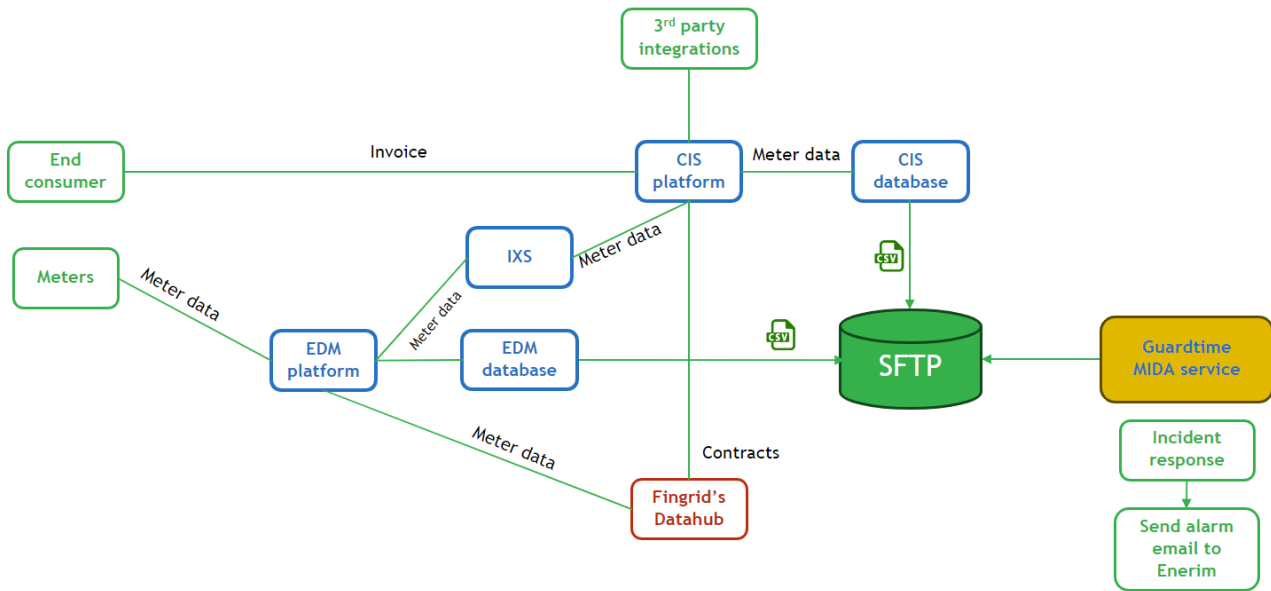


Figure 9 MIDA tool implementation to CIS platform

The platform is operating with CSV file formats and therefore MIDA tool also accept inputs in CSV file format where it can hold one to multiple measurements. The transfer of CSV to MIDA tool comes from EDM and CIS and was conducted through SFTP server using two distinct paths to separate inputs for signing and validation. This specific file transfer method is the preferred approach for Enerim and therefore a support implementation would be added to the MIDA tool.

First input to the MIDA tool comes from EDM which is also sent in parallel to CIS for storage and further processing. This input is regarded by the MIDA tool as the input to the database and thus signed to later validations. This input reading from SFTP is configurable to adjust delays, how often it is attempted, and whether inputs are to be removed upon successful registration. During the signing process each metering data reading must be uniquely identified and therefore for each of the measurements MIDA tool derives a unique identifier and calculates hash imprints for the whole measurement rows that are then signed and stored in the tool for later usage and validations.

Second input comes from the CIS component that sends the database query result from CIS database to the MIDA tool for validation. This input reading is also configurable to adjust delays, how often it is attempted, and whether inputs are to be removed once validation reports are sent. The MIDA tool takes each of the measurements from the input file(s) and compares whether such input, based on a derived unique identifier, has been already registered by the tool and validates the integrity of the whole measurement. The MIDA tool is internally continuously monitoring each registered identifier, hash imprints and blockchain proofs but verification of those are also triggered when input for validations has been provided.

