A Common Process Model for Incident Response and Digital Forensics

IMF 2007, Stuttgart, September 2007

Felix C. Freiling
Laboratory for Dependable Distributed Systems
University of Mannheim, Germany

Bastian Schwittay
Symantec (Deutschland) GmbH, Germany

Communications of the ACM, 48(8), 2006

Motivation

- Analysis of digital evidence can put people into jail
- Only generally accepted, scientific methods should be applied in the analysis
- Frameworks for performing this analysis are called **process models**
- Different process models have emerged for different areas
- Can they be unified?

Examples: Incident Response and Digital Forensics

- Incident Response (IR): detect and contain computer security incidents
- Digital Forensics (DF): obtain valid evidence for (cyber)crime
- Highly related disciplines with a lot of overlap

- Aim: unified view of IR and DF using a Common Process Model

Agenda

- Background
  - Incident Response
  - Computer Forensics
- Common Model: Unifying IR and CF
- Summary and Discussion

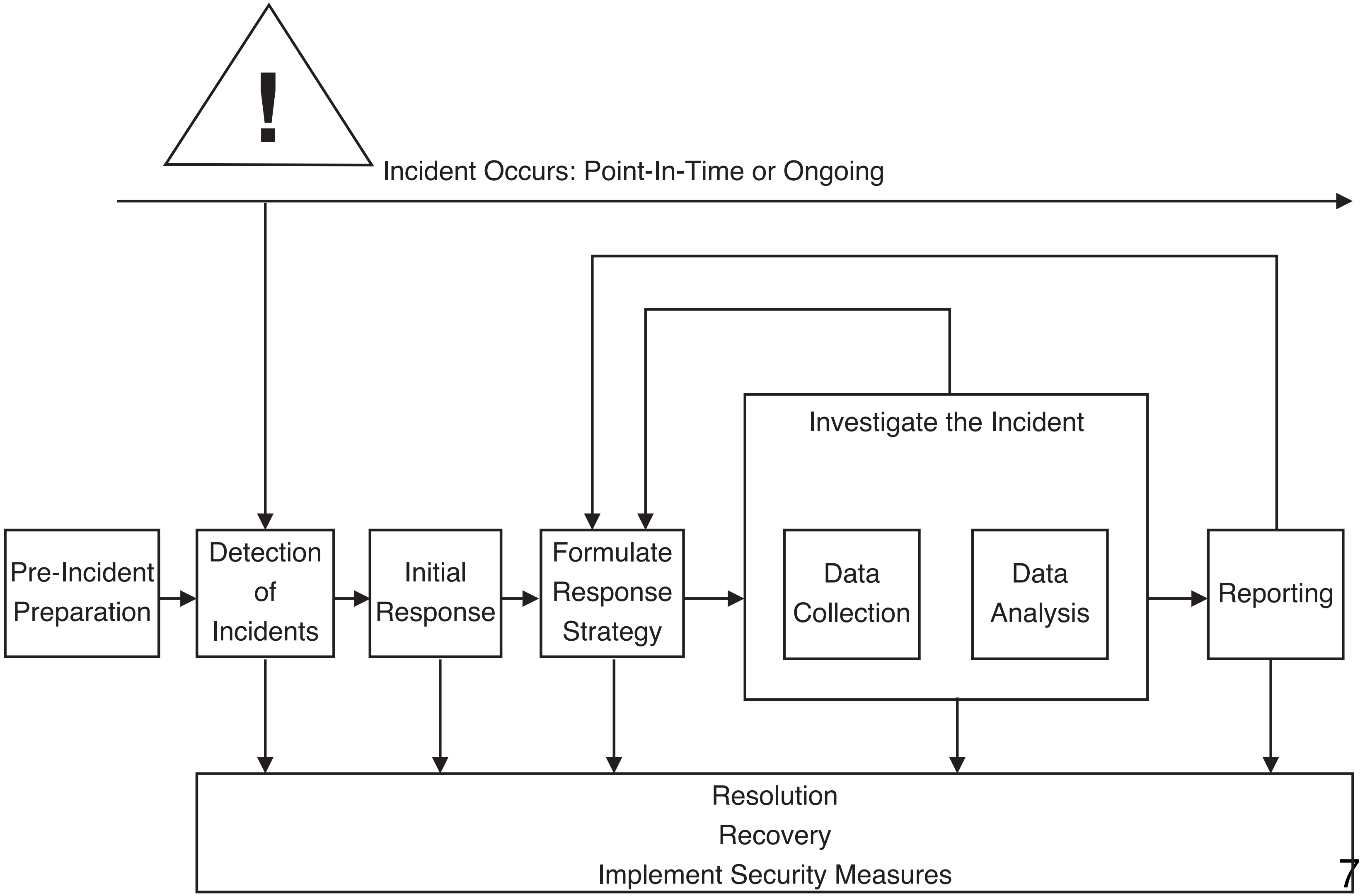
Background: Incident Response (IR)

