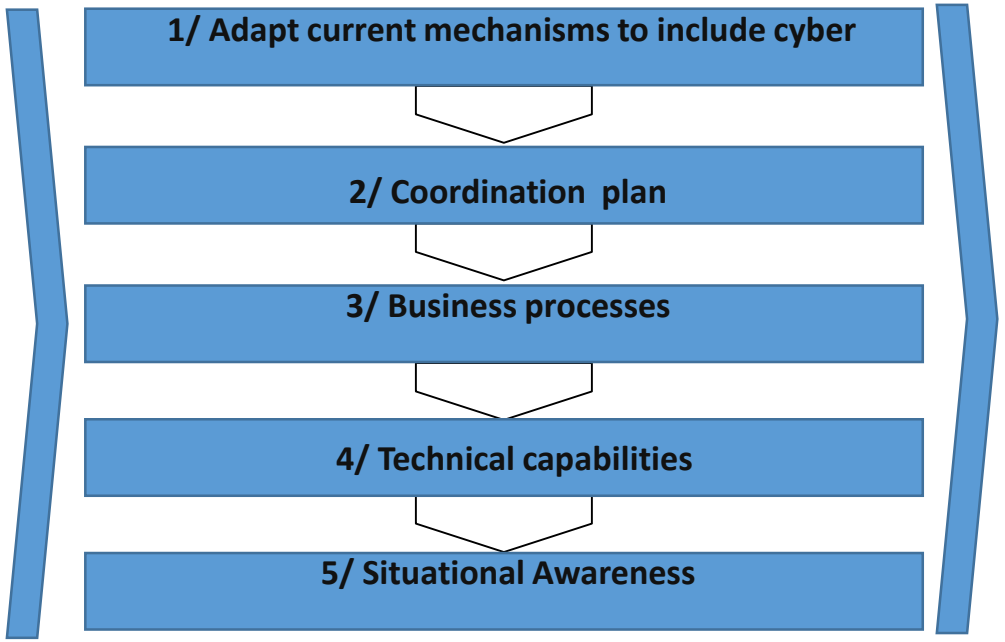
THE EU CYBERSECURITY AGENCY

BLUEPRINT GAPS

Georgios Chatzichristos
Operational Security Unit - ENISA

03 | 06 | 2019

Managing a cyber crisis



Managing a cyber crisis

Yesterday		Today
IPCR	1/ Adapt the EU crisis cooperation principles to better include cyber	IPCR
ECCCF (2013)	2/ Develop an EU cyber crisis cooperation plan	**Cyber Blueprint**
EU SOPs (2011)	3/ Formally adopt EU cyber crisis cooperation procedures	CSIRT Network Rules of Operation
CE2014-16 Prototype	4/ Build an EU cyber crisis cooperation platform	MeliCERTes
MS (ad-hoc)	5/ Establish an EU cyber crisis cooperation hub to foster situation awareness	ENISA (OpenCSAM)

Commission Recommendation of 13.09.2017 on Coordinated Response to Large Scale Cybersecurity Incidents & crises


EUROPEAN COMMISSION

Brussels, 13.9.2017
C(2017) 6100 final

COMMISSION RECOMMENDATION

of 13.9.2017

on Coordinated Response to Large Scale Cybersecurity Incidents and Crises

EN EN

Member States and EU institutions should establish an EU Cybersecurity Crisis Response Framework integrating the objectives and modalities of cooperation presented in the Blueprint following the guiding principles described there-in.

Political/Strategic level

- MS Ministers responsible for cybersecurity
- European Council, the President/Rotating Presidency
- PSC and Horizontal Working Party (Cyber Diplomacy toolbox)
- European Commission, the President
- EEAS/ High representative

Operational level

Member States

- MS Competent Authorities and Single Points of Contact (NIS Dir)
- CSIRTs, Cybersecurity Agencies
- Other National Sectoral Authorities

EU Bodies

- EC Deputy Secretary General (ARGUS)
- DG CNECT/HOME
- ENISA
- Europol/EC3
- CERT-EU
- EC Security Authority
- Other DGs
- EEAS (EU INTCEN & EUMS INT)
- EU Hybrid Fusion Cell
- European Council Presidency

