CERT participation in incident handling related to the Article 4 obligations

Toolset, Document for students

September 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Acknowledgements

Contributors to this report

We would like to thank all our ENISA colleagues who contributed with their input to this report and supervised its completion, especially Lauri Palkmets, Cosmin Ciobanu, Andreas Sfakianakis, Romain Bourgue, and Yonas Leguesse. We would also like to thank the team of Don Stikvoort and Michael Potter from S-CURE, The Netherlands, Mirosław Maj and Tomasz Chlebowski from ComCERT, Poland, and Mirko Wollenberg from PRESECURE Consulting, Germany, who produced the second version of this documents as consultants.

Agreements or Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors: Anna Felkner, Tomasz Grudzicki, Przemysław Jaroszewski, Piotr Kijewski, Mirosław Maj, Marcin Mielniczek, Elżbieta Nowicka, Cezary Rzewuski, Krzysztof Silicki, Rafał Tarłowski from NASK/CERT Polska, who produced the first version of this document as consultants and the countless people who reviewed this document.

Contact

For contacting the authors please use CERT-Relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Legal notice

Copyright Notice

Table of Contents

1 What Will You Learn

During this exercise you will learn about rules, procedures and best practices in incident handling related to personal data breaches. Information provided to you is based on data breach notification requirements for the electronic communication sector introduced by the review of the ePrivacy Directive[1]. You should know that the process of notification is parallel to normal incident handling process and it is part of it.

During the next two hours you will have a chance to exercise set of activities, which are characteristic for events involving personal data breaches. The "data breach" term is understood as a security incident related to personal data[2]. These events are usually related to breach of national law on personal data protection.

Specifically, during the exercise you will learn:

- The terminology related to data breach notification as well as to personal data protection.
- How to evaluate the severity of data breach incident.
- How to prepare notifications for different kinds of receivers – competent national bodies (data protection authorities) and individuals.
- How to conduct some specific parts of incident handling process – severity evaluation and incident notification.

Follow the trainer instructions and explanations to complete planned tasks.

2 Introduction to the exercise

Firstly it is important to know the terminology related to the data breach and personal data[3]. The most important terms and their definitions are:

- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community[4]. It can be the result of an information security incident (see below) or of loss of user control

---

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML

[2] see definition of personal data breach in the terminology part of the exercise – „Introduction to the exercise"

[3] the terminology is from the ENISA's publication: „Recommendations on technical implementation guidelines of Article 4" (http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech)

[4] amendment by Directive 2006/24/EC and Directive 2009/136/EC of Directive on Privacy and electronic communications 2002/58/EC: (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML)

(http://eur-lex.europa.eu/Lex-UriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML)

- **Information security incident** – An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security[5]
- **Personal data** – any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity[6]. In our study we considered the analysis performed by the Art. 29 WP on the explanation of the "personal data" regarding the four main "building blocks" that can be distinguished in the definition of "personal data": i.e. "any information", "relating to", "an identified or identifiable", "natural person"[7]
- **Individual** – any living natural person affected by the personal data breach. This includes users and subscribers, for private or for business purposes, without necessarily having subscribed to the service that is affected by the breach[8]
- **Sensitive personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. The scope of sensitive personal data is broad; for example, membership of a political party is seen as data revealing a political opinion (Directive 95/46/EC)[6]
- **Data controller** – the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (Article 2(d) of Directive 95/46/EC)[6]
- **Data processor** – the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (Article 2(e) of Directive 95/46/EC)[6]

2.1 The general workflow of personal data breach handling procedure.

Below there is the workflow presenting the general workflow[9] how to manage data breach cases. There are some special parts of it which are dedicated to incident handling procedures themselves and will be part of the further exercise activities, which are the parts of this exercise e.g.:

- initial assessments,
- preliminary notification,
- detailed notification.