- **Computer Security Incident** is a „violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." [NIST, Computer Security Incident Handling Guide]
- **Incident Response**: Detection and containment of computer security incidents
- Focus on quick remediation and return to day-to-day business
- Root cause analysis may be skipped to prevent costs, interruption of business, etc.
- Structured approach to IR process

IR Process Model

- Process model structures the investigation so that investigators make less errors
- Standard reference:
  - Kevin Mandia, Chris Prosise, Matt Pepe: Incident Response & Computer Forensics. 2nd Ed., McGraw-Hill, 2003.
- Process model of Mandia et al.
  - 7 phases ...

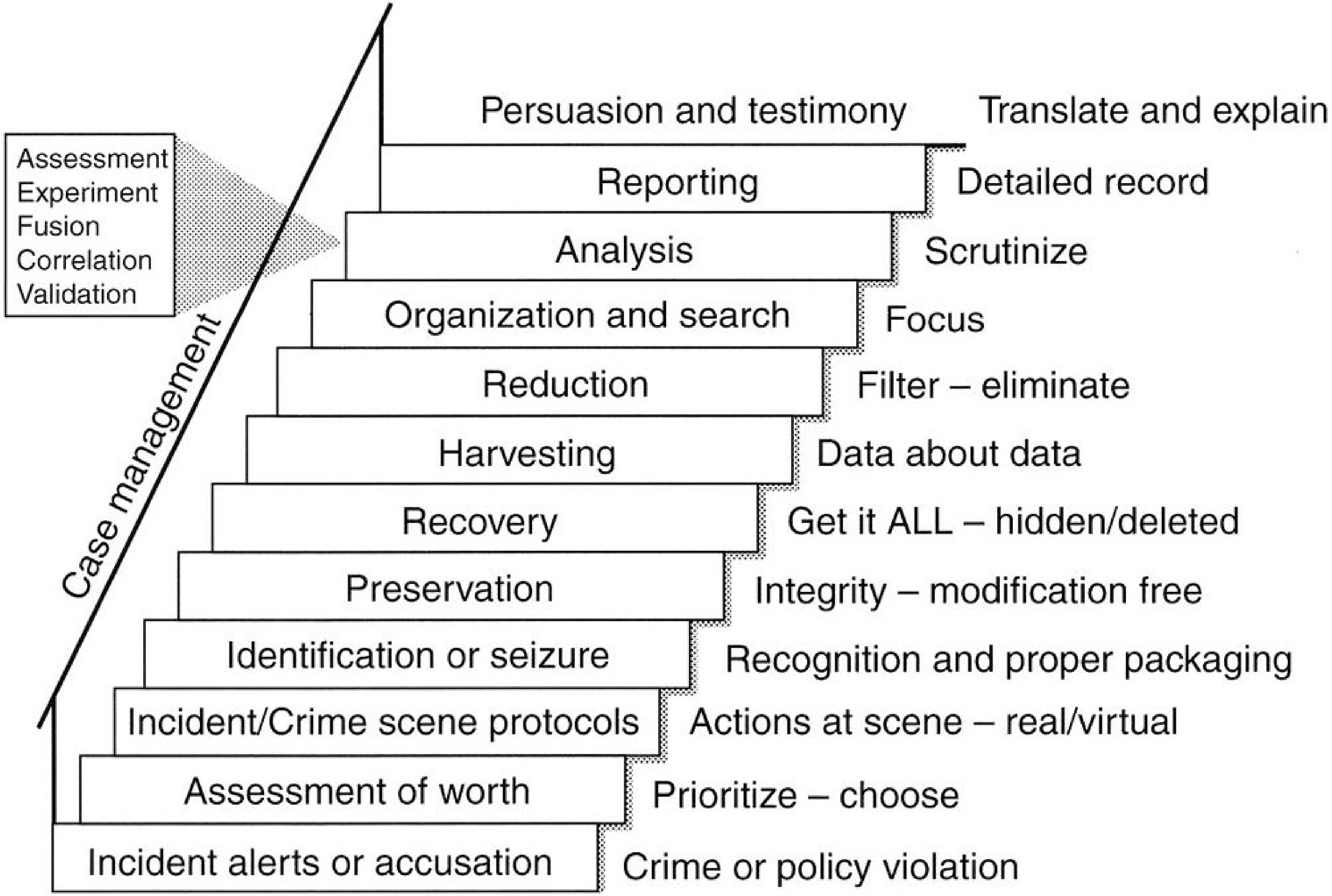
IR Process Model (Mandia et al.)



