OMG Common Threat Model

Joint OMG/NSA Workshop on Building and Using Secure ORBs April 1997

Henry Rothkopf - U.S. Government

Dr. Patrick Mallett - MITRE

R. Neil Wagoner - MITRE

Don Faatz - MITRE

Objective of Presentation

- Describe the threat model being developed by the OMG Security SIG Common Threat Model Working Group
- Report status

Organization

- Common Threat Model Working Group
- Interpretations of threats and concerns might be different
- Example of a common threat
- The road we should be on
- Approach to building the Common Threat Model
- Definition of terms and metrics
- Suggested set of initial generic threats
- Discussion of attached handouts, e.g., presentation matrix for the Common Threat Model
- Current timetable

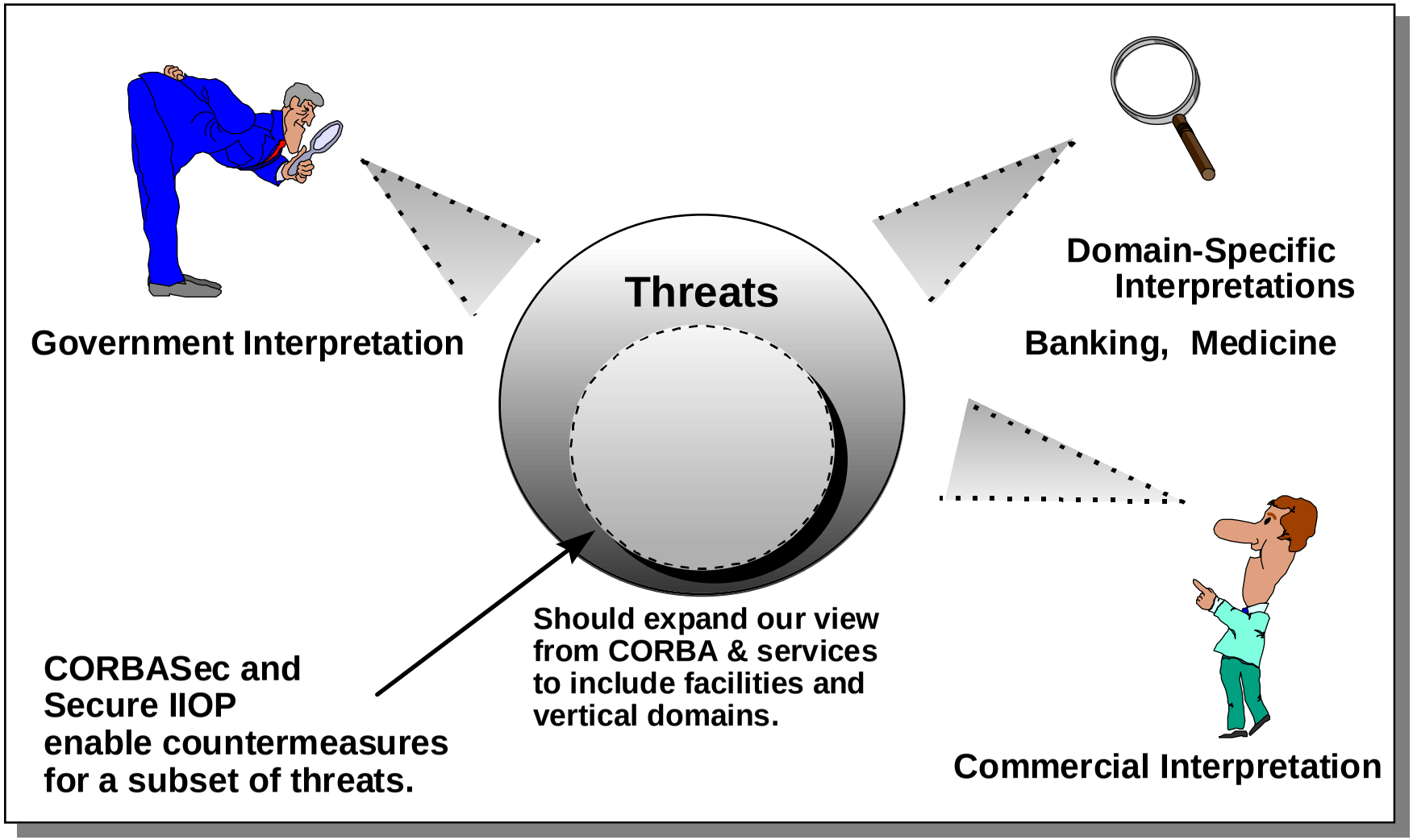
Common Threat Model Working Group

- CTM WG meetings held in Tampa, Jan 97 and Austin, Mar 97
  - Chair: Dr. Patrick Mallett
- Charter
