Data Breach and Incident Management – Discussion of GDPR Requirements and Resolution

Marcel Breuer, Task Force Data Protection, Barcelona 2018

Why should we talk about it? (1/2)

Some obligations in the case of a personal data breach

Controller:

- Notification of the supervisory authority within 72h and without undue delay (Art. 33 GDPR)
  - If there is a risk for the rights and freedoms of natural persons

- In the case of a high risk for the rights and freedoms:
  - communicate the personal data breach to the data subject without undue delay (Art. 34 GDPR)
  - In the case of disproportionate effort: There shall be public communication..

- Describe the measures taken … to mitigate the possible adverse effects (Art. 33 GDPR)
- Ensure the data privacy and restore the availability and access to the data
  (physical or technical incident, Art 32 GDPR)

Processor:

- Notification of the controller without undue delay (Art. 33 GDPR)
- Ensure the data privacy and restore the availability and access to the data
  (physical or technical incident, Art 32 GDPR)

Why should we talk about it? (2/2)

Some operational aspects

Many services are developed, produced or delivered by collaboration of

- NRENs, GEANT, Institutions and other organizations within the community

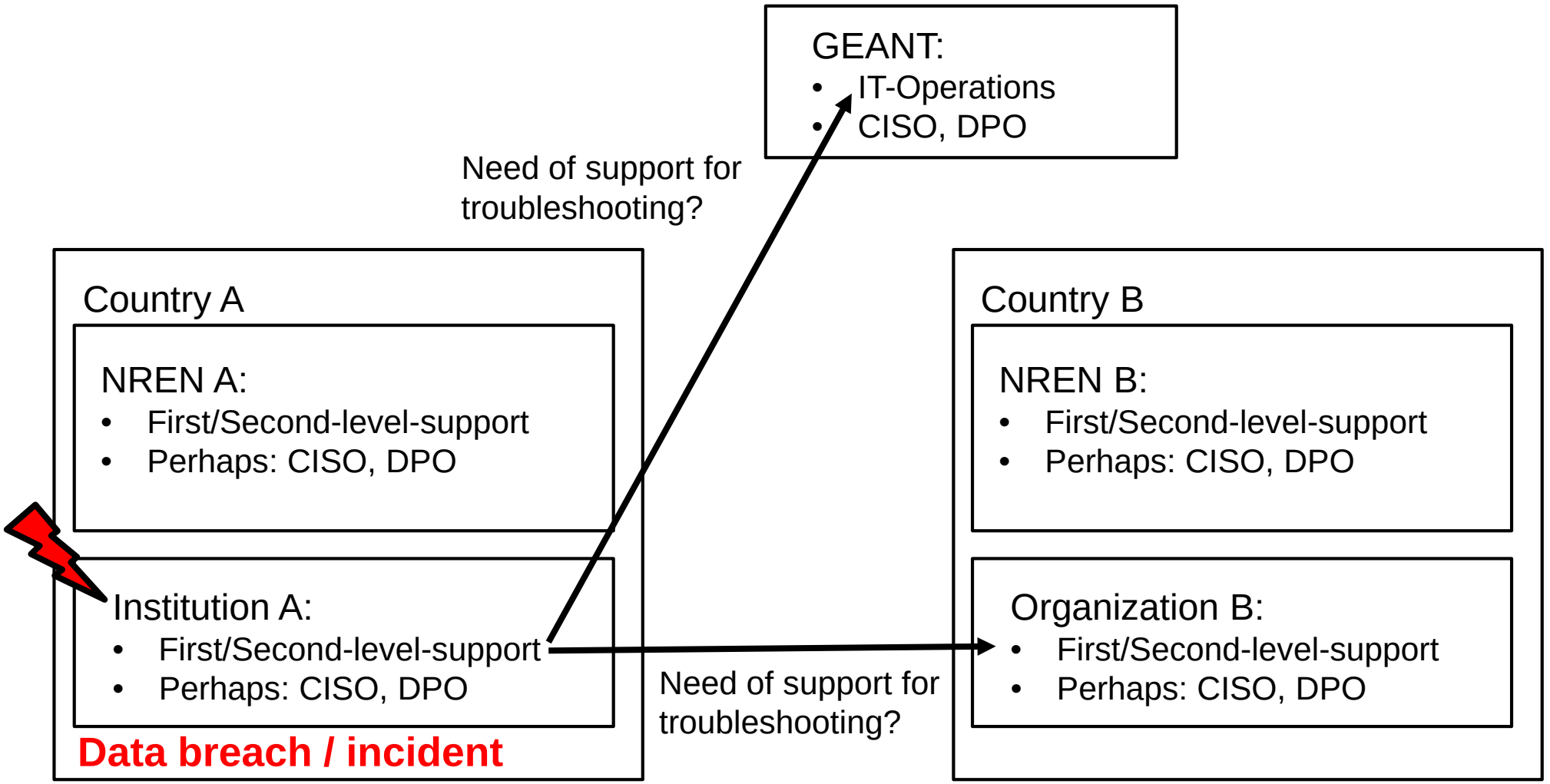
Some examples: perfSONAR, eduroam, others

Incidents can occur in most organizations (aspect of probability)

- Some incidents might be information-security-related
- Some incidents might be data-privacy-related

What does it mean from the operational perspective?