(http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF)

[5] *International Organization for Standardization (ISO), Information technology — Security techniques — Information security incident management, International Standard, ISO/IEC 27035:2011-09(E)*

[6] *Article 2(a) of Directive 95/46/EC: (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML)*

[7] *Opinion 4/2007 of the Article 29 Data Protection Working Party*

[8] ENISA's „Recommendation on technical implementation guidelines of Article 4"

[9] The workflow is part of the ENISA document: "Recommendations on technical implementation guidelines of Article 4" < http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech>

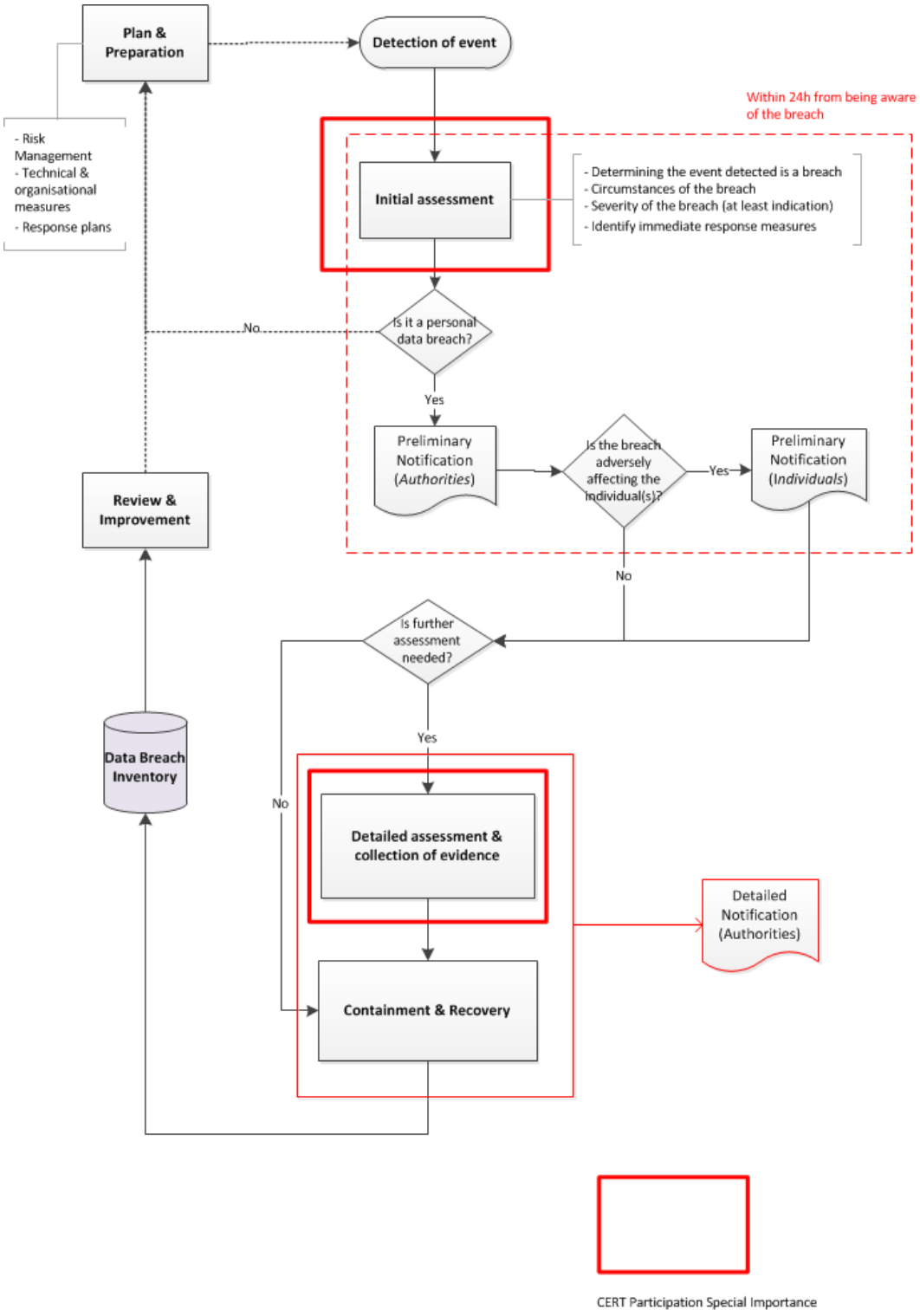

Figure 1: Personal Data Breach Management Procedure[10]

[10] ENISA's „Recommendation on technical implementation guidelines of Article 4"

3 Task 1: Data breach incident severity evaluation

Now your task is to work with particular. Spend 5 minutes in with your group to learn the case, which is described before. If you need any clarification – ask the trainer for it.

