Operational Threat & Risk Information Sharing and Analytics

TEAM Threat

OMG
WE SET THE STANDARD®

ISE

ORACLE

IBM

demandware
move faster, grow faster.

Model Driven Solutions
Where Business Meets Technology

U.S. Department of Defense
DEFENSE SECURITY SERVICE

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

CAL OES

KDM Analytics

FUJITSU

RSA INTELLIGENCE DRIVEN SECURITY

NIST

LOCKHEED MARTIN

Draft specification artifacts

Specification Document (PDF): **http://tinyurl.com/qdfl6jl**

http://www.threatrisk.org/spec/RevisedSubmission/Revised%20Operational%20Threat%20Risk%20Submission.pdf

Specification Document (.DOC): http://tinyurl.com/p6ykkrm

http://www.threatrisk.org/spec/RevisedSubmission/Revised%20Operational%20Threat%20Risk%20Submission.doc

Specification .ZIP with all models: http://tinyurl.com/o2vkkss

http://www.threatrisk.org/spec/RevisedSubmission/Revised%20threat-risk%20Submission%20machine%20readable%20files.zip

Web view of models: http://tinyurl.com/q29clvk

http://www.threatrisk.org/spec/Threat%20Risk%20Model.html

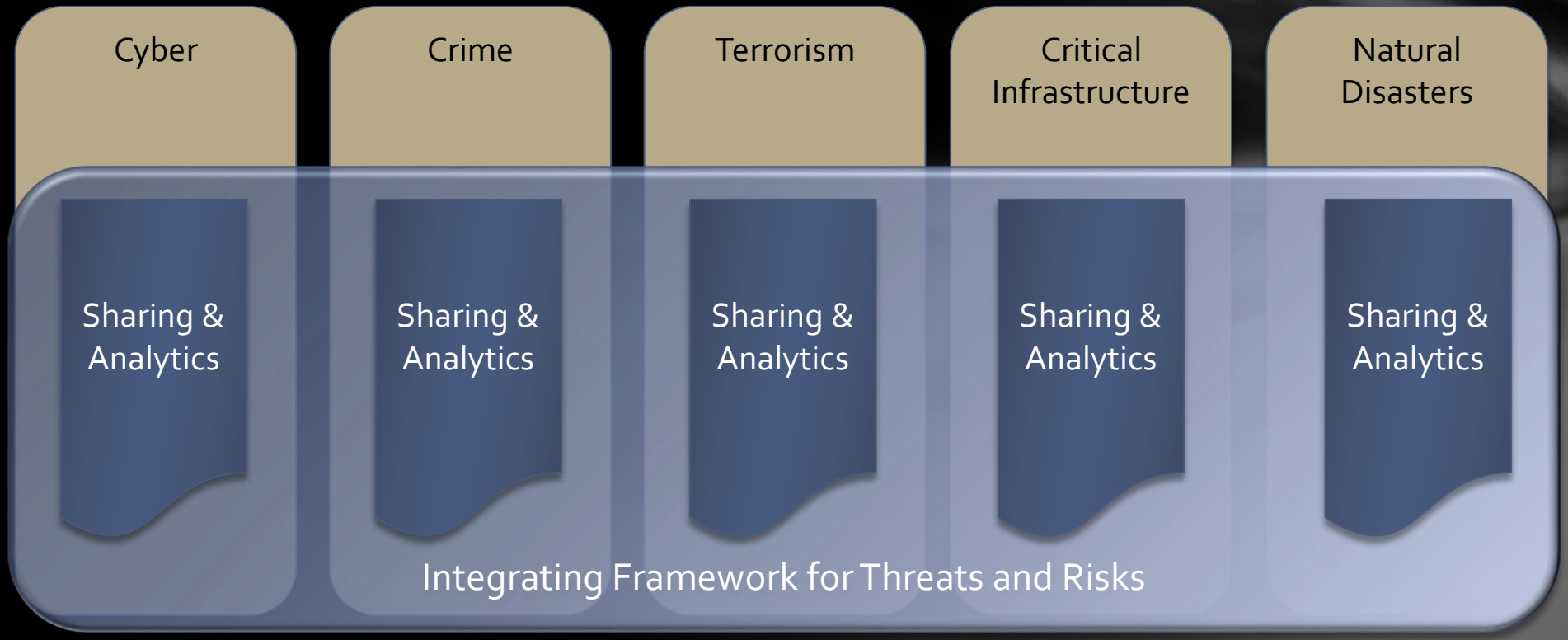
Community portal: http://threatrisk.org/

