

# ENISA's Information Sharing Good Practice Guide

**Dr. Evangelos OUZOUNIS**

**Senior Expert – Network Security Policies**

**Technical Department**

**ENISA**

**evangelos<dot>ouzounis<at>enisa<dot>europa<dot>eu**

# Why Information Sharing

## ★ Stock Taking

- ★ fragmented understanding of potential vulnerabilities, risks and threats at national level
- ★ lack of a holistic national risk management process
- ★ urgent need for a joint mechanism that continuously reviews and improves preparedness, response and recovery measures

## ★ Information Sharing

- ★ better understand a changing environment
- ★ learn in a holistic manner about intrusions, vulnerabilities and threats
- ★ jointly develop recommendations for reducing network security vulnerabilities, threats, and attacks
- ★ jointly develop methods to continuously assess existing measures
- ★ provide unique insights and strategic views to policy makers and strategists

# What is Information Sharing

- ★ a partnership of 20-30 public and private stakeholders
- ★ participants are high level security experts
- ★ meet regularly (face-face) to share sensitive information using simple protocols (e.g. Traffic Light Protocol)
- ★ address strategic issues (e.g. major/critical disruptions, protection against electronic and/or physical attacks, ..)
- ★ emphasis on preparedness; not on response nor on recovery
- ★ government's role is key in creation and operation
- ★ no participation fees
- ★ 2 chairs, one from industry and one from public
- ★ provides incentives for members to participate; respects their commercial sensitivities
- ★ emphasis on information exchange, not information transfer; no listeners, no observers

# Typical Tasks of Information Sharing

- ★ assess the impact of incidents (security breaches, network failures, service interruptions)
- ★ identify, analyse, and adopt in co-ordinated manner appropriate, sector wide preparedness measures to mitigate these threats and risks
- ★ set up internal and joint procedures to continuously review the implementation of adopted measures
- ★ Provide unique, strategic insights to policy and decision makers

# What is shared

- ★ experience and information on threats, risks, impact, vulnerabilities, incidents, counter measures,
- ★ advisory support and warnings in implementing joint, sector wide, protective good practice measures
- ★ experience and information on
  - ★ contingency planning,
  - ★ crisis management,
  - ★ analysis & mitigation of threats, risks, incidents, dependencies,
- ★ information on emerging trends and changing environments
- ★ Information on exercises, on methodologies and scenarios for conducting them

# Interfaces with other Bodies

- ★ Relationship with Law Enforcement
  - ★ Mixed approaches
- ★ Relationship with Telecommunications Regulator
  - ★ Usually not; industry members would not share information of interest to telecommunications regulator
- ★ *Relationship with CERTs/CSIRTs*
  - ★ Mixed approaches
- ★ *Relationships with other Resilience-related bodies*
  - ★ Usually not directly but via the government's representative or a major/dominant national provider
- ★ Relationships with other national information sharing schemes
  - ★ there is ad-hoc co-operation among them
- ★ Relationship with pan European Information sharing schemes
  - ★ no pan European information sharing; ENISA tries to establish one; hopefully all national platforms will co-operate

# Typical Problems/Barriers/Mistakes

- ★ National legal and/or cultural framework on public/private co-operation
- ★ Improper size, profile of participants, or expertise of experts,
- ★ Poorly defined mission and scope
- ★ not incentivizing enough providers to participation
- ★ unbalanced sharing of information (e.g. mostly from private to public stakeholders)
- ★ changing continuously participants
- ★ regularly missing meetings
- ★ fear of building a Cartel due to privileged access to information
- ★ not having proper non disclosure agreements
- ★ improper treatment of confidential information
- ★ not defining limits of liability

- ★ Information Sharing is necessary to better understand a constantly changing environment
- ★ Only a few Information Sharing Exchanges in Europe
- ★ Takes time and a lot of efforts in establishing and running an Information Sharing Exchange
- ★ Europe should take advantage from its diversity and develop national as well as a pan European Information Sharing Schemes
- ★ Co-operation among national initiatives and pan European one is necessary
- ★ ENISA helps MS to develop knowledge and expertise in information sharing; later ENISA could help MS to deploy such schemes, if interest exists