Federal Office
for Information Security

Two Aspects of Exercising Cyber Incidents

Susanne Jantsch

Federal Office for Information Security
Situation Centre and CERT-Bund

ENISA's 1st International Conference on Cyber Exercises
Paris, 27 June 2012

Outline

Two aspects of exercising cyber incidents:

- On the “local” scale:

  Internal (ICT) incident and emergency management

- On the “global” scale:

  Management of a (nation-wide) crisis due to ICT incidents

Internal incident and emergency management

- BCM → should comprise ...
- No BCM?
  - Start your BCM process (e.g. via BSI Standard 100-4) or follow special requirements or...
  - At some point will include: **Do exercises**

Note: so far, not limited to ICT/cyber

Internal ICT incident and emergency management

- ICT emergency exercises? How?

- What kind of exercises?
- How to get started?
- Too much effort?!

For more info, see last slide

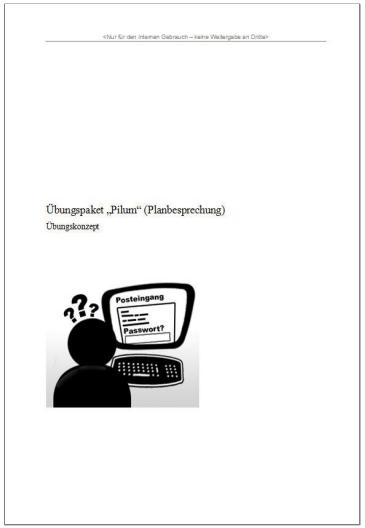
Idea: provide a semi-finished product

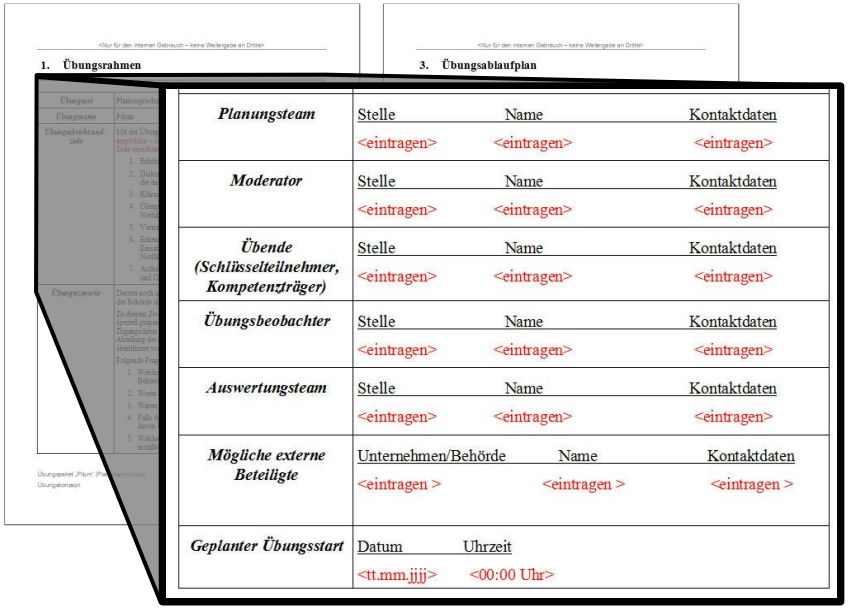
Sample Exercises

- "Generic", not too complex **exercise "template" sets**
  - Tabletop exercise
  - ICT emergency plan test
  - COMEX
- Realistic scenarios (e.g. DDoS, malware infections, insider jobs, loss of reputation, political impact)
- Purpose
  - **Facilitate internal exercises**
  - **Reduce preparation efforts**
    - Minimum: just customise to the institution (fill in names, roles, time …)
    - **Recommended**: Think! Adapt to **YOUR** organisational needs!
    - Optional: introduce org-specific details, increase complexity, ...

