Security at CC-IN2P3

FJPPN 20260210

Agenda

- Introduction
- Cybersecurity Organization at CNRS
- Cybersecurity Organization at IN2P3
- Cybersecurity Organization Landscape
- Key Cybersecurity Challenges at CC-IN2P3
- Threats and Risks
- Security Measures and Best Practices
- Case study: Cybersecurity at CC-IN2P3
- Future Challenges and Roadmap

Introduction

- Overview of CNRS and IN2P3:
  - Pivotal role in French, European and international scientific research, in particular in nuclear, particles and astro particles physics.
  - Key position in scientific data storage and data treatments for WLCG but also other tens of scientific experiments.

- Importance of cybersecurity:
  - To guarantee availability, integrity and security of the services and for science data.
  - To maintain a high level of confidence and credit with partners.

Cybersecurity Organization at CNRS

- French Government
  - Prime minister, General Secretariat for Defence and National Security
- French Ministry of Higher Education, Research and Space
  - Defense security officer (FSD)
- CNRS
  - Direction
  - Defense security officer (FSD)
  - National security cell of the CNRS (RSSI-C)
  - Regional security officer (RSSI-DR)

Cybersecurity Organization at IN2P3

- IN2P3
  - Institutional security officer (RSSI-I)
- Centre de Calcul IN2P3
  - Direction
  - Local security officer (CSSI)
  - Security policy based on ISO27001 rules
- Collaboration with agencies:
  - ANSSI (French National Cybersecurity Agency)
  - CERT RENATER (French National Research and Education Network operator)
  - EGI/SVG and WLCG security groups

Cybersecurity Organization Landscape

Prime Minister / SGDN

Res. & Ed. Ministry

FSD

CNRS

FSD

Direction

CNSSI / RSSI-C

IN2P3

RSSI-I

RSSI-DR

CC-IN2P3

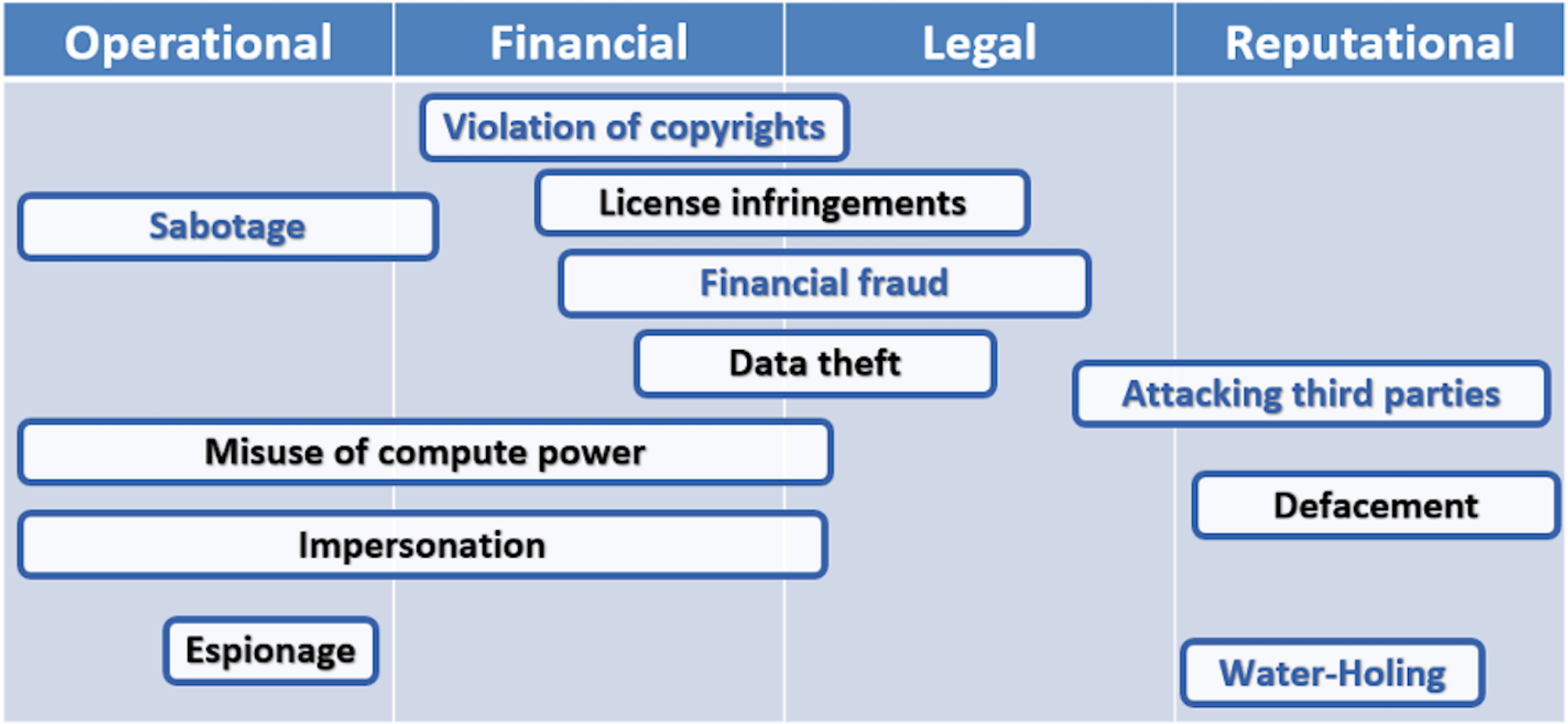
Direction

Local Security Officer

Key Cybersecurity Challenges at IN2P3

- **Many risks**:
  - Distributed computing, sensitive data and international collaborations.
- **Real-world threats**:
  - Phishing, ransomware, compromise, hijack of resources..
- **Regulatory compliance**:
  - Compliance with French/EU regulations (e.g., RGPD/GDPR, NIS2 Directive, LCEN) and internal CNRS policies (PSSI).

Threats and Risks



Security Measures and Best Practices

- Technical measures:
  - Network security (firewalls, intrusion detection, segmentation)
  - Endpoint protection (antivirus, patch management, encryption).
  - Access control and authentication (IAM, MFA, role-based access).

- Organizational measures:
  - Training and awareness programs for staff and users.
  - Incident response plan and collaboration with various emergency response teams (ANSSI and EGI/WLCG documentation and procedures).
  - Regular audits and compliance checks.

Case Study: Cybersecurity at CC-IN2P3

- Securing infrastructure:
  - Push SSL/TLS everywhere.
  - Strengthen access control for services and network.
  - Automate deployments and updates.

- Success stories:
  - Continuous mail flow control system detection.
  - ZneTS detects abnormal traffic during the latest security incident

- Lessons learned:
  - Importance of deploying updates in time.
  - Importance of controlling accesses.

Future Challenges and Roadmap

- Emerging threats:
  - Quantum computing.
  - AI-driven attacks.
  - Evolving regulatory landscape and geopolitical context.

- Current and ongoing initiatives:
  - Account lifecycle management.
  - Multi Factor Authentication.
  - Intrusion Detection Systems.

- Call to action:
  - Encourage the staff and users to remain vigilant, participate in training, and report incidents.

Conclusion and Q&A

- Summary of key points:

Thank you !