Data breach and incident management: Scenario for a collaborative service delivery



Some operational issues in this context

First-Level-Support of organization A:

- How can we find out who is controller or processor for a service?
  - **Time limit for controller! -> Data breach notification!**
- How can we get support from organization B for troubleshooting?
  - **In a timely manner?**
  - **How to contact them?**
  - Exchange of information? (Privacy? Permission?)

How to avoid contradictory or missing data breach notifications?

Does the community have a consistent view on the responsibilities?

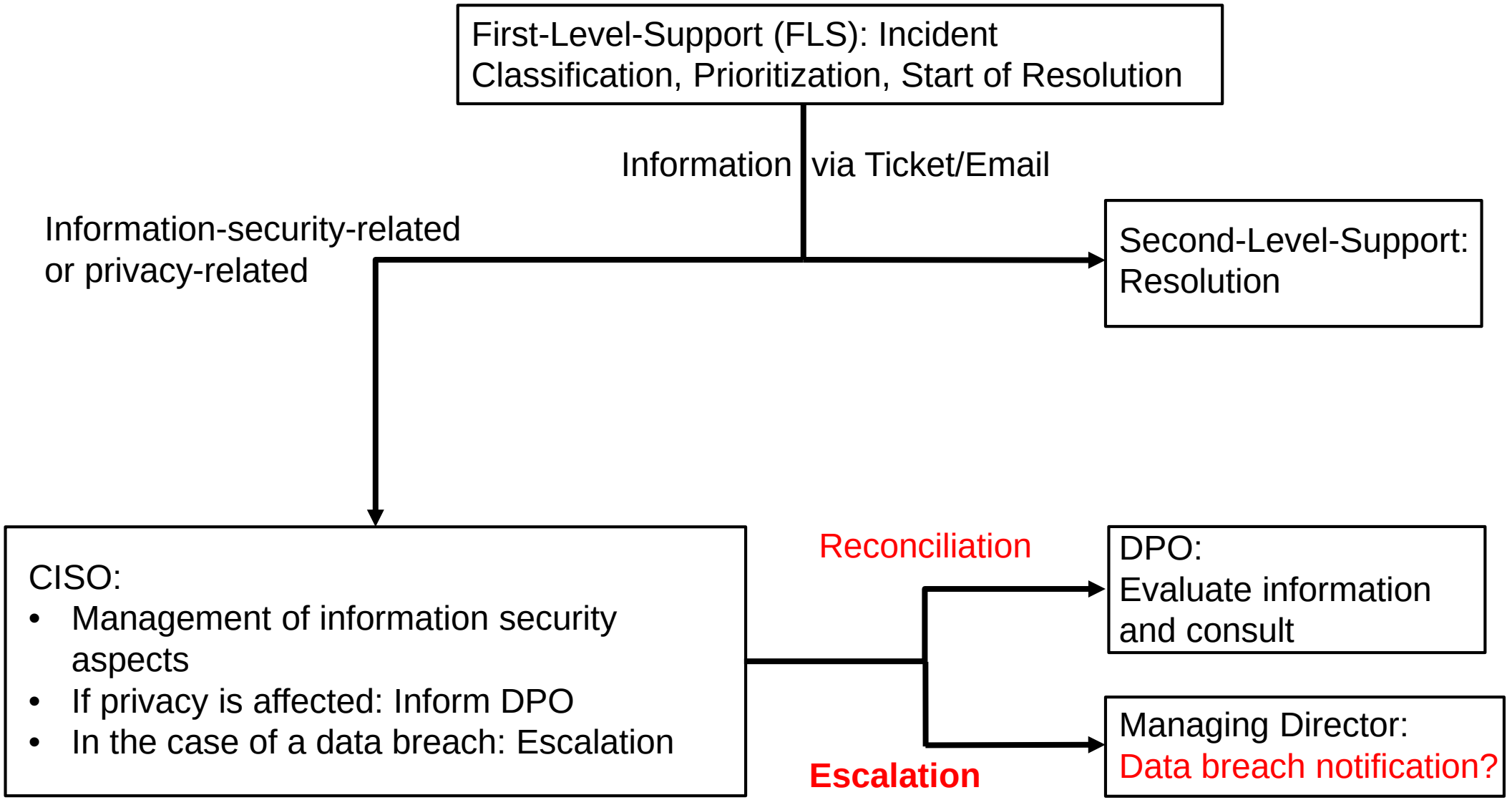
How to adopt the incident management process to fulfill the obligations?

Internal approach of LRZ

Modification of the internal security incident management process:

- Data breach as special case of a security incident
- Additional branches for risk and privacy management
- Consolidation of results of both branches

Internal approach of LRZ: Modification of Security Incident Management Process



Discussion: Current Incident-related Activities

How to adopt the incident management process for the collaborative service delivery?

- In the international context?

Which activities or projects in the community are working on aspects like

- Incident management?
- Security incident management: SIG-ISM, TF-CSIRT, SIRTFI, LRZ, others?
- Privacy: Task Force Data Protection, others?
- Crisis Management and business continuity: CLAW, others?
- Other activities within the community or in different organizations?

How to achieve a common approach considering existing activities, results?

- Prevention of reinventing the wheel

Discussion: Next Steps

Proposal

- Investigation of the status of current incident-related activities and projects
  - **Who?**
- Development of a potential common approach for data breach and incident management
  - Under consideration of the results (above)
  - **Who?**
- Presentation of status on next Task Force Data Protection meeting?