enisa 20 years!

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

BEST PRACTICES FOR CYBER CRISIS MANAGEMENT

FEBRUARY 2024

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA 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 resilience of the EU'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.

CONTACT

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

AUTHORS

ENISA

ACKNOWLEDGEMENTS

This study has been drafted within the EU Cyber Crises Liaison Organisation Network (EU-CyCLONe).

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2024

Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence https://creativecommons.org/licenses/by/4.0/. This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated.

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

ISBN 978-92-9204-658-3, DOI 10.2824/767828

TABLE OF CONTENTS

1. INTRODUCTION 9

1.1 EU POLICY CONTEXT 9

1.2 STUDY CONTEXT 9

1.3 OBJECTIVES OF THE STUDY 10

1.4 SCOPE OF THE STUDY 11

1.5 METHODOLOGY 11

2. DEFINITIONS FOR CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU 12

2.1 DEFINING A CYBER CRISIS 12

2.2 DEFINING CYBER CRISIS MANAGEMENT 16

3. STRUCTURE AND ACTORS OF CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU 23

3.1 OVERVIEW OF THE STRUCTURE OF CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU 23

3.2 ROLE AND OBLIGATIONS OF ENISA IN CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU 24

3.3 ROLE AND OBLIGATIONS OF MS AND COOPERATION MECHANISMS FOR CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU 25

3.4 ROLE AND OBLIGATIONS OF THE EUROPEAN CYBER CRISIS LIAISON ORGANISATION NETWORK IN CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU 26

4. CYBER CRISIS MANAGEMENT BEST PRACTICES AT THE OPERATIONAL LEVEL IN THE EU 28

4.1 PHASE 1 – PREVENTION 29

4.2 PHASE 2 – PREPAREDNESS 32

4.3 PHASE 3 – RESPONSE 42

4.4 PHASE 4 – RECOVERY 44

5. RECOMMENDATIONS 46

6. BIBLIOGRAPHY 48

ANNEX: ENISA'S KNOWLEDGE BASE 56

EXECUTIVE SUMMARY

This study highlights the **complexities behind the notion of cyber crisis** and the degree of **subjectivity** it involves. **The elevation of a large-scale cyber incident into a cyber crisis relies predominantly on a political decision**, and depends largely on the level of risk that EU Member States (MS) are prepared to tolerate (i.e. 'risk appetite').

Differences in interpretation of what constitutes a cyber crisis between MS pose challenges at the EU level. The definition of cyber crisis is important as it directly influences the way the crisis is managed. In the meantime, identifying the **causes, nature and impact** of a cyber crisis can facilitate the assessment of the crisis and its severity, and influence the selection and adoption of appropriate measures for cyber crisis management.

The management of a cyber crisis involves a variety of actors at the **organisational** or **corporate, sectoral, regional, national** and **EU levels.** A cyber crisis is managed at the **strategic, operational** and **technical levels,** with the operational level playing a key role in bridging the gap between the other two, ensuring that information is shared at all levels and enhancing cooperation and coordination between all relevant stakeholders. In addition, cyber crisis management frameworks are **part and parcel of general crisis management frameworks.** As a result, the **EU has a complex ecosystem of cyber security actors, structures** and **mechanisms,** with a 'highly complex and interwoven system of actors, structures and processes operating in the cyber domain', mainly because cyber crises are often transboundary by nature.

While the EU has developed a **crisis management framework specifically dedicated to the management of cyber crises** – including through the Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises (2017) (Blueprint) ([1]), the Cybersecurity Act (2019) ([2]) or the network and information security (NIS) directive (2016) ([3]) – **the NIS 2 directive (NIS2)** ([4]) **has the strongest impact on cyber crisis management at the strategic, operational and technical levels in the EU.** At the operational level, it will consolidate ENISA's support to MS ([5]) in cyber crisis management, introduce new obligations for MS and assert the EU-Cyber Crises Liaison Organisation Network (EU-CyCLONe) as the key player in cyber crisis management. **NIS2 enables a more coordinated approach through greater cooperation between MS and relevant EU institutions, bodies and agencies (EUIBAs).**

In this study, cyber crisis management at the operational level in the EU is analysed around the four phases of the cyber crisis management cycle, namely **prevention, preparedness,**

([1]) European Commission (2017), Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, pp. 36–58), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017H1584&qid=1702033489333.

([2]) European Parliament and Council of the European Union (2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, pp. 15–69), https://eur-lex.europa.eu/eli/reg/2019/881/oj.

([3]) European Parliament and Council of the European Union (2016), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, pp.1–30), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148.

([4]) European Parliament and Council of EU, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2020, pp. 80–152), https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

([5]) See Chapter 3.4 'Role and obligations of ENISA in cyber crisis management at the operational level in the EU'.

response and recovery, which should be framed by **an all-hazards approach**, given that threats can have many different origins.

The best practices identified show that MS have already introduced some effective cyber crisis management measures at the operational level. These are likely to continue to grow and evolve, as MS implement NIS2 and develop their own responses to the challenges of cyber crisis management.

The identified best practices are shown below.

The prevention phase aims to better prevent and reduce the risk of cyber crises and to minimise their effects should they arise.

- **BP #1.** Adoption of a national definition of 'cyber crisis', taking into account its transboundary dimension.
- **BP #2.** Development of information security standards specific to the national public sector, to be reviewed and updated regularly.
- **BP #3.** Foster national initiatives which promote the creation of prevention programmes such as centralised distributed denial-of-service attack (DDoS) mitigation programmes.

The preparedness phase aims to develop plans to support response operations.

- **BP #4.** Definition of a governance structure, provision of specific capabilities and appointment of a crisis coordinator, whose nomination is mandatory under NIS2, ensuring their department has the necessary operational and technical cyber skills to directly coordinate stakeholders during a cyber crisis.
- **BP #5.** Mapping and gathering information on critical entities and their most critical assets to enable rapid action.
- **BP #6.** Establishing instantaneous, secured communication channels during a crisis.
- **BP #7.** Formalisation of a clear allocation of roles between the parties involved in responding to a cyber crisis in an overall plan.
- **BP #8.** Development of escalation criteria for activating the cyber crisis plan and deploying the relevant cooperation units/groups, taking into account factors such as time, priority, players involved, severity of the attack, etc.
- **BP #9.** Development of a methodology and risk assessment tools to optimise coordination and interoperability in the event of a crisis.
- **BP #10.** Testing of the overall plan for operations in response to cyber crises through a multiannual programme of cyber crisis management exercises and training sessions.
- **BP #11.** Setting up training sessions for current and future staff responsible for cyber crisis management at the operational level.
- **BP #12.** Development of a communication strategy including a clear format for messaging, stakeholders to involve, priority levels and time factor and communication channels to be used.

The response phase aims to stem the cyber crisis and prevent further damage.

- **BP #13.** Encourage the mobilisation of private-sector certified 'trusted providers' to provide technical assistance to victims.
- **BP #14.** Supporting victims' crisis communication, for instance with a unified and transparent message.