Download Now

Problem Space

- There is a critical need to understand and mitigate threats and risks – to "connect the dots".
- The Landscape of threats is changing
  - Multiple attack vectors, cyber/physical and other
  - Advanced threats utilize multiple vulnerabilities
- There are multiple communities addressing the same threats
  - Cyber/physical, emergency management, safety, defense, etc.
- No comprehensive consistent semantic framework
  - Existing systems provide insular treatment of threat/risk relationships
  - Comprehensive system would allow system-of-systems interoperability (private/private, public/private)

What we need is an integrating framework that supports automated data mapping



An integrating framework that helps us deal with all aspects of a risk or incident

A federation of risk and threat information sharing and analytics capabilities

Primary classes of use cases

Transformation from one information sharing data format to another

- Example: STIX Cyber Event to NIEM to a CAP Alert

Analytics of information federated from multiple sources

- Examples:
  - Fusion center "connects the dots" between a stolen laptop (from NIEM) and a cyber incident (From STIX)
  - Bio hazard detected by automated instruments and collaborated by local health care professionals

Approach

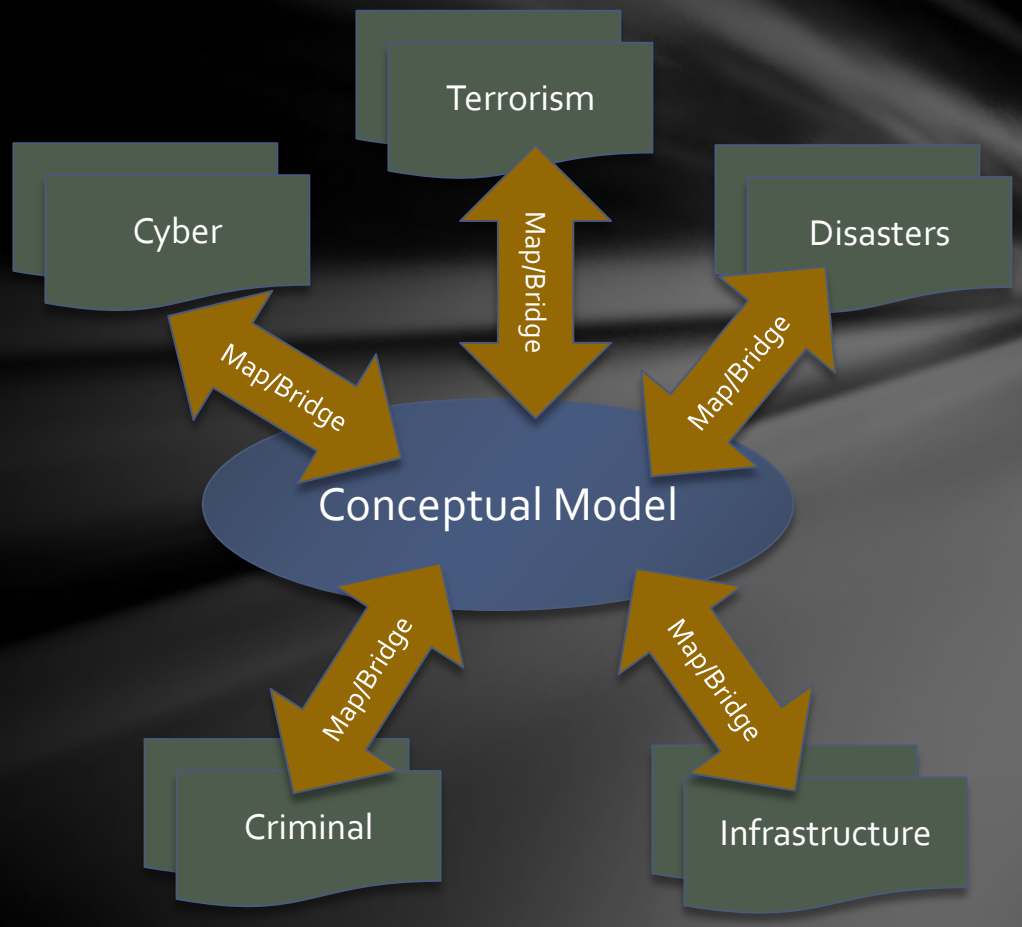
Highlight O(N) vs. O(N^2)

Construct a conceptual model informed by existing schema, research and best practices