D6.6 Data breach management plan (V2)

MIDA tool is being designed to generate validation reports on each validation input file that is sent to a configured email address. These reports can be sent in all cases, regardless if there were no errors in the validation process (Figure 10) or integrity validation errors or not signed entries (Figure 11). The validation report would include information about

- The file name that was provided (helps to identify the provided dataset),
- How many of these measurements were registered in the database,
- How many of those were valid (integrity is intact), and
- How many of the associated signatures could be verified against the blockchain.

Validating 7 metering data rows from SFTP path /ValidationInput/CISmeterdata_07_11_2023.csv.

Validated metering data was contained in 1 unique blocks.

Row validation result:

7/7 metering data rows were valid.

Block validation results:

7/7 rows contained a matching block in database.

1/1 blocks had a valid signature.

Figure 10 Example of validation results with OK results.

Additionally, in case of the failed verification, two files are also attached to provide outtakes on the specific entries, one for those that did not pass the integrity validation and another for entries that were not registered, for further inspection and analysis.

D6.6 Data breach management plan (V2)

Validating 7 metering data rows from SFTP path /ValidationInput/CISmeterdata_08_11_2023.csv.
Validated metering data was contained in 2 unique blocks.

Row validation result:
2/7 rows failed validation.

Block validation results:
1/7 rows did not contain a matching block in database.
2/2 blocks had a valid signature.

2 attachments • Scanned by Gmail ⓘ

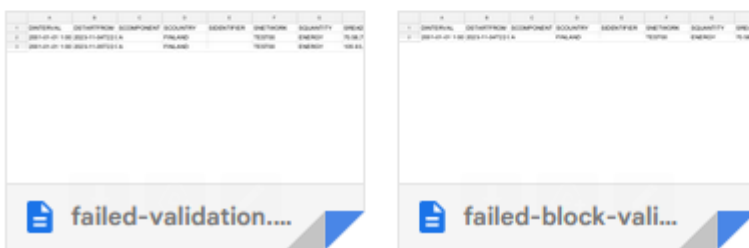


Figure 11 Example of validation results with failure and errors.

MIDA tool deployment and testing will be presented in D4.4 “Complex cyber-attacks detection tool” and validation and evaluation under WP7’s related deliverables.

5.2.4 Demonstration – Response

In the demonstration, MIDA tool detected inconsistency in one metering series, which caused an alarm email to be sent to Enerim. Following actions of the response step shown in Figure 12 were taken.

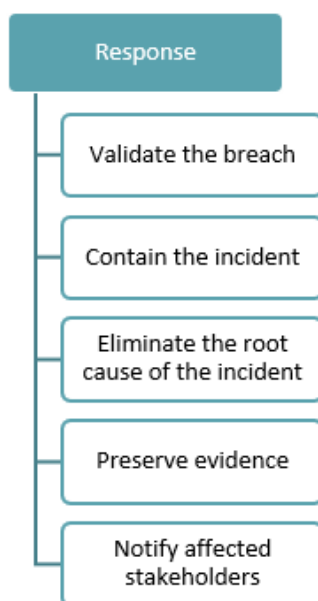


Figure 12 Response step

Enerim **validated** the alarm and analyzed log files, which confirmed the data breach incident. Further investigation confirmed database tampering affecting one metering series. The incident was **contained** by disconnecting any outside connections and restricting access to the database. User credentials were revoked and new credentials and passwords for authorized users were created.

In this demonstration, threat agent and root cause are considered to be according to Finnish pilot Scenario 1, which is discussed more in the validation work of the CyberSEAS demonstrations in Work Package 7. Understanding the root cause of the breach, the vulnerability of the system was **eliminated**.

The log files were saved and **evidence** of the breach preserved. These log files would be later used in the post incident review to re-create the data breach incident.

After the incident, Enerim contacted National Cyber Security Centre Finland (NCSC-FI) for the incident reporting. In this case, incident was **notified** by filling a data breach web form. Additionally, other stakeholders were informed of the incident e.g. internal business stakeholders, energy retailer, DSO, and customer affected.