  - Identify and document threats and concerns from all vertical domains (i.e., business areas) to build a common threat model that can be used to:
    - Ensure completeness of the CORBA Security Specification
    - Support a common consensus for any needed changes to the CORBA Security Specification
    - Educate the larger community on the importance of security
- The model will be documented in an informational white paper along with educational briefings

Common Threat Model Working Group (Concluded)

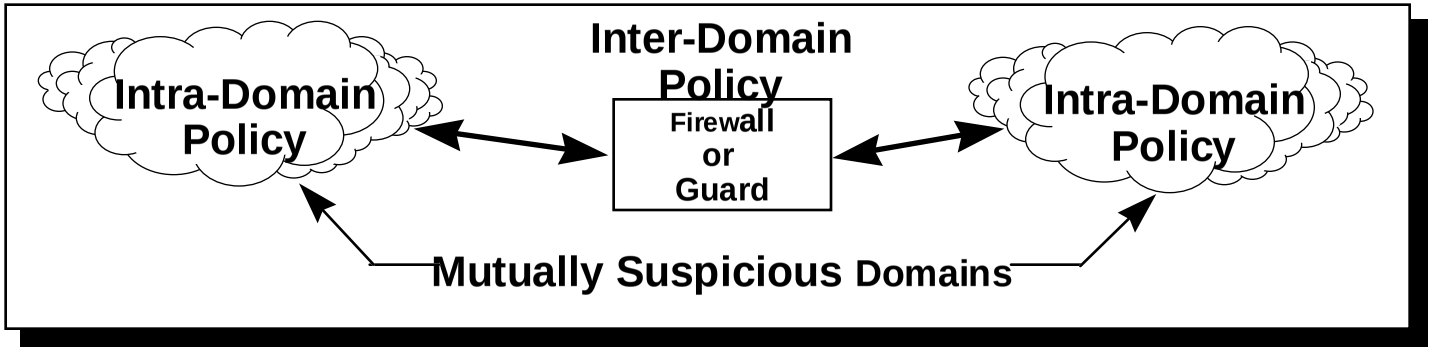
- The group agreed that the threat model should include the following:
  - Domain interpretations of the concerns and threats in specific terms relevant to that business area, with description of likely damage
  - A set of generic threats factored from the threats identified in the various domains
  - A set of generic countermeasures or security services needed to defeat or mitigate the generic threats