The case is the following:

i. *The company database administrator notices an access to database at rare hours during a night. He/she investigates the case and decides that it is probably an attack from outside the company The company cooperates with banks and in its business contracts to process personal data of banks' customers*

ii. *He reports the fact to the company security team. Company security team plays the role of the internal CERT. They have good specialists on network and computer forensics and some of them participated in the events organised by CERT community, for example FIRST Conference. Currently they are trying to convince the company management that their team should become an official CERT team and join European CERT community – TERENA TF-CSIRT.*

iii. *The security team contacts the company network and system administrator to explain the case. They explain the possible scenario of a data breach and recommend and suggest some control activities to further investigation of the case. He recommends inter alia tocheck network connections to the database server, authorisation logs in the local network and remote connections to the company's network.*

iv. *The administrator discovers a new unauthorized account which was created 3 days ago with the administrative privileges on the database server. During this investigation they also discover that the host intrusion detection system was not active for almost one week. There is no clear evidence why it was deactivated. Was it an intentional activity or was it a system failure.*

v. *the further investigation shows the fact of copying from the company's database server, more than 10 000 records included personal data like names of company customers, their credit cards data as well as postal addresses and authorisation data, to the online service (online shop). The system administrators ensure that data was encrypted with AES 256 algorithm.*

vi. *customer list includes citizens from Germany, The Netherlands, Poland, Greece and the United States*

Now you should prepare your own evaluation of the incident severity. To calculate the potential impact of data breach you should estimate two main factors: identifiability and level of exposure.

Identifiability is understood as the ability to identify a person from the personal data that have been breached (according to the Directive 'an identifiable person is one who can be identified, directly or

indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity').

Level of exposure can be evaluated as the result of few important factors and the most important are nature of the data breach, implemented controls and delay in identifying the breach. There are no simply and unambiguous values. An evaluation comes from users' knowledge and experience.

3.1 Initial assessment

Your task is to prepare the initial assessment. Propose your calculation of identifiability and level of exposure. Both can be scored between 1 and 4. Value of one is the least identifiable and the least exposed. The value of four represents the most identifiable and exposed asset.

To complete this task use calculations values presented in the Appendix and use the table below to determinate the final value.

Calculation of the impact[11]

Impact assessment – *Calculation of impact*				
A. Identifiability / B. Level of exposure	**1**	**2**	**3**	**4**
1	**1**	**2**	**3**	**4**
2	**2**	**3**	**4**	**5**
3	**3**	**4**	**5**	**6**
4	**4**	**5**	**6**	**7**

4 Task 2: Data breach notification to data controller and individuals

4.1 Preliminary notification

Now you should prepare two notification reports. One for data controller and second for individuals who were victims of data breach notification. In the Appendix section you can find the table "Example template of a data breach notification form to the competent authority". To better understand your task the trainer will provide you one example. The report of the fictitious company YOU JOB KEEPER Limited.

Learn what kind of concrete fields and information should include the notification, according to the proposed law. If you have your own ideas of the notification format, you can propose them and they will be discussed during the exercise summary.

In your work you should consider the ePrivacy Directive[12] regulations …

[11] Article 2(a) of Directive 95/46/EC: (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML)

[12] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic*

> 'The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition to the notification to the data subjects, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.'

… you should prepare your own list of information taking into consideration the purpose of this notification, especially regarding victims who should not only learnt about the fact of their personal data breach but also learn about consequences and possible actions they should take.

Learn more from the trainer about detailed information which should consist of technical reports from your investigation as well as results of attacked organisation's undertaken steps. Also if you have any information which should be used for identifying the source of the breach, or you have already identified it, this also should be a part of the detailed report.

5 Summary

Now it is time to make a summary of the exercise. You will present the results of your group work and discuss them with other groups.

6 References

Please use the following sources for further reading about the data breach notifications.

1. ENISA Recommendations on technical implementation guidelines of Article 4. (http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech)
2. European Network and Information Security Agency, Good Practice Guide for Incident Management, December 2010. http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management

communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047. (http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML)

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu