EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBER EUROPE 2022: AFTER ACTION REPORT

Findings from a PAN-EUROPEAN cyber crisis Exercise

DECEMBER 2022

CONTACT

To contact the authors, please use exercises@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA: Nikolaos Christoforatos, Ifigenia Lella, Evangelos Rekleitis, Christian Van Heurck, Alexandros Zacharis

LEGAL NOTICE

COPYRIGHT NOTICE

Print ISBN 978-92-9204-606-7 DOI: 10.2824/385167 TP-04-22-224-EN-C
PDF ISBN 978-92-9204-603-3 DOI: 10.2824/397622 TP-04-22-224-EN-N

CYBER EUROPE 2022: AFTER ACTION REPORT

Findings from a PAN-EUROPEAN cyber crisis Exercise

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

TABLE OF CONTENTS

PART I
EXERCISE OVERVIEW

1 INTRODUCTION

Cyber Europe is a series of **EU-level cyber incident and crisis management exercises organised by ENISA.** It is aimed at both the public and private sectors from the EU and EFTA Member States.

The exercises simulate large-scale cybersecurity incidents that escalate into cyber crises, offering opportunities to analyse advanced technical cybersecurity incidents but also test participants on their capabilities for dealing with complex situations. **The exercises aim to test the participants' readiness and capacity to tackle challenging and realistic cyber crises.**

The exercises are organised by ENISA together with planners from participating countries and institutions.

Cyber Europe 2022 aimed to accomplish several Goals and Objectives which are detailed below.

2 GOALS

Cyber Europe 2022 was designed to fulfil a list of **Goals (G).** These Goals were developed to provide the organisers and the participants with a clear scope and a purpose for their participation in the event.

The 2022 edition aimed to achieve the following Goals:

G1. Test EU-level technical and operational cooperation during cyber-crises

G2. Provide opportunities to test local-level incident response and resilience plans

G3. Train EU- and local-level technical capabilities.

These Goals were complemented by the following secondary (also known as implicit) Goals:

- **Help to build trust**
- **Engage the private sector**
- **Improve situational awareness**
- **Test the public affairs response**
- **Improve the exercise's process and capabilities.**

3 OBJECTIVES

The Goals of Cyber Europe 2022 were designed to remain broad and all-encompassing. To further assess the relevance and the added value of the exercise, specific **Objectives (O)** were derived from the Goals. Each Objective was assigned specific metrics for evaluation purposes in order to facilitate assessment of the extent to which they were achieved.

The different Objectives targeted by this exercise are described below, categorised per Goal.

G1. Test EU-level technical and operational cooperation during cyber-crises

O01. Test the quality of information-sharing
O02. Test incident response capability at EU level
O03. Evaluate situational awareness
O04. Test the articulation between the technical and operational levels
O05. Test the operational coordinated handling of public communication

G2. Provide opportunities to test local-level incident response and resilience plans

O06. Provide opportunities to participants to test their intra-organisational procedures, if they exist (Business Continuity Plans (BCPs), Crisis Management Plans, etc.)
O07. Provide opportunities to participants to test cross-organisational cooperation
O08. Provide opportunities to participants to test local-level cooperation activities and/or contingency plans, if they exist

G3. Train EU- and local-level technical capabilities

O09. Provide opportunities to train in a wide variety of cybersecurity and crisis management skills
O10. Identify training needs for the future

The aim was to achieve the **Goals** and **Objectives** by means of the main Cyber Europe 2022 scenario presented in the following subsection.

4 SCENARIO

Cyber Europe 2022 revolved around **the healthcare ecosystem** and tested the **resilience of several relevant stakeholders,** including national Computer Security Incident Response Teams (CSIRTs), cybersecurity authorities, ministries of health, healthcare organisations such as hospitals and clinics, eHealth service providers, and health insurance providers. The participants had to address an **escalating cyber crisis,** tackling **multiple incidents simultaneously.**

The scenario aimed at **realistically** mimicking **technical incidents.** These incidents are detailed in Figure 1 below, which highlight how they covered several elements, with some aimed at gaining a foothold and others aimed at tampering with medical devices. The second figure describes the sectors targeted by the attacks and their potential impacts.