Background: Digital Forensics (DF)

- Part of forensic science: Obtain, analyze and present **digital evidence**
- Evidence handling suitable for a court of law
- Reliable, repeatable and well-documented methods for analysis
- Process model of Casey: **Investigative Process**
  - General model for digital investigations
  - Includes tasks of first responders
  - De facto standard
- Eoghan Casey: Digital Evidence and Computer Crime. 2nd Ed., Academic Press, 2004, Kapitel 4.
- 11 phases ...

Investigative Process Model



Assessment
Experiment
Fusion
Correlation
Validation

Case management

Persuasion and testimony	Translate and explain
Reporting	Detailed record
Analysis	Scrutinize
Organization and search	Focus
Reduction	Filter – eliminate
Harvesting	Data about data
Recovery	Get it ALL – hidden/deleted
Preservation	Integrity – modification free
Identification or seizure	Recognition and proper packaging
Incident/Crime scene protocols	Actions at scene – real/virtual
Assessment of worth	Prioritize – choose
Incident alerts or accusation	Crime or policy violation

Comparison: IR vs. DF

- IR puts focus on:
  - Management and quick containment of the security incident
  - Integration of investigation into the business processes of an organization
  - Usually quick return to service
- DF puts focus on:
  - Detailed and careful handling of digital evidenve and analysis
  - Scientific approach
- Orthogonal aspects

Agenda

- Background
  - Incident Response
  - Computer Forensics
- **Common Model: Unifying IR and DF**
- Summary and Discussion