Technical level

- CSIRTs network
- ENISA
- CERT-EU
- Europol/EC3

Shared Situational Awareness

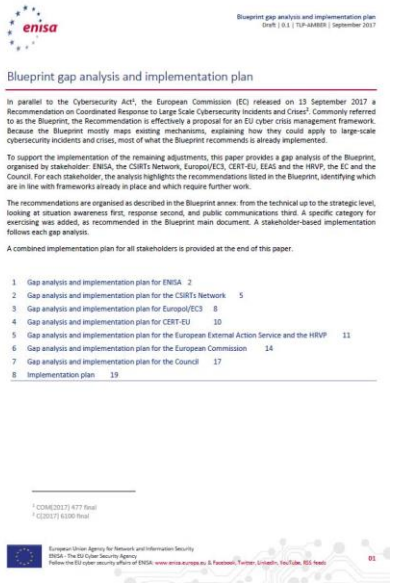
Coordinated Response

Coordinated public communication

EC Recommendation

ENISA Gap analysis

EU PACE 18 LLs



Blueprint gap analysis and implementation plan

Draft | 0.1 | TLP-AMBER | September 2017

Blueprint gap analysis and implementation plan

In parallel to the Cybersecurity Act[1], the European Commission (EC) released on 13 September 2017 a Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises[2]. Commonly referred to as the Blueprint, the Recommendation is effectively a proposal for an EU cyber crisis management framework. Because the Blueprint mostly maps existing mechanisms, explaining how they could apply to large-scale cybersecurity incidents and crises, most of what the Blueprint recommends is already implemented.

To support the implementation of the remaining adjustments, this paper provides a gap analysis of the Blueprint, organised by stakeholder: ENISA, the CSIRTs Network, Europol/EC3, CERT-EU, EEAS and the HRVP, the EC and the Council. For each stakeholder, the analysis highlights the recommendations listed in the Blueprint, identifying which are in line with frameworks already in place and which require further work.

The recommendations are organised as described in the Blueprint annex: from the technical up to the strategic level, looking at situation awareness first, response second, and public communications third. A specific category for exercising was added, as recommended in the Blueprint main document. A stakeholder-based implementation follows each gap analysis.

A combined implementation plan for all stakeholders is provided at the end of this paper.

[1] COM(2017) 477 final
[2] C(2017) 6100 final

European Union Agency for Network and Information Security
ENISA - The EU Cyber Security Agency
Follow the EU cyber security affairs of ENISA: www.enisa.europa.eu & Facebook, Twitter, LinkedIn, YouTube, RSS feeds

01

Main message

Most of the Blueprint requirements are already there. There is however significant room for improvement on alignment in mechanisms and protocols for effective SA, Response & Public Communication between EU bodies, Agencies, and MSs, at the **Operational** & **Technical** levels.

Coordinated Response

- *Improvement in procedures*
  - Ongoing work at EUIs & Member States
    - NIS CG Work stream 7 work on SOPs for the Operational level (MSs)
    - ENISA, EDA, Europol EC3, CertEU MoU roadmap (EUIs)
  - Need for closer, more efficient cooperation and information exchange between EU Institutions (Operational EU SOPs, 24/7)
  - Improve interoperability between EU Institutions and Member States (Operational level SOPs)

- *Improvement in capabilities*
  - MeliCERTes platform under development (CSIRTs Network)
  - Confidential information exchange (Capabilities)

Situational awareness sharing

- *Improvement in trainings*
  - frequent exercises

- *Improvement in capabilities*
  - New capabilities (classified/unclassified)

- *Improvement in Policies*
  - EU Institutions mandate restrictions
  - National restrictions
  - Trust building measures

Public communication

- ENISA public communication playbook (2018)
- Better coordination (at all levels) through frequent exercises

Recommendations

Spread the information / provide more trainings

- EU Institutions, bodies and Agencies

Develop Operational SOPs

Improve information exchange between EU Institutions

- Mandates, legal issues, 24/7, capabilities

Improve ‘vertical’ collaboration

- EU Institutions, bodies and Agencies

Integrate existing protocols (i.e. LE ERP)

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu