CSIRT – LEA cooperation

Remarks for the Launch event of CyberEAST

Hein Dries

10 YEARS EaP Eastern Partnership

OUR RIGHTS
OUR FREEDOMS
OUR EUROPE

NOS DROITS
NOS LIBERTÉS
NOTRE EUROPE

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

A happy marriage?

Why is this a topic?

Different roles and responsibilities!

CSIRT:

- Incidents
- Preventative
- Damage control

LEA:

- Crimes
- Reactive
- Attribution

Both provide Security

Expertise

Deconflicting tasks

Not every security incident has a criminal component

Not every incident is a crime

Not every threat comes with an adversary with bad intentions

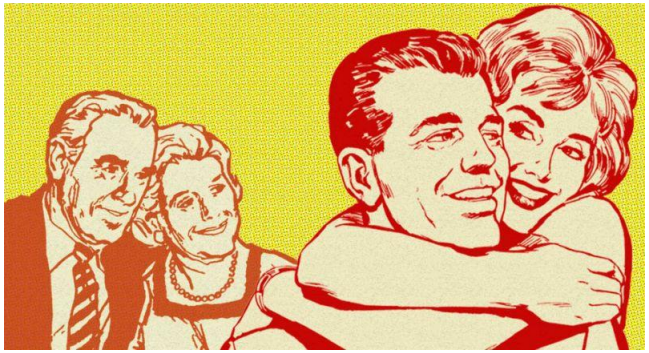
A happy marriage?

Why bother?

Many incidents involve criminality

Many crimes lead to security incidents (and vv)

Many threats are posed by an adversary with bad intentions



Legal basis

Police
- Enforce cybercrime legislation/Public order
- Digital evidence/Attribution
- Tightly regulated exchange of information (need to know)

CSIRTs
- Coordinating task
- Often informational/awareness oriented
- Critical Infrastructure: increased mandate to set standards
- Often focussed on sharing information as much as possible (TLP)

EU: NIS directive
- NIS authority
- National CERT
- Goal: Critical infrastructure protection
- Attacks on Information systems (separate directive: requires monitoring and information exchange)

ALL: Data protection

Cooperation..What..Where?

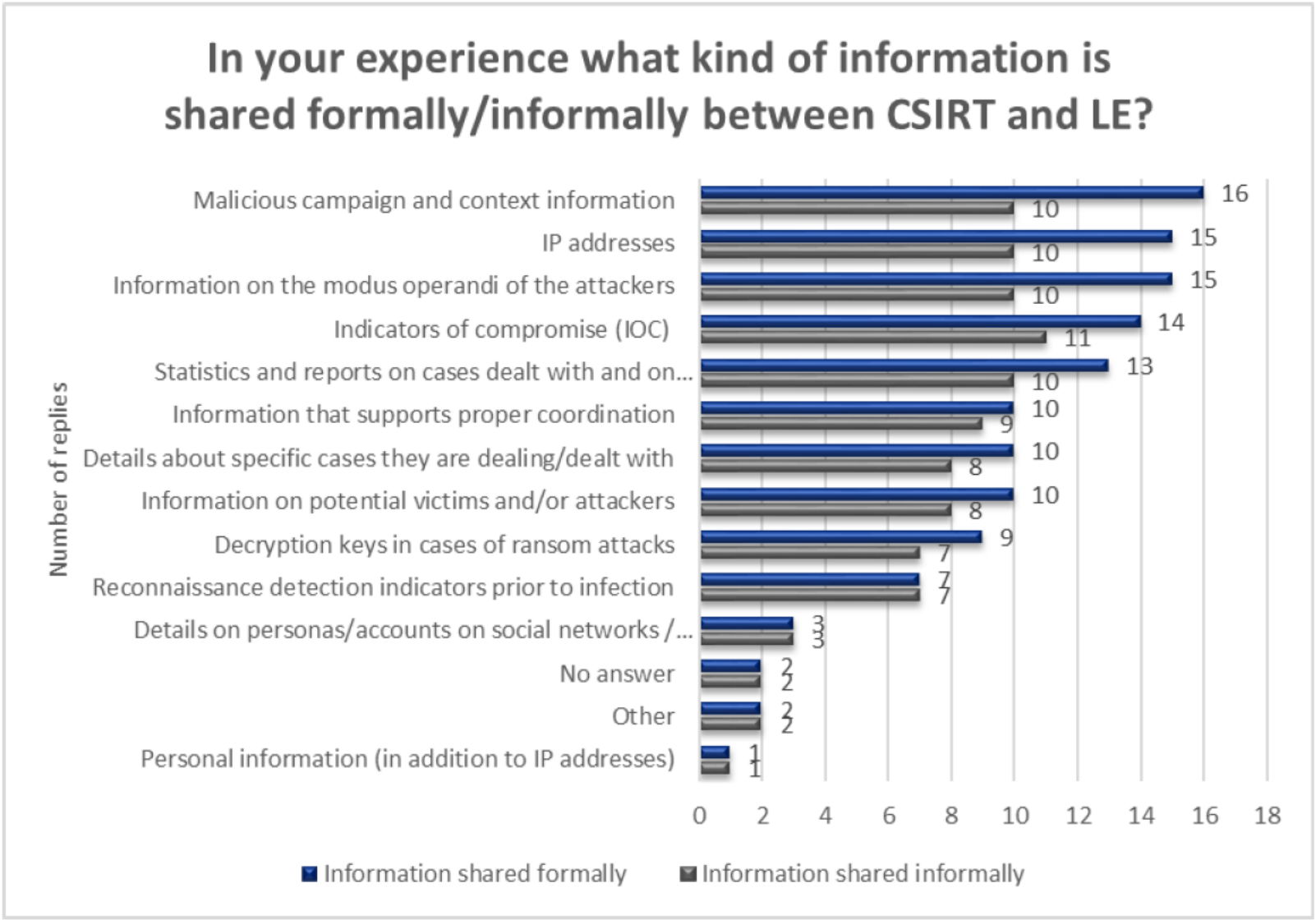
Areas of cooperation?

- **Critical Infrastructure**
- **Data breaches**
- **Large scale incidents involving attacks on information systems**