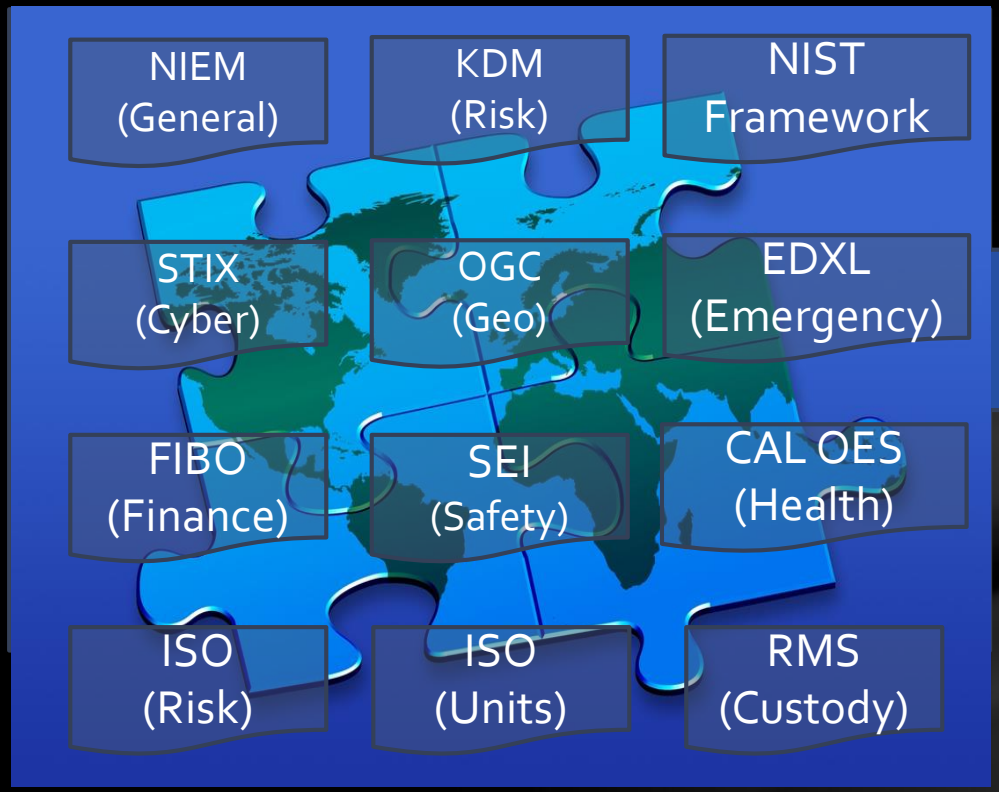
- This conceptual model is independent of specific data structures, technologies and terminologies

Define mapping models between the conceptual model and purpose/technology schema

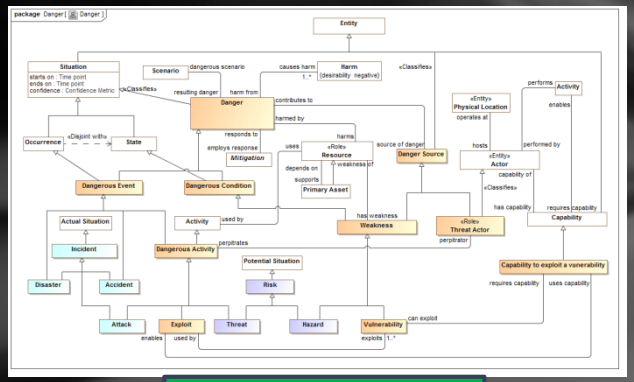
Make both models sufficiently precise that they can drive automated bridging between any mapped schema



Conceptual Model Inputs



Conceptual Model



MAP

STIX, NIEM, EDXL, Others

There is still more to do to fully integrate the above and we anticipate more inputs and use cases

The Process

Building a community and standards to protect against threats and risks

Open Community Process

Our goal is to create and encourage

- Open standards for threat and risk information sharing
- A community of information providers, consumers, analysts and products

- The standards process is organized under the "Object Management Group" (www.omg.org)
- The community "home" is www.threatrisk.org

While not required by OMG process, the submission team publishes draft specifications to invite comment, engagement, community building and implementation. OMG Membership is encouraged but not required.

Stakeholders may contribute to the specification.

We are also exploring options for open source implementations

Who Is OMG?

Object Management Group (OMG):

- Founded in 1989
- More than 470 member companies
- The largest and longest standing not-for-profit, open-membership consortium which develops and maintains computer industry specifications.
- Continuously evolving to remain current while retaining a position of thought leadership.