Interpretations of Threats and Concerns Might be Different



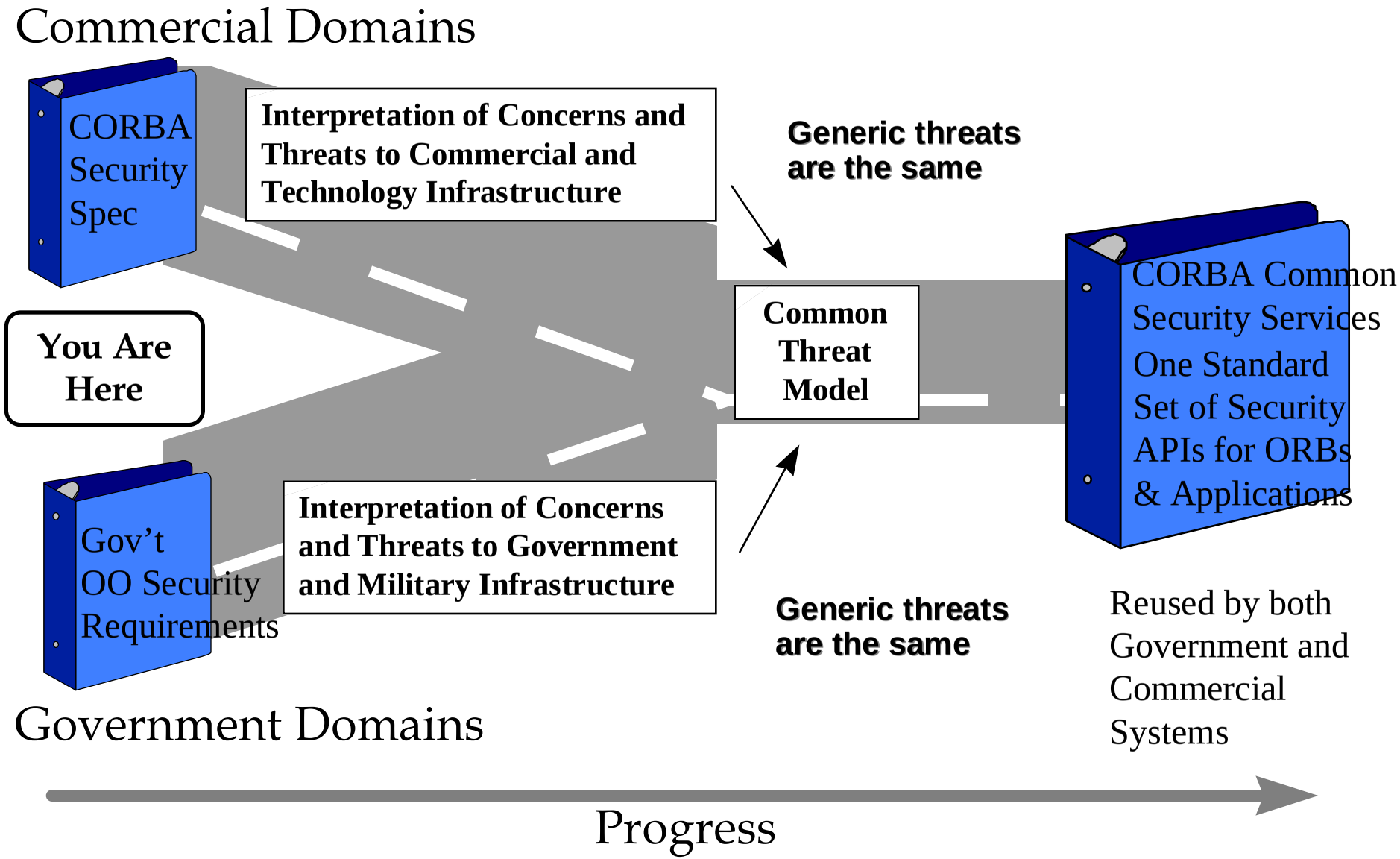
Example of a Common Threat

- Unauthorized access of information from external domain
- Government and commercial countermeasure patterns are the same
  - Assurance requirements may be stronger for Govt.

