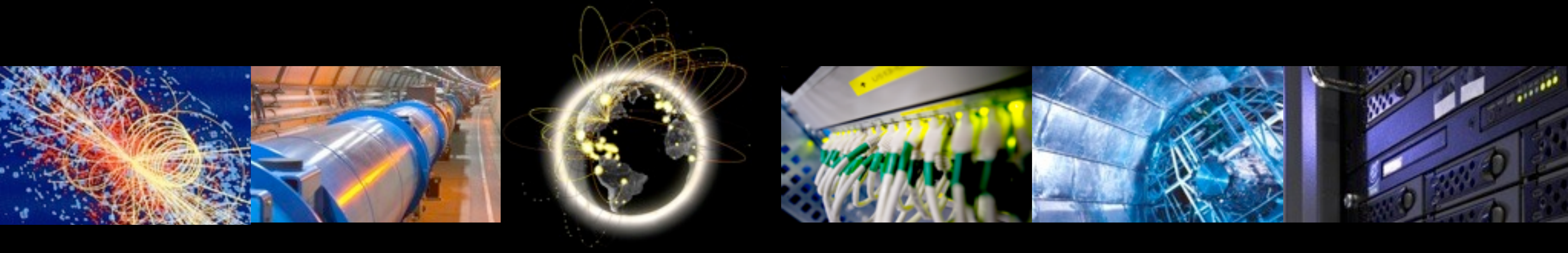
WLCG Computer Security risks analysis

WLCG Management Board, 20th March 2012



Process

- WLCG Risk analysis
  - First task of the Security TEG
  - https://espace.cern.ch/WLCG-document-repository/Boards/MB/WLCG_Risk_Assessment.pdf
  - “Live document”
- Objectives of the document
  - Identify our assets (what we want to protect)
  - Identify the main threats stemming from malicious intents
  - Score and highlight the most important risks
    - Based on likelihood of each threat
    - Based on the typical impact of the realisation of the threat
  - Discuss the risks and how they affect our assets

Risk analysis

- highlighted the need for fine-grained traceability
  - Essential to contain, investigate incidents, prevents re-occurrence
- Aggravating factor for every risk:
  - Publicity and press impact arising from security incidents
- 11 separate risks identified and scored. Top risks:

Risk
Misused identities (“SSH”-type included)
Attack propagation between WLCG sites
Exploitation of a serious OS vulnerability
Threats originating from trust services
Negative publicity on a non-event
Insecure configuration leading to undesirable access
Insufficient protection of information leading to sensitive data leakage
Incidents on resources not bound by WLCG policies
Exploitation of a serious VO/middleware software vulnerability
Data removal/corruption/alteration
DoS from an external organisation

Goals

- Identify the areas where risks have to be managed
- Prioritise the efforts to improve our security
- Evaluate how well a given control and security measure is effective at protecting our assets
  - Measure costs vs benefits
- Future work
  - Propose recommendations and mitigations