The objective of the scenario was to **enable the players to react accordingly** to each incident in order to minimise the damage incurred, with the general objective of testing the operational and technical layers. The scenario, which spanned two days, began on the first day by engaging the participants around a **disinformation campaign of manipulated laboratory results** and a **cyberattack targeting the networks of European hospitals** as well as **internet and cloud service providers.**

Figure 1. Overview of the technical scenario

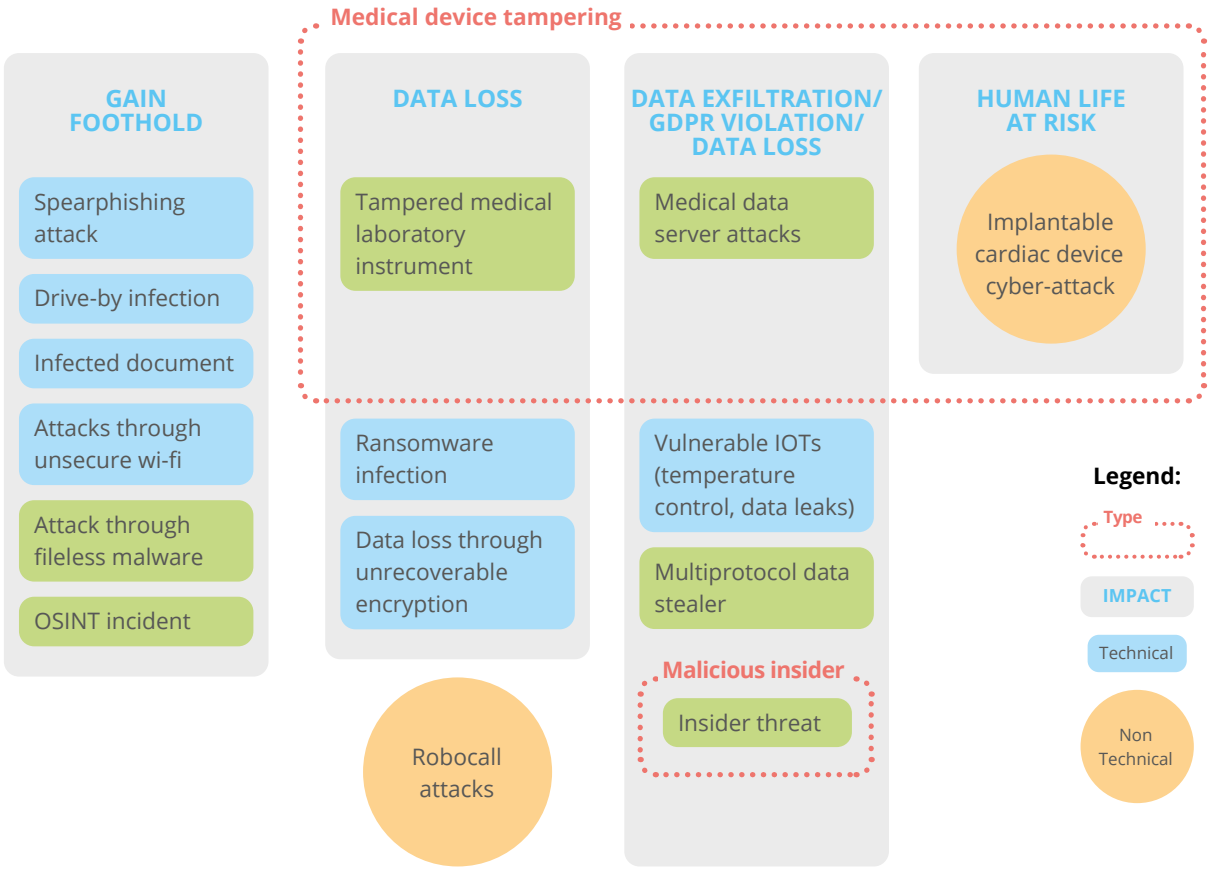


Figure 2. Targeted sectors and potential impact of the attacks

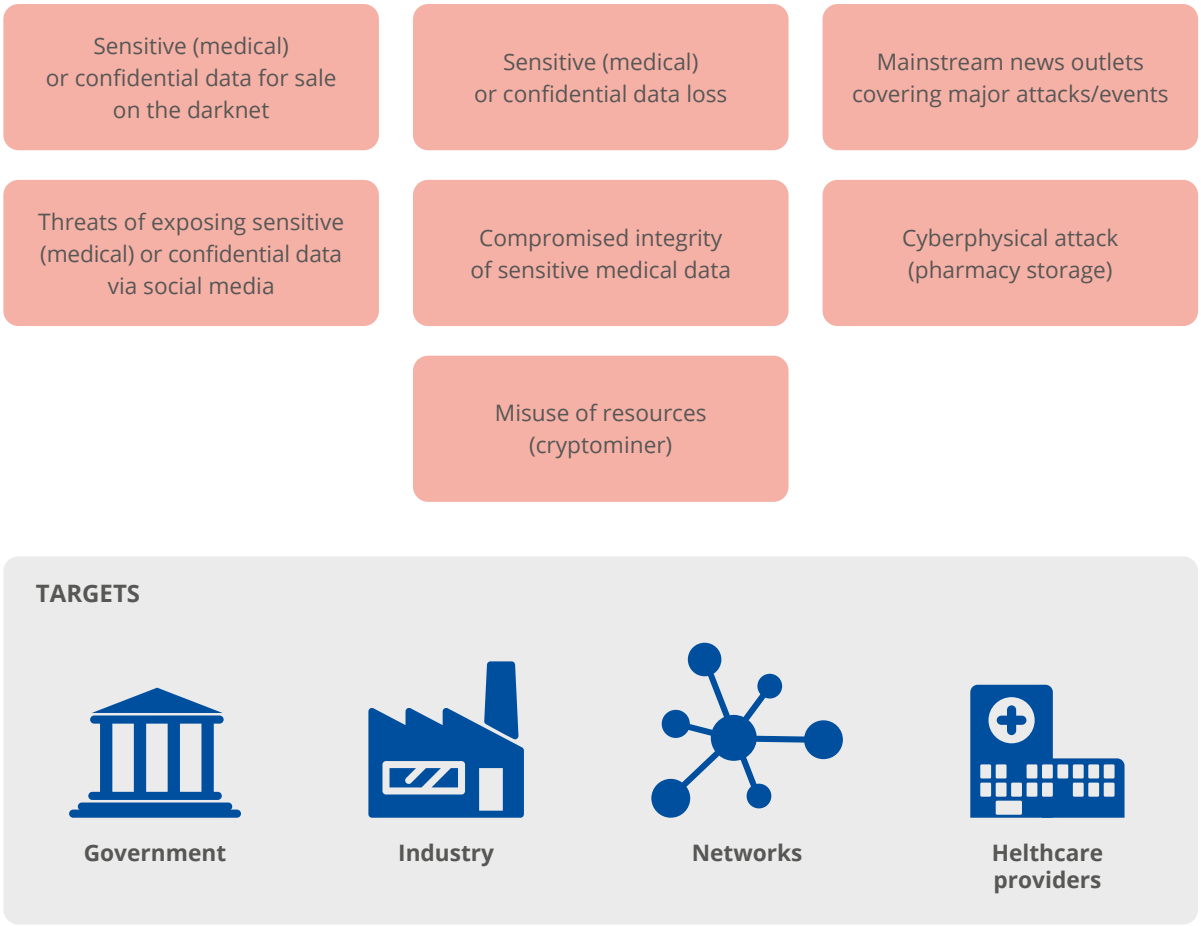
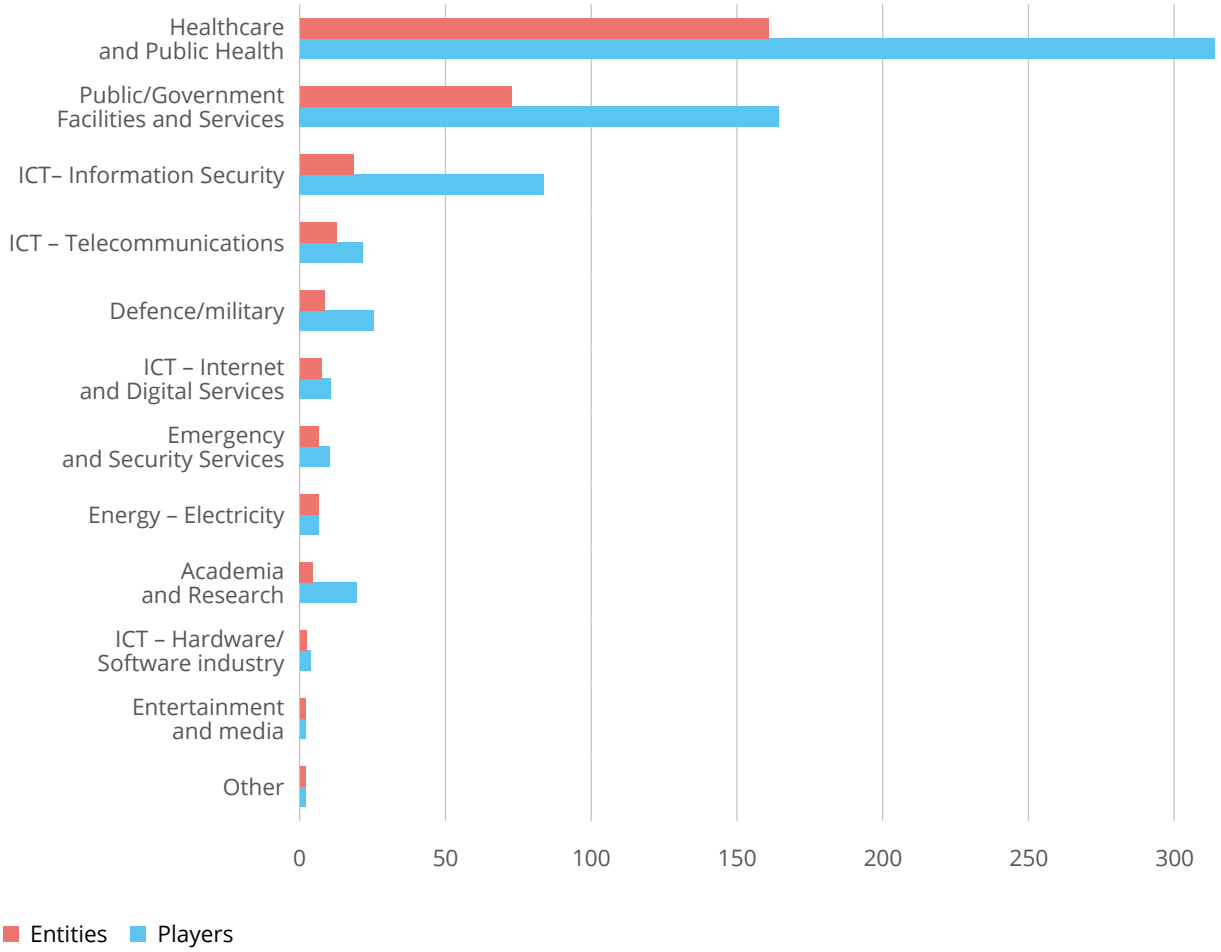