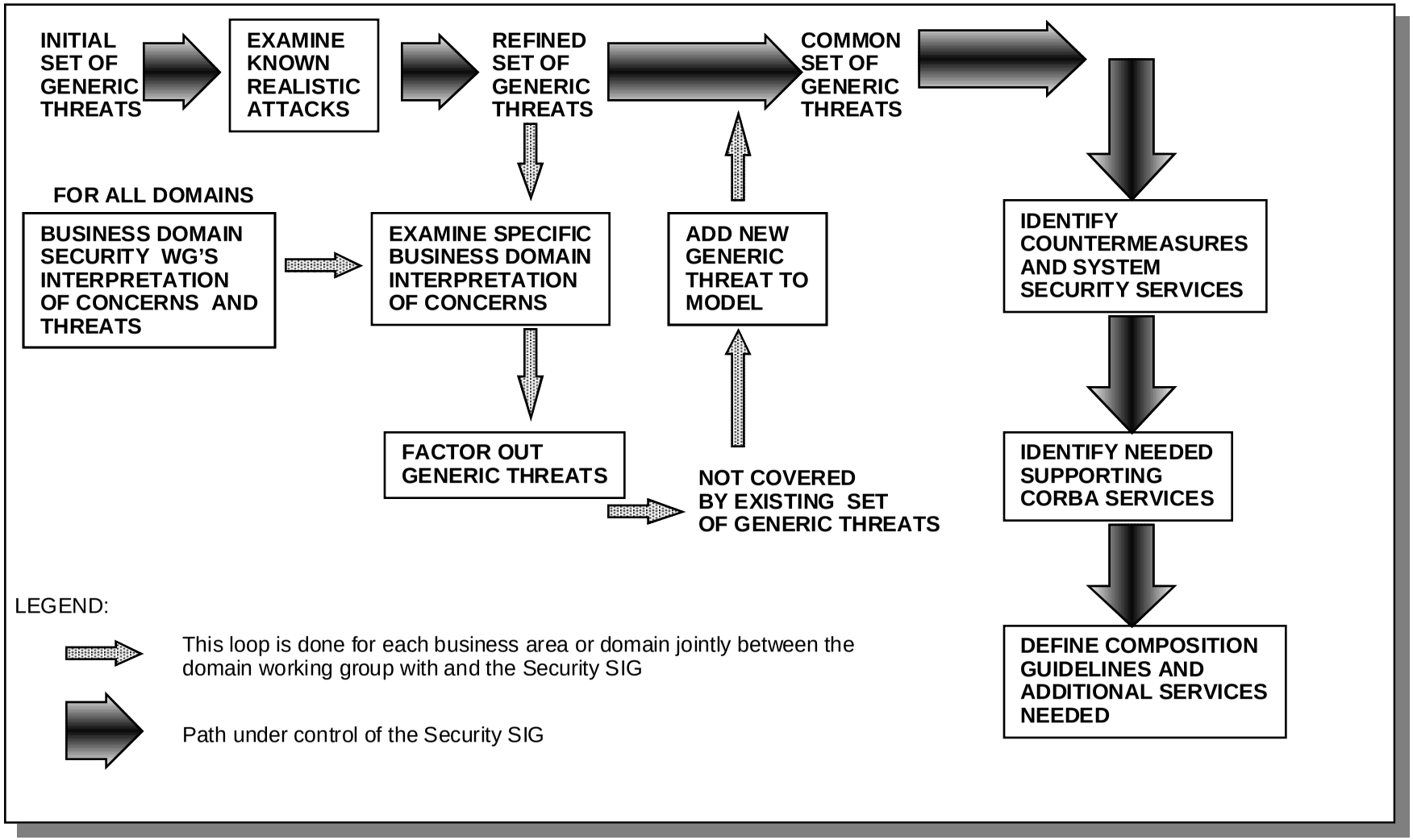


- Government and industry use the same technologies for information systems
  - Types of loss due to compromise may be different
- Information warfare attacks are equally likely against commercial and government targets

The Road Were On



Approach to Building the Common Threat Model



Definition of Terms and Metrics

- Threat
- Vulnerability
- Countermeasure
- Scenario
- Likelihood
- Harm
- Impact
- Risk

Definitions [re CORBA Sec Appx E]

- **Threat**
  A potential system misuse that could lead to a failure in achieving the system security goals

- **Vulnerability**
  A system weakness that leaves the system open to one or more threats

- **Countermeasure**
  A measure or technique for countering or mitigating the effects of a threat

Definitions

- **Scenario**
  An example of given type of threat

- **Likelihood**
  A metric describing the probability of a given threat occuring