Developing Standards

Standards are developed using OMG's mature, worldwide, open development process. With over 20 years of standards work, OMG's one-organization, one-vote policy ensures that every vendor and end-user, large and small, has an effective voice in the process.

Finance Healthcare Insurance Government







OMG's Best-Known Successes

Common Object Request Broker Architecture

- CORBA® remains the only language- and platform-neutral interoperability standard

Unified Modeling Language

- UML® remains the world's only standardized modeling language

Business Process Modeling Notation

- BPMN™ provides businesses with the capability of understanding their internal business procedures

Common Warehouse Metamodel

- CWM™, the integration of the last two data warehousing initiatives

Meta-Object Facility

- MOF™, the repository standard

XML Metadata Interchange

- XMI®, the XML-UML standard

Submitters and Contributors (Thus Far)

Model Driven Solutions division of Data Access Technologies

KDM Analytics, Inc.

International Business Machines, Inc.

RSA, The Security Division of EMC

Lockheed Martin, Inc.

Oracle Corporation

Fujitsu

TEAM THREAT

Information Sharing Environment (ise.gov)

Demandware

U.S. Air force

U.S. Defense Security Services

California Public Safety (http://www.Caloes.ca.gov)

U.S. National Information Sharing Model PMO (https://www.niem.gov/)

Duke Energy

NSA/UCDMO

NIST

INCOSE

Integrated Networking Technologies, Inc.

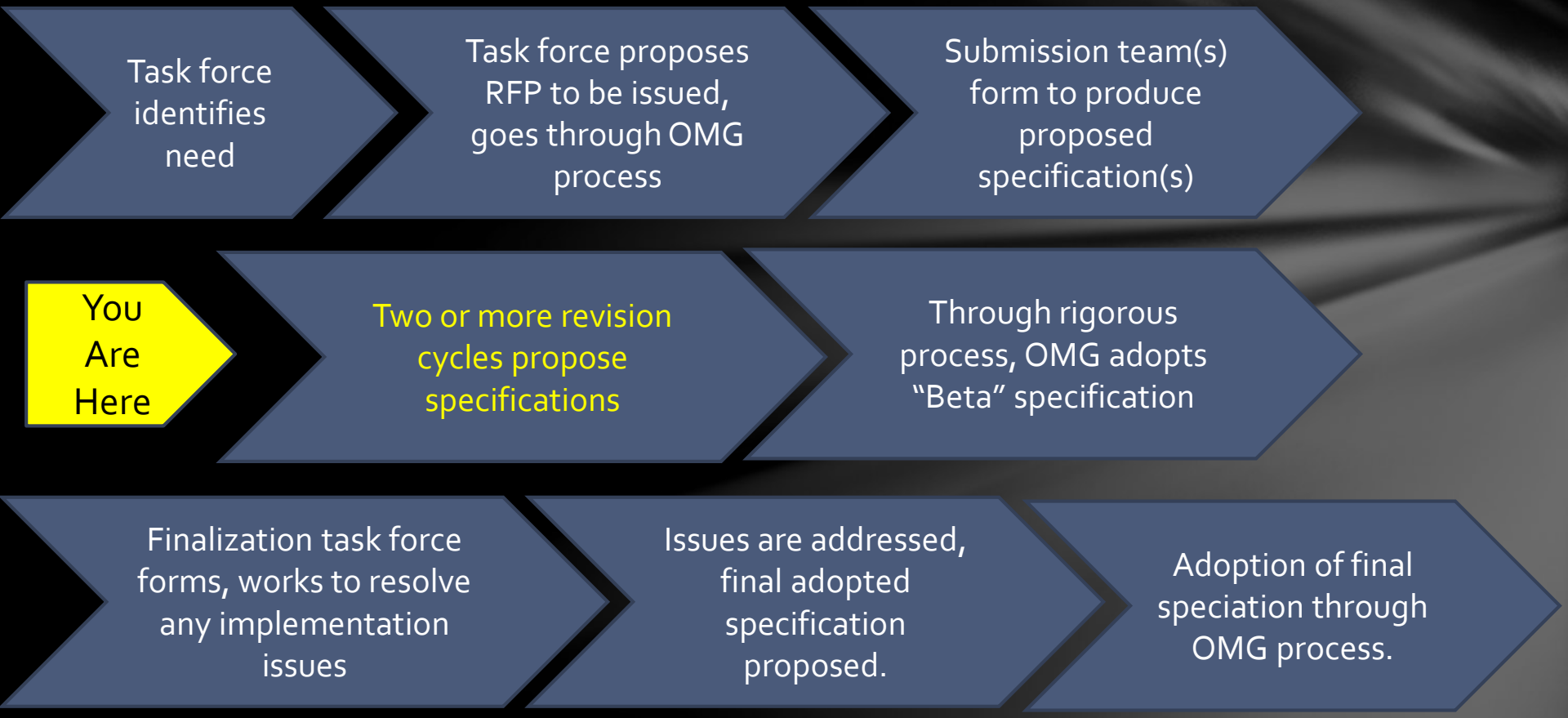
Tibco Software Inc.