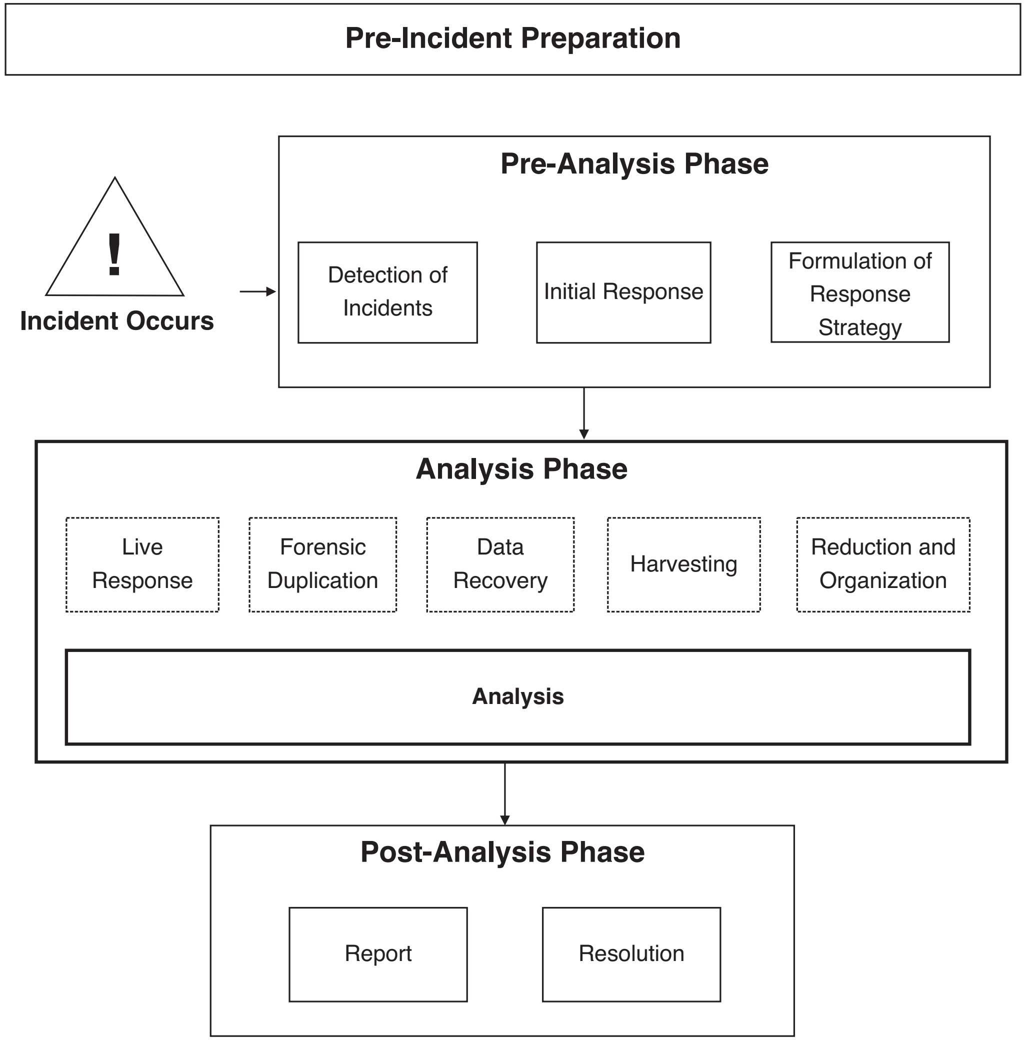
The Common Model (CM)

- Combine IR and DF processes:
  - Adds a management aspect to DF
  - Adds choice of suitable response strategy to DF
  - Adds option to conduct full-scale forensic analysis to IR

- Three phases to structure the response to a computer security incident
  - Pre-analysis phase
  - Analysis phase
  - Post-analysis phase

- Each phase divided into multiple steps
- Pre-Analysis phase determines depth of analysis phase