- **Harm**
  The type or description of damage to the system (or enterprise) resulting from a successful threat
  (The CTM uses 4 categories or types: unauthorized disclosure, denial of service, unauthorized manipulation, and unauthorized use)

- **Impact**
  A metric describing the seriousness of damage to the system (or enterprise) resulting from a successful threat

Definitions

- **Risk**
  A metric describing the degree to which use of the system exposes the system or enterprise to potential harm; relative to any specific threat, risk is a function of:
  - ***Likelihood of the threat***
  - ***Impact if the threat attack is successful***
  - ***Effectiveness of countermeasures to the threat***
- ***In some cases, it is also useful to define a risk metric based on only the first two factors (before considering the effect of countermeasures)***

Likelihood Metric

- **Low**
  - **Highly unlikely and not expected to occur; requires conspiracy and/or expert-level knowledge**
- **Medium**
  - **May occur under unusual circumstances; requires a single user with operator-level knowledge**
- **High**
  - **Expected to occur with some frequency; may occur during the course of normal operations (e.g., accidental errors)**

Impact Metric

- **Low**
  - **Minor damage due to data loss, corruption, compromise, or denial of service, such as violation of administrative policy**
- **Medium**
  - **Moderate damage due to data loss, corruption, compromise, or denial of service, such as release of sensitive information**
- **High**
  - **Extensive damage due to data loss, corruption, compromise, or prolonged denial of service, such as violation of highly sensitive data, endangerment of life, loss of integrity mechanisms, or corruption of security policy rules**

Risk as a function of Impact and Likelihood

Impact	Likelihood		
	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

Effectiveness of Countermeasure Metric (1/3)

- **Low**
  - **The countermeasure is widely believed to be weak or can be circumvented with moderate effort. For example, it may rely heavily on human (non-security personnel) security awareness. If countermeasure fails or is circumvented, component will continue to operate, and may result in denial of service and unauthorized disclosure, manipulation, and use of information. In some cases, the countermeasure may actually reduce security by inducing inappropriate user actions.**

Effectiveness of Countermeasure Metric (2/3)

- **Medium**
  - **Adversary must expend some time using available tools in order to circumvent the countermeasure. Such countermeasures may rely moderately on security awareness by non-security personnel, for example requiring operators to not inadvertently disclose vital data (e.g.., password, cryptographic key) or requiring operators to activate countermeasure in the face of eminent threat (e.g., zeroize button to clear key material). Generally, if countermeasure fails, component will continue to operate, and may result in unauthorized disclosure or manipulation of information.**