Hitachi

NC4

Others pending approval

Summary Of OMG RFP Process



Status

Threat Modeling project kicked off in Dec 2013

Initial submission was made May 2015

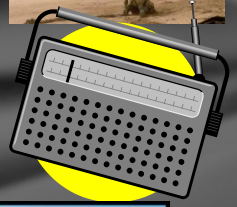
Revised Submission November 2015, to be presented at December OMG meeting

Next (and probably final) revised submission May 23rd

Full adoption by OMG Board of Directors: Mid to late 2016

Implementation efforts need not wait, draft specification can (and should) be implemented to validate the proposed standard.

Stakeholder roles in our community



Risk/Threat Information Sources | **Data Fusion & Brokers** | **Analysts** | **Defenders** | **Responders**

Vendors & Service Providers

One organization may play multiple roles

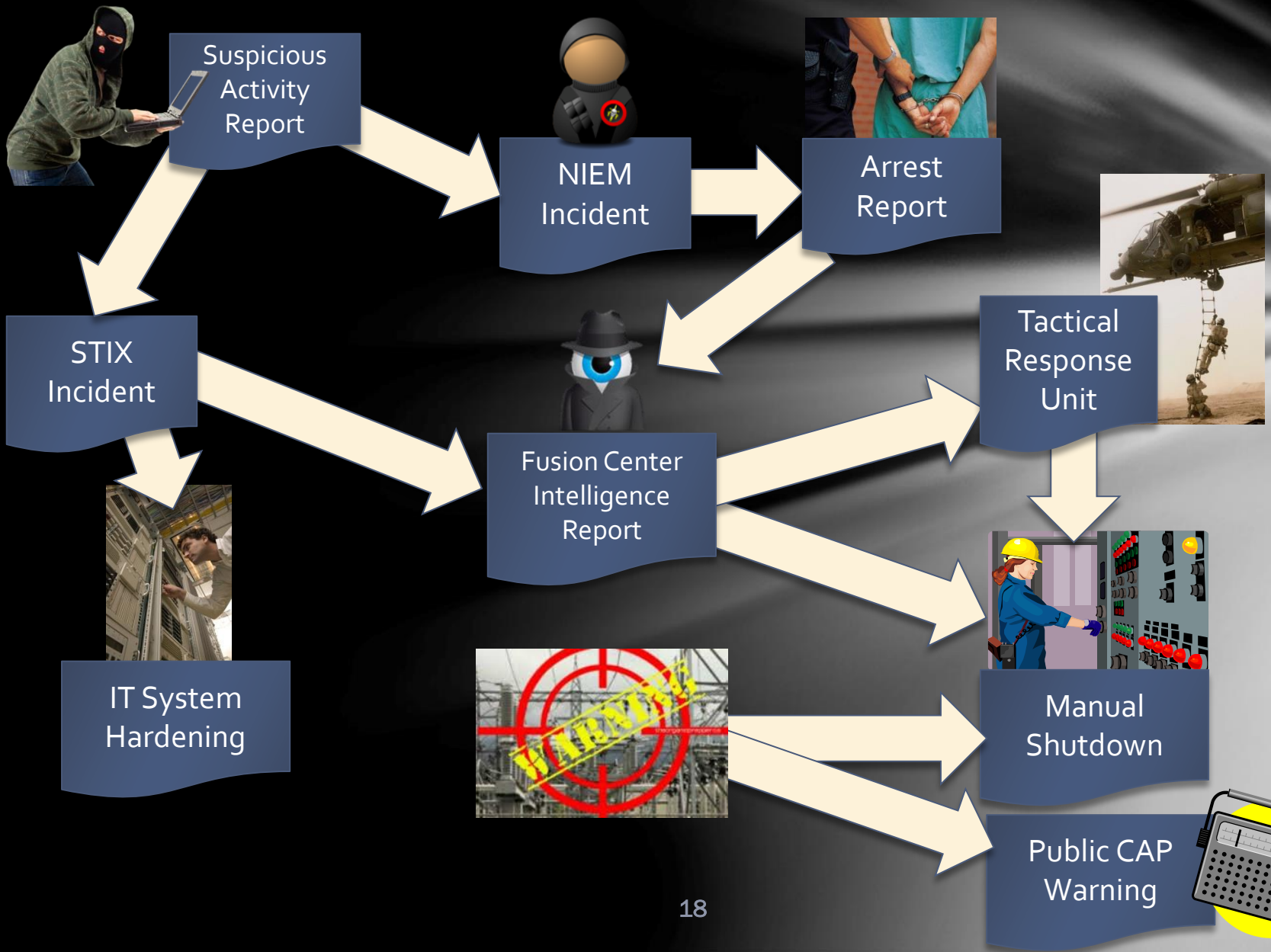
Use Case – Critical Infrastructure

Target: A group of organizations that collaboratively manage critical infrastructure and utilize Industrial Control Systems.

Power, water and other critical infrastructure are threatened by cyber and physical terrorism.