In case of cyber attack to a critical infrastructure such as energy infrastructure, it is mandatory to report to the NCSC-FI of the incident. NCSC-FI's reporting template of the data breach form is shown in the CyberSEAS deliverable D6.7 Rules & Tools for Operators' Coordination and Reporting to CERTs in Case of Incidents.

5.2.5 Demonstration – Recovery

A business that relies on handling and storing data, must make sure that the data is recoverable in case of any incident including hardware and software failures or cyberattack.

As in the demonstration, the damage was only for one user, thus the measurement values could be restored by hand. For more serious incident, where large amount of data or the database is compromised, higher level recovery strategy must be implemented. The recovery strategy involves determining recovery techniques, checkpoint backups, checkpoint intervals, and incremental backups. [46] [47]

The starting point of the database recovery is to determine the time the incident, thus recovering only clean data and preserving integrity of the database. In case of database is hosted by cloud service, the customer database would be recovered by informing the cloud database provider of the attack and incident time from which the recovery point would be chosen.

5.2.6 Demonstration – Review

Following the five-steps of the preparation plan, incident response was conducted systemically and accordingly by the plan. In the post incident review, the timeline of the incident and response was re-created step-by-step. This was done to gain more insights about the incident and to understand the processes and people involved.

An example of incident tracking by timestamps (individual timestamps omitted):

[YYYY-MM-DD HH:MM:SS] Threat agent intrusion

[YYYY-MM-DD HH:MM:SS] Threat agent access the database

[YYYY-MM-DD HH:MM:SS] Manipulation of the metering record

[YYYY-MM-DD HH:MM:SS] MIDA tool detecting inconsistency in one record

[YYYY-MM-DD HH:MM:SS] MIDA tool sent an alarm email

[YYYY-MM-DD HH:MM:SS] Email received by the email host

[YYYY-MM-DD HH:MM:SS] Email read by a human

[YYYY-MM-DD HH:MM:SS] Validating the attack

[YYYY-MM-DD HH:MM:SS] Beginning of the response including actions

[YYYY-MM-DD HH:MM:SS] Beginning of the recovery including actions

[YYYY-MM-DD HH:MM:SS] System recovered

The damage was assessed, and no permanent damage occurred. Damage was limited to only one customer record, which was deemed as a minor inconvenience. The root cause for the attack was found and the problem was fixed. The preparation plan was updated accordingly. Lessons learned were shared within the company stakeholders.

Lessons learned included:

D6.6 Data breach management plan (V2)

- The incident response plan was necessary and up to date, but need to be revised after the incident.
- CVIAT risk assesment tool provided meaningful insights of possible vulnerabilities.
- MIDA tool detected database tampering.
- Alarm sent by MIDA was timely and response to the alarm was immediate.
- Log files proved valuable in validating the attack.
- Protection of log files is important and can be assured by: include log of all acces to data, deny tampering and unauthorized access, log change of user rights, automate monitoring of log files.
- Necessity to improve database security by acces restrictions and active monitoring.
- Back-up files were available and timely updated.
- Key employees were trained appropriately and cyber-incident exercise was held.
- A new risk assessment was conducted.

6 Conclusions (Updated)

This document is a deliverable reporting contributions made under Task 6.3 of project CyberSEAS. The document reviewed data breach management frameworks where the recommendations and instructions provided by the national authorities in different countries including Finland, Germany, Greece and Italy are provided. Then, a few recent data breach incidents in different European countries are reviewed. The focus was tried to be on incidents in energy supply chain. In case of no major incident in the domain, incidents in other main infrastructures or other major incidents are reviewed. The aim of the review was to extract the best and worst practices as well as to explain the lessons learned from the incidents. By comparing the data breach management frameworks as well as the data gathered from the incidents and the relevant lessons learned during the studies, a list of recommendations about how to manage data breach incidents is provided. Finally, a common model of data breach management is provided with an example case of a demonstration.