Common Model: Overview



Pre-Incident Preparation

Incident Occurs

Pre-Analysis Phase

Detection of Incidents

Initial Response

Formulation of Response Strategy

Analysis Phase

Live Response

Forensic Duplication

Data Recovery

Harvesting

Reduction and Organization

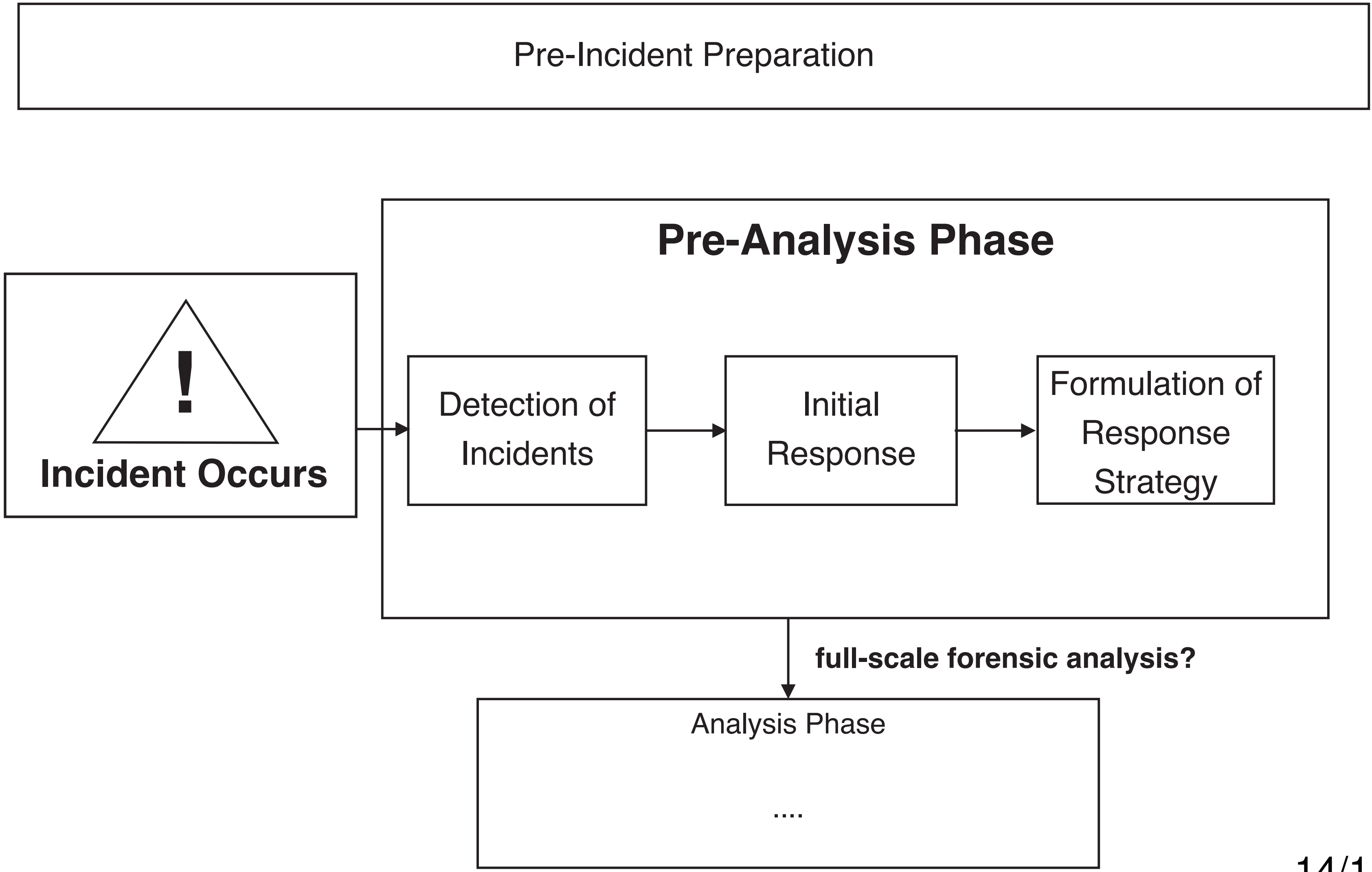