Industrial Control Systems are increasingly computer controlled and connected (directly or indirectly) to the internet and may embed compromised control hardware/software from questionable sources.

Potential Information Flows



In January 2015 Massachusetts faced the Hazard of major winter storms across the region. Potential Harm from blizzards and winter storms includes negative economic impact, limited road accessibility, restricted emergency management, non-availability of utility, property damage, personal injury and death, and more.

The onset of a winter storm or blizzard was predicted by the National Weather Service (NWS).

Example of structuring risk information

In January 2015 Massachusetts faced the Hazard of major winter storms across the region.

Is formalized as

Major winter storms : Hazard

Is defined by

Hazard

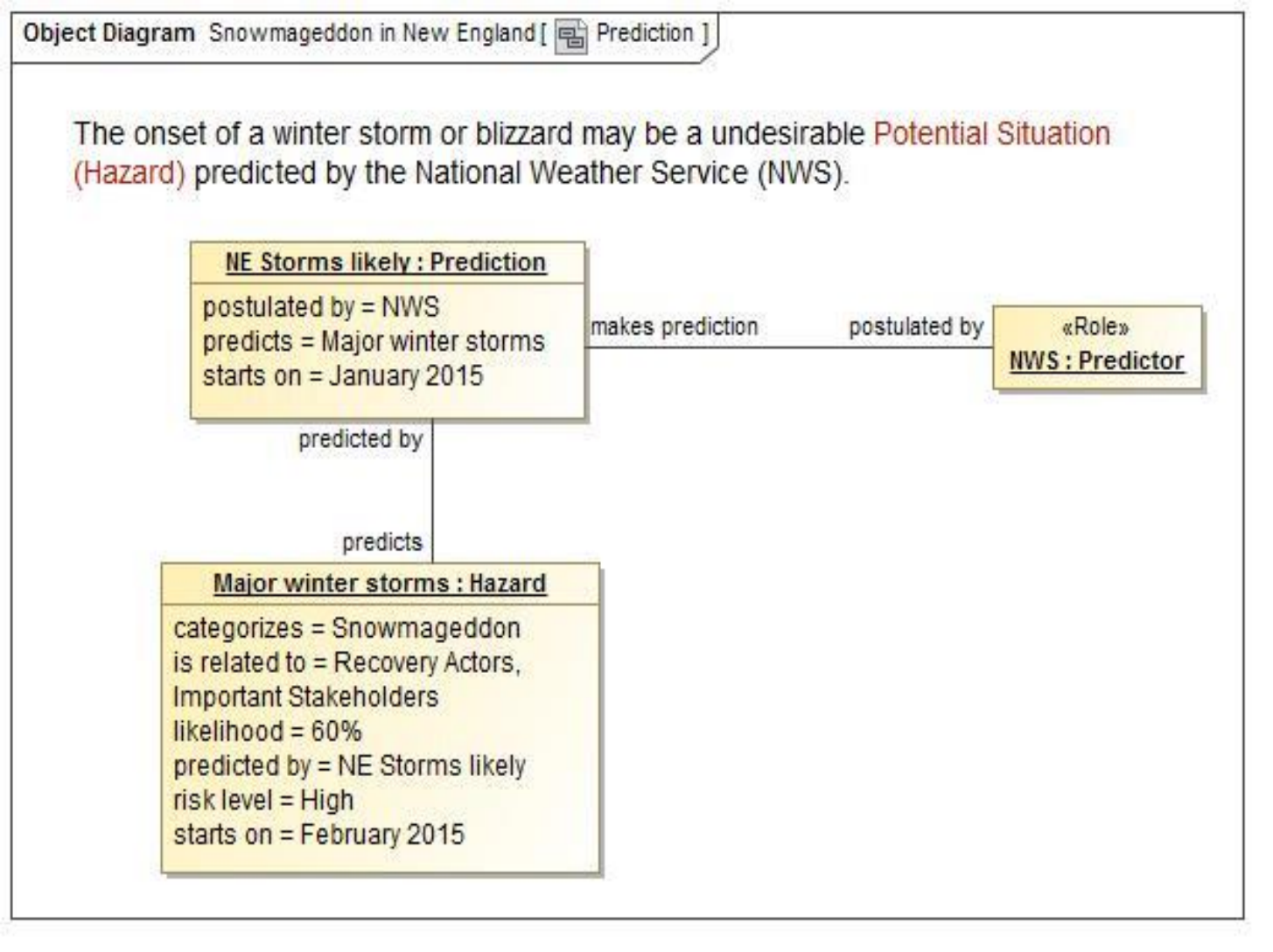
A hazard is a condition that may lead to undesired consequences. Hazards lack intent and do not require the involvement of a threat actor.

