



Mission Impact Module & Mission Impact Assessment

Workshop on Cyber Defence and Security

Alexander Motzek* of the Panoptesec project

* Universität zu Lübeck
Institut für Informationssysteme
Ratzeburger Allee 160, 23562 Lübeck, Germany
motzek@ifis.uni-luebeck.de

September, 8th & 9th 2015



Mission Impact Assessment - Central Question

Something is not available / impacted inside our infrastructure.

What does that mean for our company?

Hippocratic Oath: Do not cause any harm to the company.

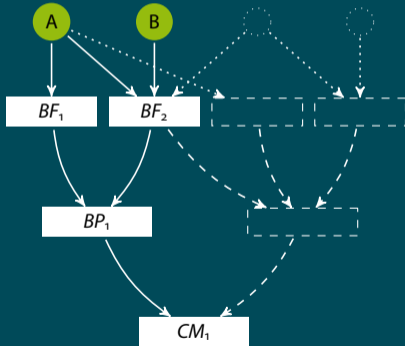


Approach - Dependency Models

- ▶ Requires experts with **broad expertise**
 - Unavailable

- ▶ Available: **Individual experts** with focused expertise
 - Three **different views**

View 1: The Company



- ▶ Dissect company into **smaller pieces**
- ▶ Business process modeling (**BPMN**)
- ▶ Three business layers

- ▶ **Mission Critical Devices** (A&B)
scratch surface of infrastructure

View 2: The Infrastructure



- ▶ Identified **MCDs** are only the **tip of an iceberg**
- ▶ **Identification might be inaccurate** from an operational view
- ▶ Not assessable, but verifiable by expert
- ▶ **Automatic dependency analysis**

View 3: The Impacts



- ▶ A **node** might be **impacted**
- ▶ e.g., **fail**, crash, attacked, **patched**

- ▶ **Will impact** dependent nodes...
- ▶ ... will impacted business processes...
- ▶ Will impact **the company**.



Mission Impact Assessment

- ▶ Given a set of impacted nodes, is the **company impacted** as well?
- ▶ Assessed through well-defined **Graphical Probabilistic Model**
- ▶ **Combines** all three **disjoint expertise** based on probability theory



Panoptesec

- ▶ **Analyzes potential countermeasures** for their impact to the company.
- ▶ *“Shutting a server down, might be even more harmful than a potential attack”.*
- ▶ **Do not harm a mission through collateral damage.**



Panoptesec

Live Demo