- **…**

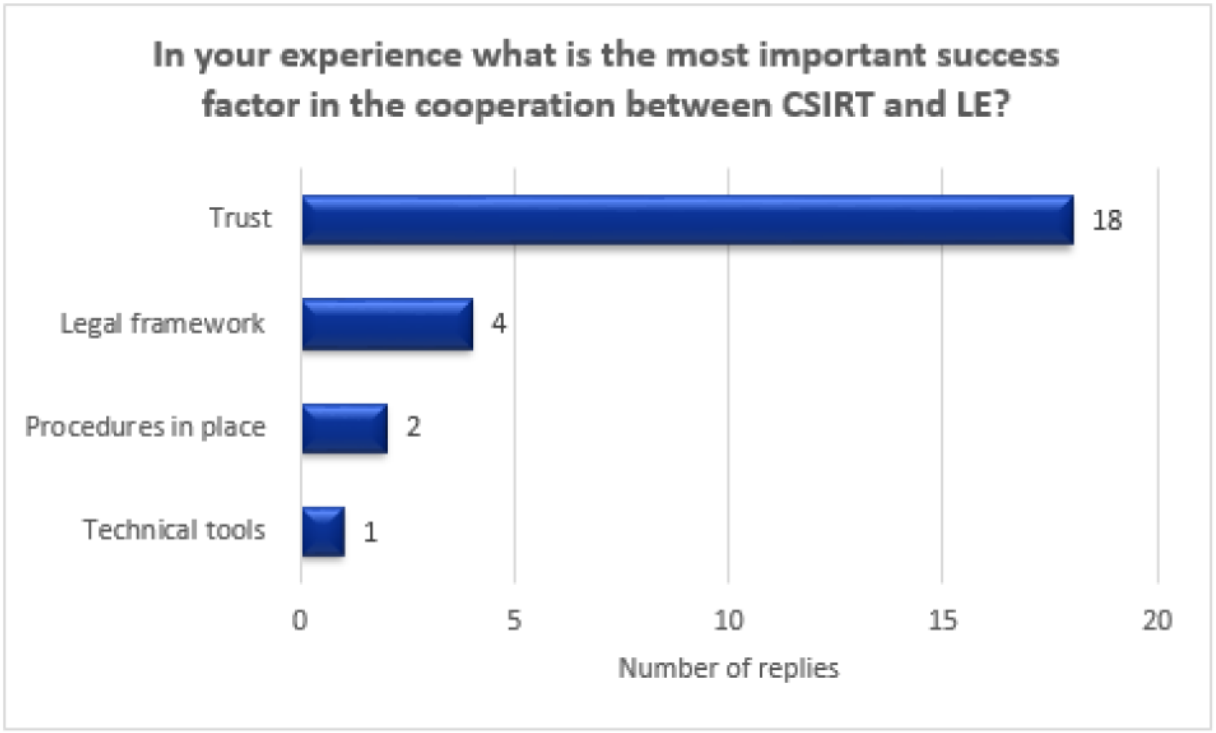
CERTS: Sectoral approach (constituencies)
Law Enforcement: Topical Approach (areas of expertise)