Analysis

Post-Analysis Phase

Report

Resolution

Pre-Analysis Phase


Pre-Incident Preparation

Incident Occurs

Pre-Analysis Phase

Detection of Incidents

Initial Response

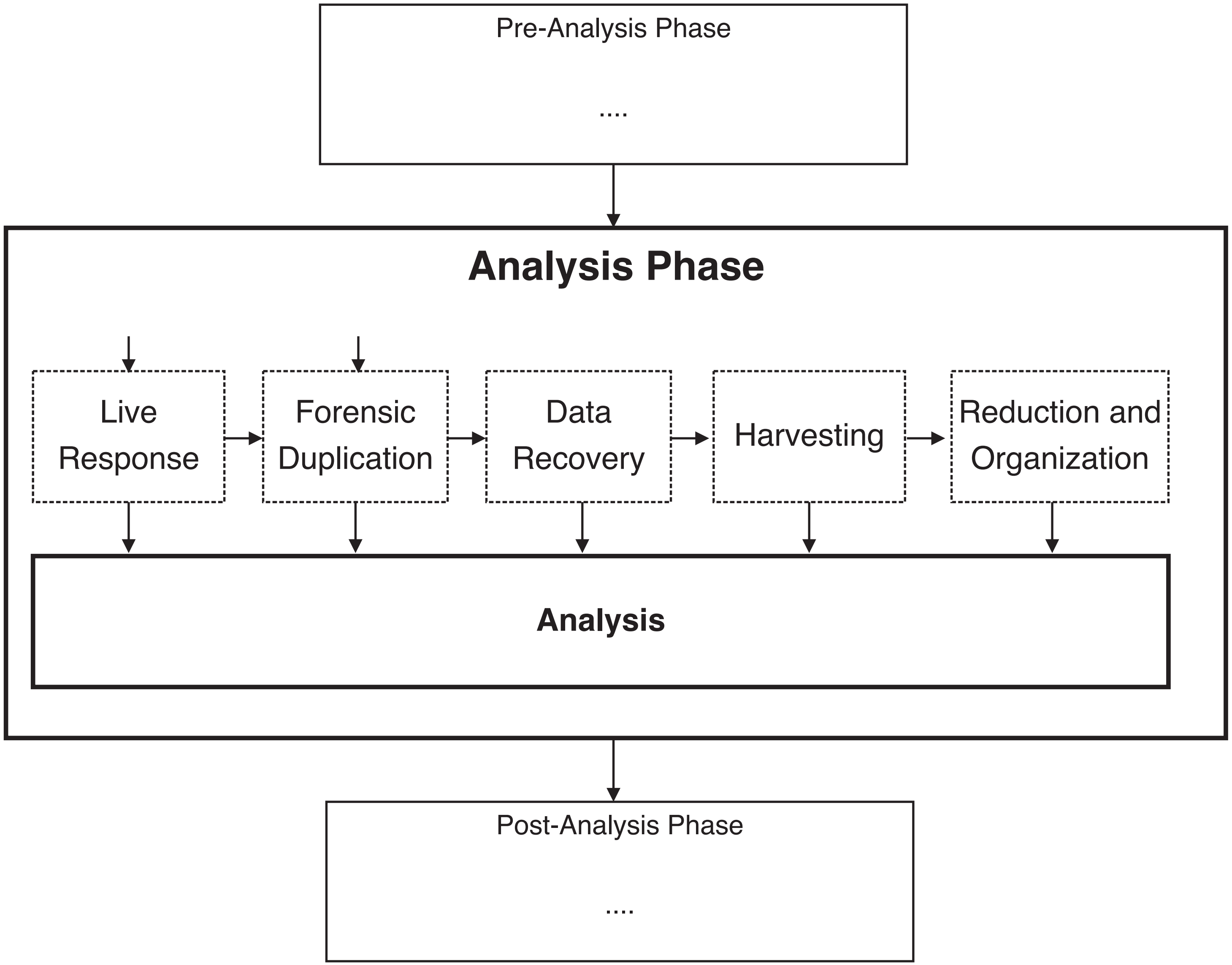
Formulation of Response Strategy

full-scale forensic analysis?