7 References

- [1] [Online]. Available: <https://slo-tech.com/novice/t693532>.
- [2] [Online]. Available: <https://www.cert.si/si-cert-2017-01/>.
- [3] [Online]. Available: <https://www.lifo.gr/now/tech-science/hackers-dierreysan-dedomena-poy-ishyizontai-oti-ypeklepsan-apo-tin-kybernoepithesi>.
- [4] [Online]. Available: <https://www.tovima.gr/2022/08/23/finance/desfa-krisima-eggrafa-sto-dark-web-meta-fin-kyvernoepithesi-fovoi-gia-diarroi/>.
- [5] [Online]. Available: <https://www.kathimerini.gr/society/562008733/oi-chaker-piso-apo-tin-epithesi-ston-desfa/>.
- [6] [Online]. Available: <https://www.bleepingcomputer.com/news/security/greek-natural-gas-operator-suffers-ransomware-related-data-breach/>.
- [7] [Online]. Available: <https://www.radiflow.com/blog/behind-the-news-the-ragnar-locker-attack-on-greek-natural-gas-supplier-desfa/>.
- [8] [Online]. Available: <https://heimdalsecurity.com/blog/desfa-suffers-cyberattack-ragnar-locker-ransomware-claims-responsibility/>.
- [9] [Online]. Available: <https://www.businessnews.gr/epixeiriseis/item/238436-adae-prostimo-3-2-ekat-evro-se-cosmote-gia-diarroi-prosopikon-dedomenon>.
- [10] [Online]. Available: <https://www.lifo.gr/now/greece/prostima-6-ekat-eyro-se-cosmote-kai-325-ekat-ston-ote-gia-diarroi-dedomenon-syndromiton>.
- [11] [Online]. Available: <https://www.dikastiko.gr/eidhsh/prostimo-mamoyth-9-250-000-eyro-se-cosmote-kai-ote-gia-diarroi-dedomenon-syndromiton-toys-to-deytero-megalytero-meta-apo-ta-73-ekatommyria-eyro-sti-vodafone-gia-tin-ypothesi-tsalikidi/>.
- [12] [Online]. Available: https://el.wikipedia.org/wiki/%CE%A0%CE%B1%CF%81%CE%B1%CE%B2%CE%AF%CE%B1%CF%83%CE%B7_%CE%B4%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD.
- [13] [Online]. Available: <https://www.twl.de/das-ist-tw/ueber-uns/hackerangriff-faq/>.
- [14] [Online]. Available: https://www.rheinpfalz.de/lokal/ludwigshafen_artikel,-was-die-tw-ihren-kunden-nach-dem-hackerangriff-raten-_arid,5065241.html.
- [15] [Online]. Available: https://www.datenschutz.rlp.de/fileadmin/lfdi/Taetigkeitsberichte/ds_tb29.pdf.