Maps To

A data syntax and vocabulary

```
<drn:PotentialDanger>Major winter storms</drn:PotentialDanger>
```

A Potential Storm? Who said this?



Precepts

- The purpose/organizational/technology specific schema will not (should not) go away
- A "one size fits all" solution will not work
  - There will be no one technology
  - There will be no one terminology or language
  - There will be no one data structure for threats and risks
- Our focus is <u>federation</u>
  - Understanding the concepts behind the schema
  - Mapping them to/through a common conceptual model
  - Enabling interoperability by bridging between the specific schema
  - Supporting integration and coordination of mitigation and response capabilities

Core Concept: Comprehending Planned and Unplanned Threats

- "All hazards" include man-made and natural disasters/system failures
  - There is not always an actor involved (e.g. hurricane, system malfunction)
- Intentional threat actors are not the only source of threats
  - Non-malicious actors may constitute significant threat (e.g. spear-phishing victim, power plant operator)
  - Defenders (e.g. system admins, law enforcement, medical staff) are also actors with defensive plans
  - Victims are actors as well

Core Concept: Attacker/Defender Symmetry

- Attack perspective:
  - Defender: Attackers/hazards are threats
  - Attacker: Targets are opportunities
- Defense perspective:
  - Attacker: Successful defense is a threat to the intentions/objectives
  - Defender: Maintaining effective defensive posture is an opportunity
- Threat vs. Opportunity is in the eye of the emoticon – it is not sufficient to create static classifications

Understanding the models

Kinds of models

Conceptual models

- Defines the terms and concepts of the threat & risk domain as a semantic model. Conceptual models can also be transformed to ontologies.

Data models

- Represents specific logical or physical data schema for a specific purpose – more concrete and structured.
- Data models are a direct representation of some kind of schema, e.g. XML Schema, SQL Schema or RDF Schema.

Mappings

- Mappings relate a data model to one or more conceptual models to provide for automated transformation and federation of information in these deferent formats.
- The conceptual models become the "pivot point" between multiple data representations of the same and related concepts.

Pivoting Through a Conceptual Model

Data representations (Schema & Instances)