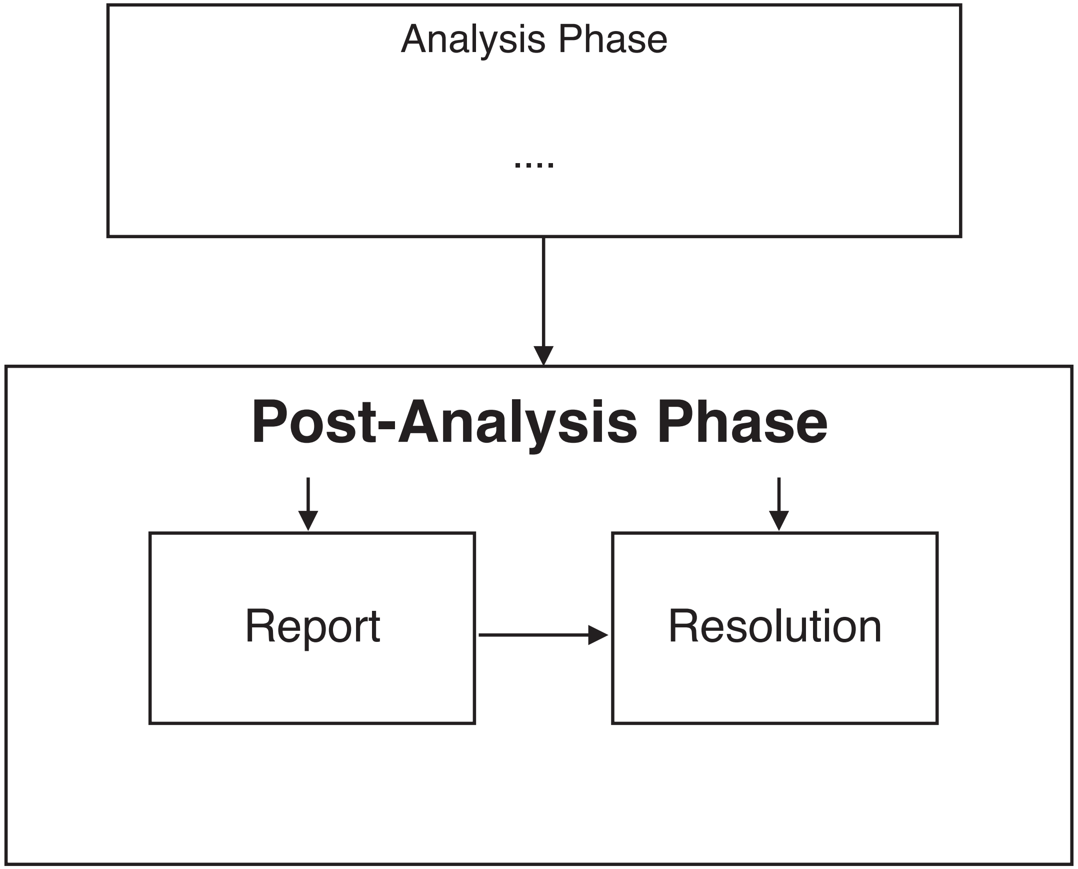
Analysis Phase

....

Analysis Phase



Post-Analysis Phase



Discussion (1/2)

- Unified view of IR and DF
- Flexible approach:
  - Takes organisational issues into account
  - Enforces scientific rigor where appropriate

- When to do a full-scale forensic analysis?
  - Hard factors:
    - Response posture: Does the organization follow a „zero tolerance" policy?
    - Legal constraints: Must the incident be communicated to the police?
  - Soft factors:
    - Attacker threat level: Does the attacker represent a great threat?
    - Potential damage: Is the expected damage large?

Discussion (2/2)

- Formalized criterion for soft factors:

  Attacker Threat Level x Potential Damage > X

- Similar to risk equation:

  Risk = Threat x Vulnerability x Cost

  - AttackerThreatLevel ~ Threat
  - Potential Damage ~ Cost
  - „Vulnerability = 1": incident has already occured

References

- Felix Freiling: Vorlesung Digitale Forensik. Frühjahrssemester 2007, Universität Mannheim, Chapter 4.
- `http://pi1.informatik.uni-mannheim.de/filepool/teaching/forensik-2007`
- Bastian Schwittay: Towards automating analysis in computer forensics. Diplomarbeit, RWTH Aachen, Department of Computer Science, 2006, Chapters 2 and 3. `http://pi1.informatik.uni-mannheim.de/filepool/theses/diplomarbeit-2006-schwittay.pdf`