- [16] [Online]. Available: <https://heise.de/-4720113>.
- [17] [Online]. Available: <https://www.spiegel.de/netzwelt/technische-werke-ludwigshafen-von-hackern-erpresst-millionenbetrag-gefordert-a-4eb288a3-5f53-44db-99d9-60f46de529f3>.
- [18] [Online]. Available: https://www.twl.de/das-ist-tw/Newsroom/news/detail?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=152&cHash=d83f78fea835ac677037513eef9a8a09.
- [19] [Online]. Available: <https://heise.de/-4714059>.
- [20] [Online]. Available: <https://www.sueddeutsche.de/panorama/kriminalitaet-ludwigshafen-am-rhein-hackerangriff-auf-technische-werke-ludwigshafen-dpa.urn-newsml-dpa-com-20090101-200504-99-929440>.
- [21] [Online]. Available: https://www.rheinpfalz.de/lokal/pfalz-ticker_artikel,-hackerangriff-auf-tw-kundendaten-gestohlen-_arid,5061178.html.
- [22] [Online]. Available: https://www.rheinpfalz.de/lokal/ludwigshafen_artikel,-nach-hacker-angriff-rund-100-000-tw-kunden-werden-per-brief-informiert-_arid,5068833.html.
- [23] [Online]. Available: https://www.twl.de/fileadmin/user_upload/twl/02_Dokumente/01_unternehmen/01_geschaeftsberichte/WEB_TWL_Gescha__ftsbericht_2020_final.pdf.
- [24] [Online]. Available: https://www.rheinpfalz.de/lokal/ludwigshafen_artikel,-twl-hackerangriff-spuren-f%C3%BChren-ins-ausland-_arid,5267316.html.
- [25] [Online]. Available: <https://twitter.com/Entega/status/1535978377034747906>.
- [26] [Online]. Available: <https://www.entega.ag/aktuelles-presse/pressemeldungen/pressemeldung/daten-von-cyberkriminellen-ins-darknet-gestellt/>.
- [27] [Online]. Available: <https://heise.de/-7138161>.
- [28] [Online]. Available: <https://www.spiegel.de/netzwelt/entega-hackerangriff-beim-darmstaedter-energieversorger-a-41ef0e01-943d-4a5a-99de-5c9b0541c1b2>.
- [29] [Online]. Available: <https://www.faz.net/aktuell/rhein-main/hackerangriff-auf-darmstaedter-energieversorger-entega-18098072.html>.
- [30] [Online]. Available: <https://www.golem.de/news/entega-weitere-unternehmen-von-hackerangriff-betroffen-2206-166087.html>.

- [31] [Online]. Available: <https://www.hessenschau.de/wirtschaft/entega-fes-mainzer-stadtwerke-it-dienstleister-wird-von-hackern-erpresst,entega-hack-100.html>.
- [32] [Online]. Available: <https://heise.de/-7140974>.
- [33] [Online]. Available: <https://www.hessenschau.de/wirtschaft/entega-systeme-laufen-nach-hackerangriff-wieder-normal,kurz-entega-100.html>.
- [34] [Online]. Available: <https://www.hessenschau.de/wirtschaft/nach-cyberattacke-auf-darmstaedter-energieversorger-15-millionen-euro-loesegeld-gefordert---entega-zahlte-nicht,entega-loesegeld-nicht-gezahlt-100.html>.
- [35] [Online]. Available: <https://www.spiegel.de/netzwelt/web/hacker-veroeffentlichen-kundendaten-von-hessischem-energieversorger-a-3deda450-3193-49ad-bae9-ee581cf64928>.
- [36] [Online]. Available: <https://www.entega.de/hackerangriff/>.
- [37] [Online]. Available: <https://www.swr3.de/aktuell/nachrichten/hackerangriff-daten-mainzer-stadtwerke-entega-100.html>.
- [38] [Online]. Available: <https://heise.de/-7186378>.
- [39] [Online]. Available: <https://www.swr.de/swraktuell/rheinland-pfalz/mainz/hackerangriff-trifft-mainzer-stadtwerke-100.html>.
- [40] [Online]. Available: <https://www.zdnet.com/article/croatias-largest-petrol-station-chain-impacted-by-cyber-attack/>.
- [41] [Online]. Available: <https://t.co/OJluaAPeLV>.
- [42] [Online]. Available: <https://www.finalsite.com/blog/p/~board/b/post/ransomware-lessons-learned>.
- [43] [Online]. Available: <https://docs.oasis-open.org/cacao/security-playbooks/v2.0/cs01/security-playbooks-v2.0-cs01.html>.
- [44] [Online]. Available: <https://www.omg.org/spec/BPMN/2.0/PDF>.
- [45] A. M. J. P. R. S. D. Mehdi Akbari Gurabi, "SASP: a Semantic web-based Approach for management of Sharable cybersecurity Playbooks.," In Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22)., 2022.
- [46] IBM, "Database recovery strategy," [Online]. Available: <https://www.ibm.com/docs/en/configurepricequote/9.4.0?topic=strategies-database-recovery-strategy>.
- [47] IBM, "Developing a backup and recovery strategy," [Online]. Available: <https://www.ibm.com/docs/en/db2/11.5?topic=recovery-developing-backup-strategy>.