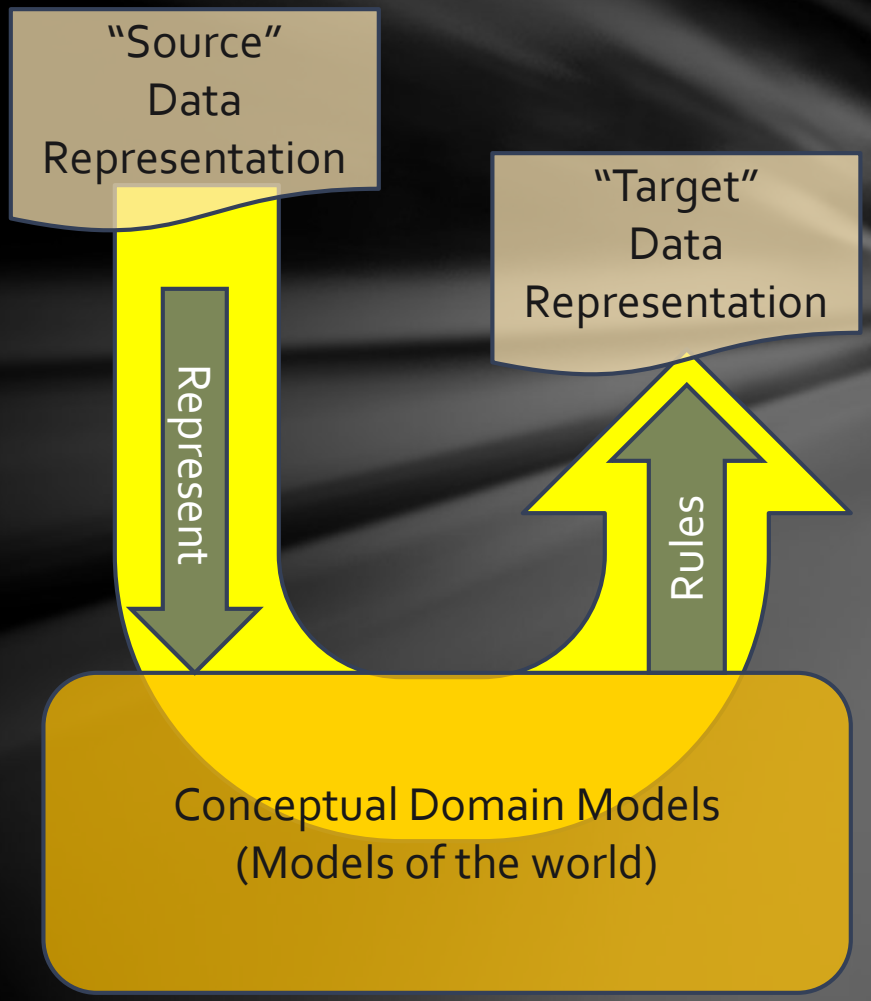
- Model data for a purpose using a technology
- "Instances" are data structures (e.g. SQL tables or XML documents) – "facts" about the things in the world from some perspective

Conceptual Domain Models (CDM)

- A conception of the world by a group of stakeholders – less purpose specific
- "Instances" are things in the world – so can't be in models

Using abstraction, we can have multiple representations of facts about the world in different data structures and technologies

Rules define how domain concepts can be represented in a particular form – rules can be simple and generic or heavyweight and specific, depending on the representation.



Mappings included

STIX – Structured Threat Information Exchange, for Cyber threat information. (Moving to Oasis "CTI")

NIEM – National Information Exchange Model – For justice, public safety and other domains.

Risk Model – A concrete risk model for data interchange is included and mapped as none currently exists as a standard.

NIST 800-53 – Security and Privacy Controls for information systems. This is not a data mapping but shows how the concepts support the controls.

Note: More mappings are anticipated as the initiative unfolds. Some may be published but not standardized.

Representing the data and schema

Options

- UML Diagrams
- Tables
- Schema

UML is about the information and semantics, not the diagrams. The diagrams and tables support communication of the concepts.

30	Consequence	affects	to act on; produce an effect or change in:
31	Consequence	degree of affect	A metric for how much the consequence affects the objective
32	Consequence	desirability	The desirability of the consequence as importance times degree of affect. May be positive or negative.
33	Consequence	impact	Impact = desirability * likelihood

Conceptual Model Layering

Operational threat situational awareness and response

Operational risk evaluation and mediation

Cross-risk/threat – specific "wide and shallow" risk and threat concepts/ E.G. Risk, threat, danger, consequence

Generic Library – Provides concepts and links across multiple viewpoints, not just threat/risk. E.G. Person, Objective

Kernel– Foundational concepts for modeling anything: Entities, Roles, Relations, Types, Information, Rules, Identity, Etc…

Subset of the model from SIMF

Conceptual Model Packages

Core Concepts

Foundation

Identifiers

Information

Patterns

Process

Quantities and Units

Rules

Situations

Timeframe

Generic Concepts

Ability

Actors

Assessment

Control

Credentials

Enterprise

Entity Kinds

Intent

Location

Observation

Organization

Person

Prediction

Resources

Systems

Threat and Risk Specific Concepts

Campaign

Course of Action

Cyber

Danger Categories

Incident

Indicator

Kill Chain

Mitigation

Risk Treatment

Threat

Undesirable Situations

Vulnerability

Next Steps

Further engagement of stakeholders

Validation against user requirements, use cases and data

Reference and pilot implementations