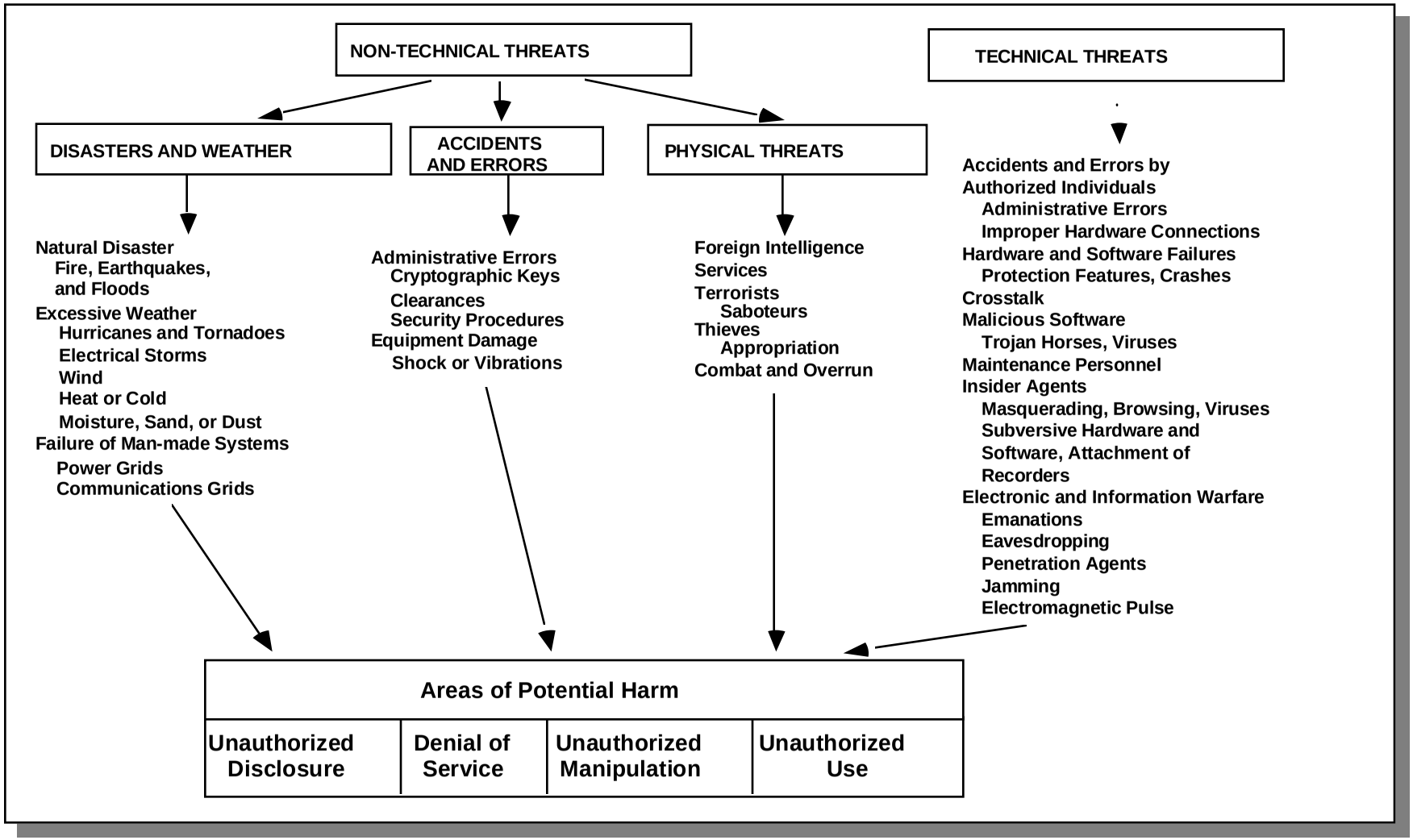
Effectiveness of Countermeasure Metric (3/3)

- **High**
  - **Adversary must expend inordinate amount of time and resources to attempt defeat of countermeasure. Examples include: using cryptographic or technical security protection mechanisms which are NSA endorsed or evaluated using criteria such as ITSEC or the Common Criteria; or employing Government-endorsed and widely accepted technical mechanisms and procedures. Generally, if the countermeasure fails, component will not operate, or failure does not result in unauthorized disclosure or manipulation of information.**

Risk Refined by Effectiveness of Countermeasure

Risk as a Function of Impact and Likelihood	Effectiveness of Countermeasure		
	Low	Medium	High
Low	Low	Low	Low
Medium	Medium	Low	Low
High	High	Medium	Low

Suggested Set of Initial Generic Threats



Handouts: Draft CTM

- Draft presentation matrix for the CTM
- New potential threats for consideration
- Major concerns from the NII threat paper
- Summary of Austin meeting
- Summary of threat discussions with the CORBA Medical Domain

Current Timetable

Jan 97 (Tampa)	Security SIG buy-in, start CTM WG Initial Threat Model
Mar 97 (Austin)	Input from Vertical Domains, Update Threat Model
Apr 97 (Baltimore)	Brief CTM at Work Shop
May 97 (Italy)	Input from Vertical Domains, Update Threat Model
Jun 97 (Quebec)	Draft for Comment Review with Security SIG
Sept 97 (Ireland)	CTM Completed, Brief to PTC