Figure 3. Cyber Europe 2022 planners

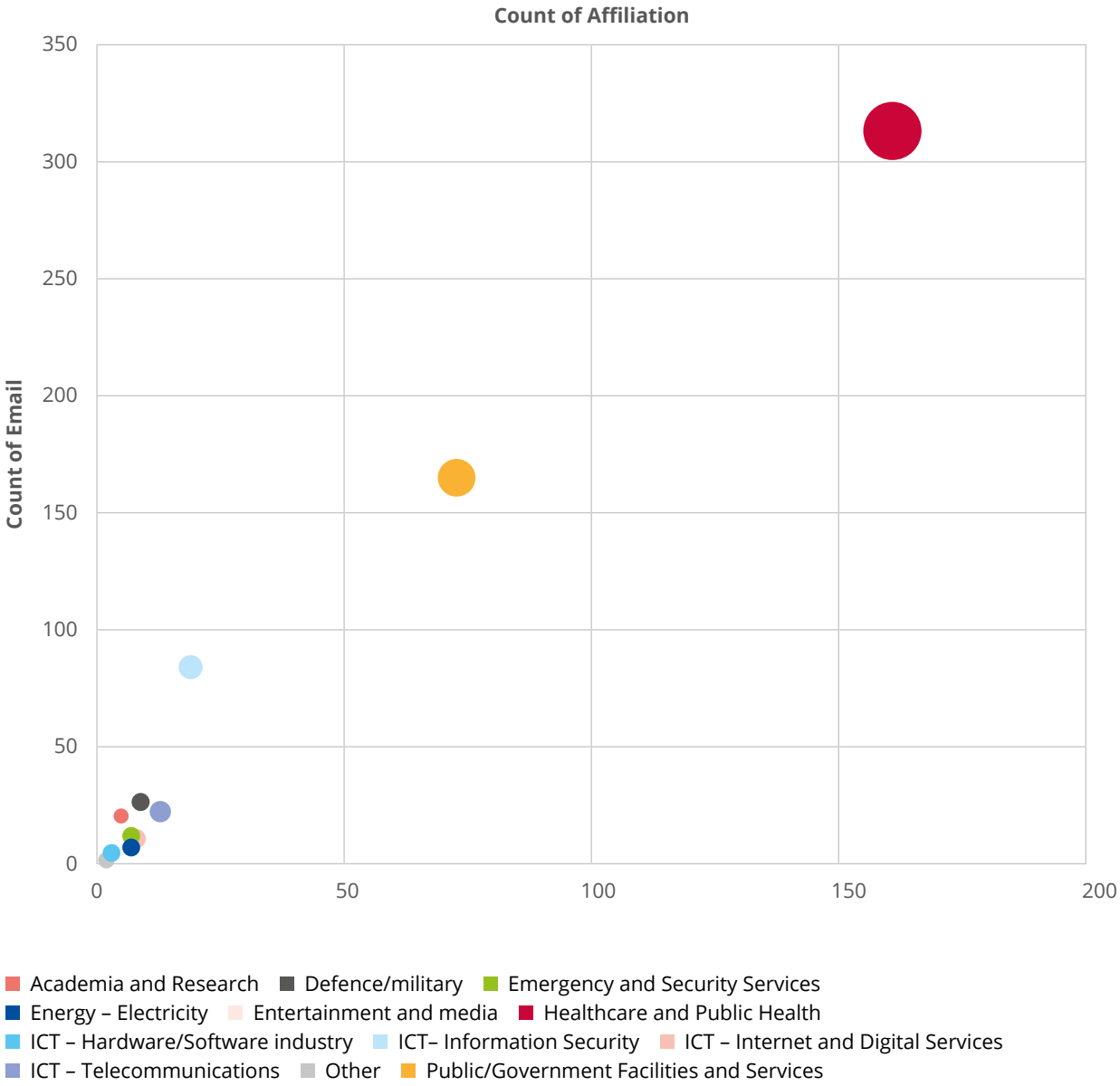
Figure 4. Participants per Sector



In total, 918 participants (planners, players and monitors)[1] officially registered for the exercise, representing the 27 EU Member States, 2 EFTA countries (Norway and Switzerland) and several EU institutions and agencies (including CERT-EU, EAAS, EDPS, EUSPA, EUROPOL and the European Commission). As illustrated in Figure 4, the Healthcare and Public Health sector was the most widely represented sector, but participants came from a wide range of sectors.