ENISA: study on cooperation

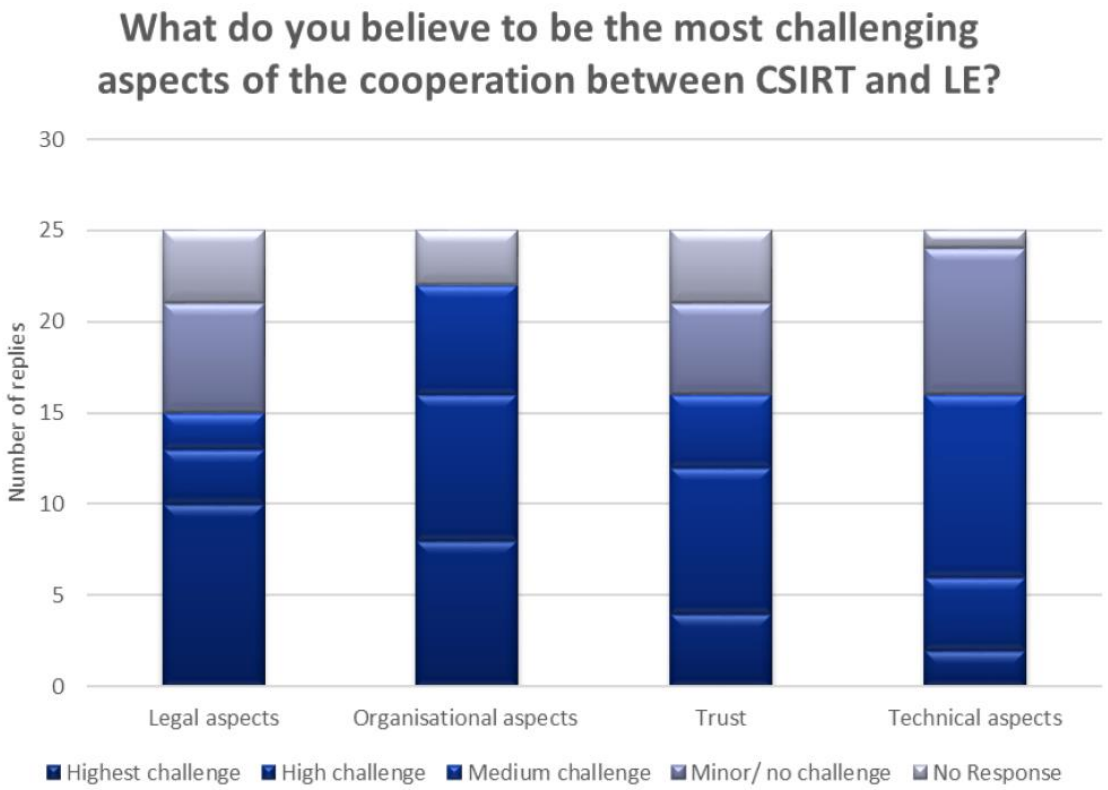
ENISA: LEA-CSIRT Cooperation Survey



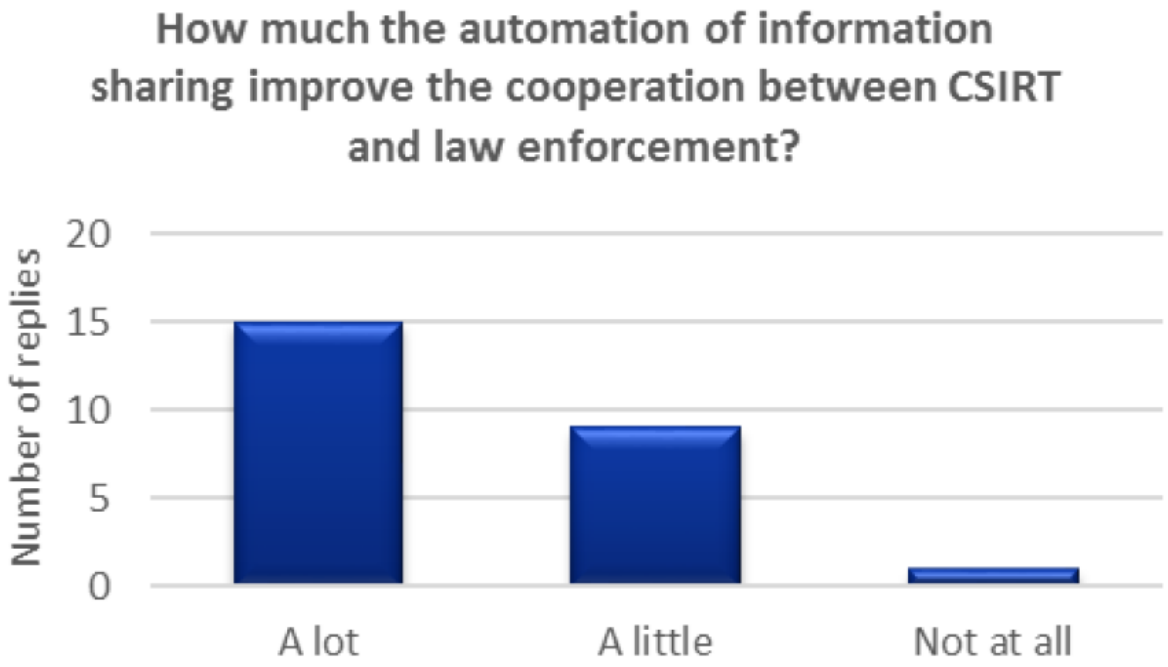
ENISA: LEA-CSIRT Cooperation Survey



ENISA: LEA-CSIRT Cooperation Survey



ENISA: LEA-CSIRT Cooperation Survey



Challenges (legal)

ENISA:

- **Data retention**
- **Secrecy of criminal investigations and the 'need to know'**
- **Sharing of personal data, including IP addresses**
- **Fundamental rights**
- **Chain of custody and evidence admissibility**
- **Diversity of legal frameworks between Member States and the timing of the investigative Cooperation between Member States**

Challenges (technical , organisational)

ENISA (technical):

- **Validation of the digital forensic tools**
- **Different technical maturity levels across different communities**
- **Lack of common tools, tools for automated or semi-automated transfer of the data, and coordination tools**
- **Taxonomy-related challenges**

ENISA (oraganisational):

- **Need for reciprocal understanding of the structures, roles and strengths**
- **Digital forensics expertise and the digital forensics training**

Challenges (legal)

ENISA:

- **Data retention**
- **Secrecy of criminal investigations and the 'need to know'**
- **Sharing of personal data, including IP addresses**
- **Fundamental rights**
- **Chain of custody and evidence admissibility**
- **Diversity of legal frameworks between Member States and the timing of the investigative Cooperation between Member States**

Questions?

- Questions?

Thank you for your attention

Hein Dries
VIGILO
The Netherlands
+31 71 7113243
hein@vigilo.nl