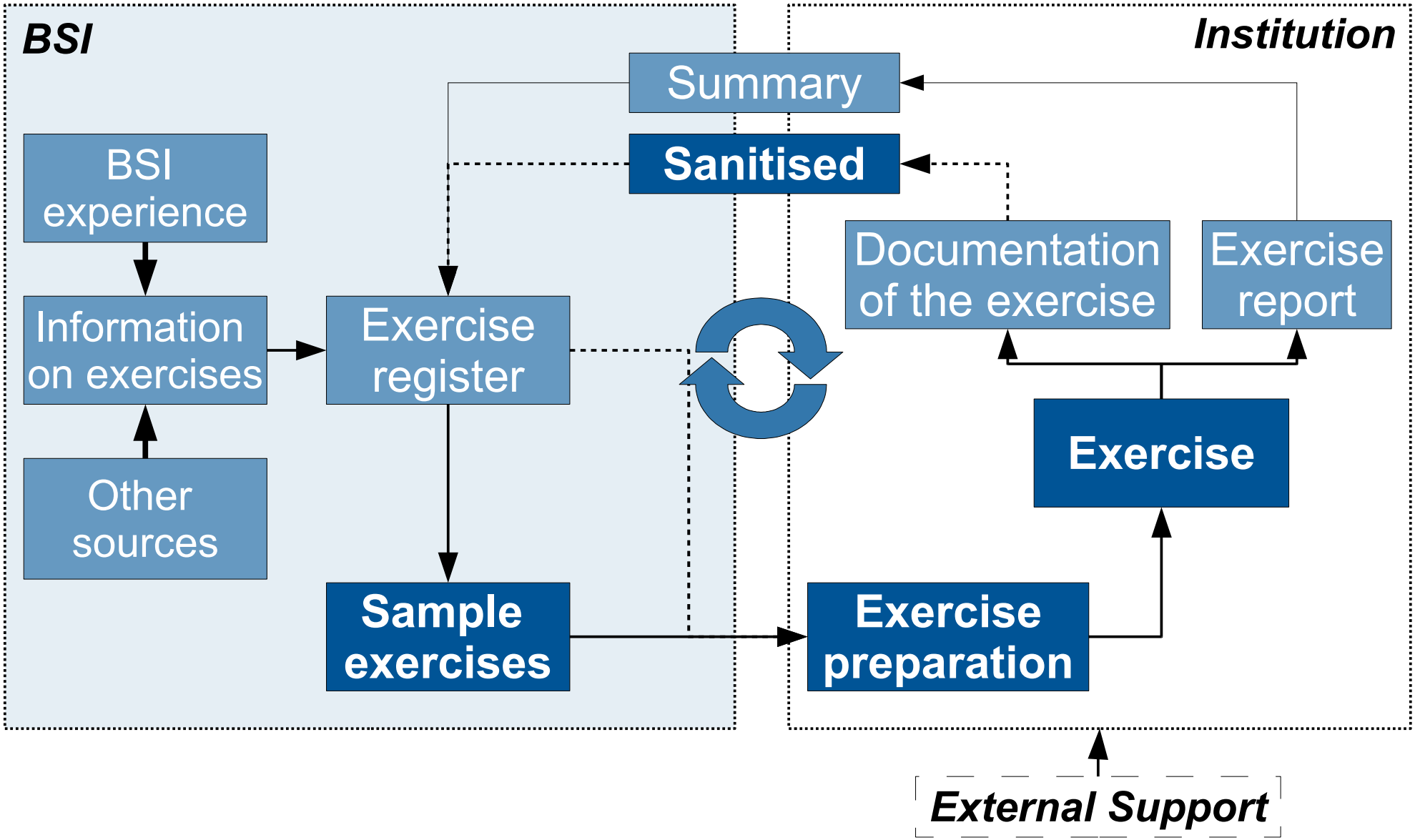
Contents of a sample exercise

- Brief description
  - Scenario outline
  - Recommended audience
  - Purpose
  - Complexity /effort
- Exercise concept
- Slides or script
- Templates for
  - Invitations
  - Protocol
  - Report
- Extra material where required, depending on exercise





Aim: “give and take”



The other aspect

When “local” cyber incidents aren't as local as they seem...

Crisis management exercise example: Germany's LÜKEX

- **LÜKEX** = **L**änder**ü**bergreifende **K**risenmanagementübung/**Ex**ercise*
  (cross-Länder crisis management command post exercise)
- Participants: Crisis management staffs from federal and Länder levels plus CIP plus selected participants on community level
- Series of Exercises
  - 2004: Power Outage
  - 2005: Big Sports Event (Preparation for WM 2006)
  - 2007: Pandemia
  - 2009/10: Terrorist attacks and threats (dirty bomb)
- Duration: about 2 days

*Organised by the Federal Office of Civil Protection and Disaster Assistance (BBK) under the auspices of the BMI

LÜKEX 11

- Theme of LÜKEX 11: cyber incidents
- However: LÜKEX 11 was **NOT** a cyber exercise
  - It was still a **strategic crisis management exercise**
  - **It used an ICT scenario**
- Audience (as in the LÜKEXes before)
  - general crisis management staff (high policy level)
  - police officers, firefighters, disaster recovery, civil protection, ...

  CERTs, CISOs, CIOs, IT service providers etc. participated from the second row

LÜKEX 11
Scenario overview

- ICT incidents had increased steadily before STARTEX
- At STARTEX
  - Knowledge about a new malware, but little details
  - Warning that “more will happen” on exercise day one
  - Several incidents hit the media
- During the exercise
  - Additional incidents occurring “locally”, all participating parties hit, some more, some not so bad.
  - (Fictitious) sample analysis reveals step by step details of the highly complex malware with several malicious functionalities
  - First consequences that are felt by the population
  - The media receive anonymous hints
  - Data leakages occur

LÜKEX 11
The challenges for the participants

- CM staff had to **deal with the CONSEQUENCES** on ICT
  - Assessment and plan of actions
    - Requires listening and talking to the ICT specialists
    - Integration of new aspects in the situational picture
  - Crisis communication!
- CERTs, ICT CM staffs, CISOs, CIOs, IT service providers in **two roles**
  - Acting as **advisers to their CM staff**
  - Responsible for **dealing with the (fictitious) ICT incidents** in their own realm
    - Assessment and coordination of measures
    - What information to share
    - Use information / advice coming in via information sharing

Lessons from LÜKEX as a combined exercise

- Use **existing** structures (here: crisis management)
- CM staff ARE dependent on ICT. **Make them aware!**
  - Make them understand the basics of your field
  - Translate the complex things!
  - Explain the differences

    e.g.: ICT is ubiquitous, instantaneous and simultaneous
- The non-ICT partners are also experts. **Learn from them!**

  Here: Staff organisation and staff work
- Cooperation with cyber-dependent parties is more than cooperation of their CIOs and CISOs...

Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Susanne Jantsch
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5026
Fax: +49 (0)22899-10-9582-5026

susanne.jantsch@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de
www.bsi.bund.de/IT-Krisenmanagement

Related links

- CIP Implementation Plan
  https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/Impleme
- IT Emergency and Crisis Management Exercises
  http://www.bmi.bund.de/cae/servlet/contentblob/560098/publicatio
- COMCHECK and ALEX
  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/co
- BSI Standard 100-4
  - https://www.bsi.bund.de/ContentBSI/EN/Publications/BSI_standar