1 These figures account only for participants who registered on the Cyber Exercise Platform. Several organisations chose to participate using a generic functional mailbox and distributed exercise information among multiple participants and teams. As a result, it is safe to assume that the actual real number of participants was significantly higher.

Figure 5. Number of Emails and Number of Affiliations per Participating Sector



The figure above illustrates the number of emails (i.e. personal emails) and affiliations (i.e. functional mailboxes) per participating sector.

An observers programme ran in parallel to the execution of the exercise, with representatives from EUIBAs (EU Institutions, Bodies and agencies) and the international cybersecurity community present in the ENISA offices in Halandri (Athens) during the two days of the exercise.

The programme was an opportunity for stakeholders to engage in fruitful discussions, exchange lessons learnt and discuss opportunities for future collaboration.

Figure 6. Cyber Europe 2022 observers

5 TAKEAWAYS FROM THE EXERCISE

Following the completion of Cyber Europe 2022, a survey was circulated to **collect feedback from the participants**. The data collected was complemented by findings from the planners collected during the exercise, observations from the ENISA exercise team and finally analysed by ENISA. **The detailed findings were compiled in a report shared with the planners**.

One key takeaway is that **Cyber Europe 2022 can be regarded as having been a success as all parties involved identified areas for improvement**. This proves that Cyber Europe is helpful in identifying what works, but also where there are shortcomings and areas for improvement.

The lessons learned from the participants in Cyber Europe were compiled in the following word cloud.

GENERAL TAKEAWAYS

Cyber Europe 2022 Goals and Objectives

The Goals and Objectives set by Cyber Europe 2022 (CE2022) were mainly achieved. In a nutshell, CE2022 provided the testing and training opportunities to the participants that were stated in the main Goal.

The more detailed analysis confirmed that the exercise also achieved secondary (implicit) goals. Although not every participating entity was able to engage in all secondary areas, **the exercise scenario offered the opportunity** to all participating countries and institutions to do so.

- **The uptake of the detailed findings at the Objectives level,** which were shared with the planners, **should result in the improvement of procedures, communication and coordination processes** that are in place at local, sectoral, national, cross-border and EU-wide levels.

Figure 7. Word cloud "Lessons learned by the participants"

The future of Cyber Europe

- **An exercise like Cyber Europe as a training and testing ground is needed, as it successfully identifies gaps and development points across the board in order to improve the cybersecurity posture of all participating stakeholders.** Cyber Europe 2022 was notably able to engage several stakeholders from the private and public sectors in collaboration and working together towards achieving a common goal: improving EU-wide coordination during major cyber crises.
- **The ENISA Cyber Exercise Platform (CEP) used for the planning and execution of the exercise could benefit from a refresh** in order to be able to be accommodate future expectations and improve the user experience for all involved.
- **Cyber Europe 2022 confirmed the importance of preparing optimally for such a large-scale exercise,** investing more effort in the preparation of the results in order to produce a more useful output. The preparation helps to better identify gaps and areas for improvement, determines the impact of participating in such an exercise and facilitates recruiting players with different roles.
- **The planners agreed with ENISA's observations that receiving improved support and training for their crucial role as planners would help them get even more out of future Cyber Europe exercises.** It would also help level the playing field for all players. This would ensure the exercise is adequately tailored to local-level specificities.

Participating entities and sectors

- **Cyber Europe 2022 confirmed the importance of allocating sufficient budget and resources to cybersecurity teams in the healthcare sector,** given the severity of the challenges linked to cyber-attacks.
- **Cyber Europe 2022** provided a training ground for Standard Operating Procedures and Business Continuity Plans. **The exercise confirmed the need for frequent testing at local level in order to continuously improve and strengthen the healthcare sector's resilience with regard to cybersecurity threats.**

TP-04-22-224-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost the resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

Publications Office
of the European Union

ISBN 978-92-9204-603-3