Achieving All-Hazards Threat & Risk Information Sharing and Federation

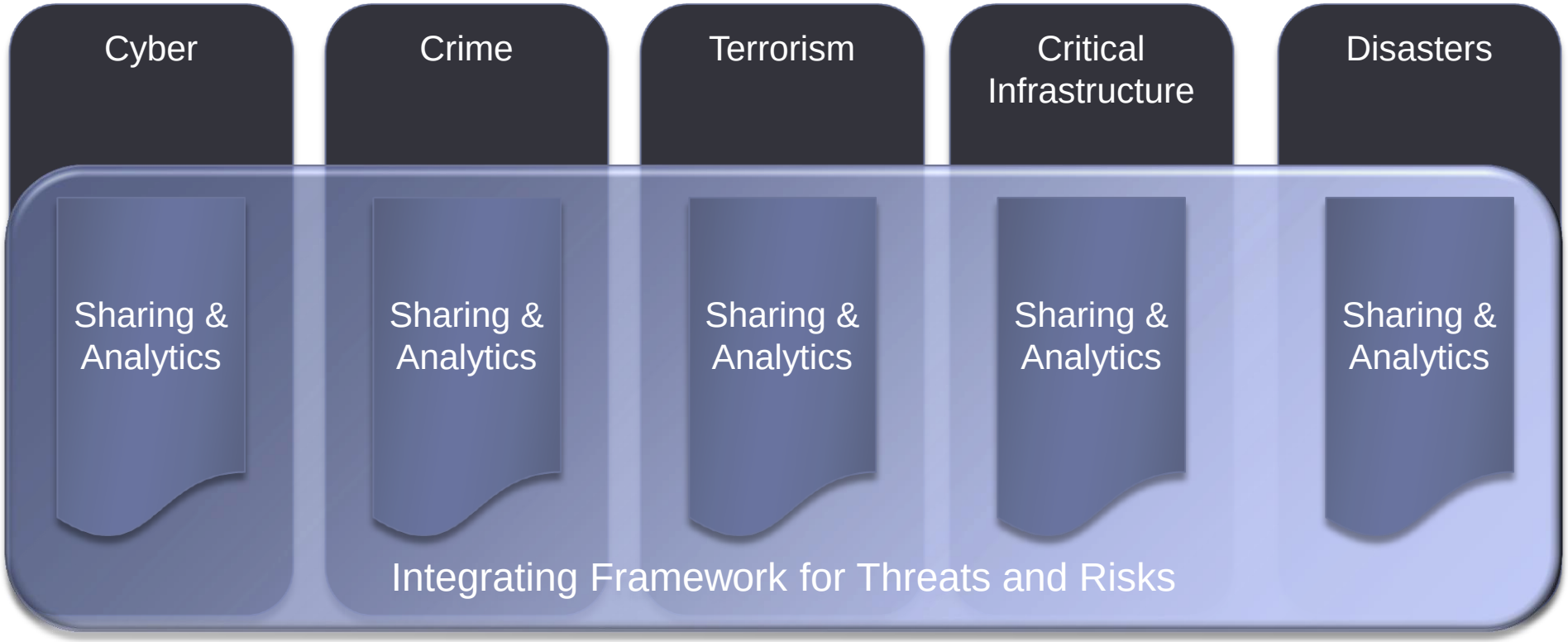
The conceptual model approach

What we have heard

- Call to action from the highest levels of government
- Threats to critical infrastructure
- Insider threats
- Blended attacks – the 70%
- Counterintelligence & defense
- Information as a national asset
- All threats, all hazards
- Understand your critical assets,. Costs of complexity, Change of processes
- Threats to retail across cyber and physical
- The challenge of securing complex systems
- The challenges of situational awareness across domains
- All source threats to industry and government
- Importance of secure and trusted supply chains
- Regular reports of cyber and physical attacks
- Patterns in massive data at extreme speeds
- Security is a team sport

- So what can we do about it?

Goal: An integrating framework

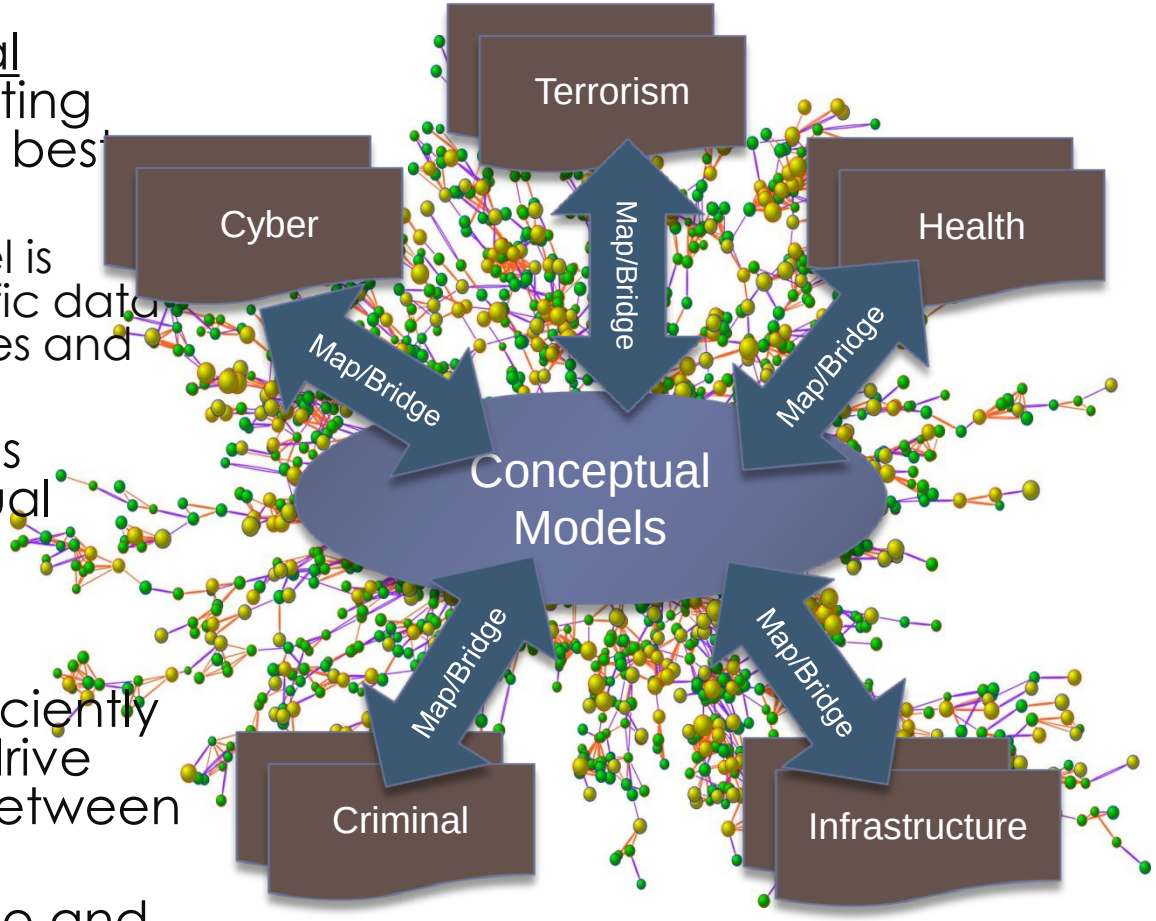


An integrating framework that helps us deal with all aspects of a risk or incident

A federation of risk and threat information sharing and analytics capabilities

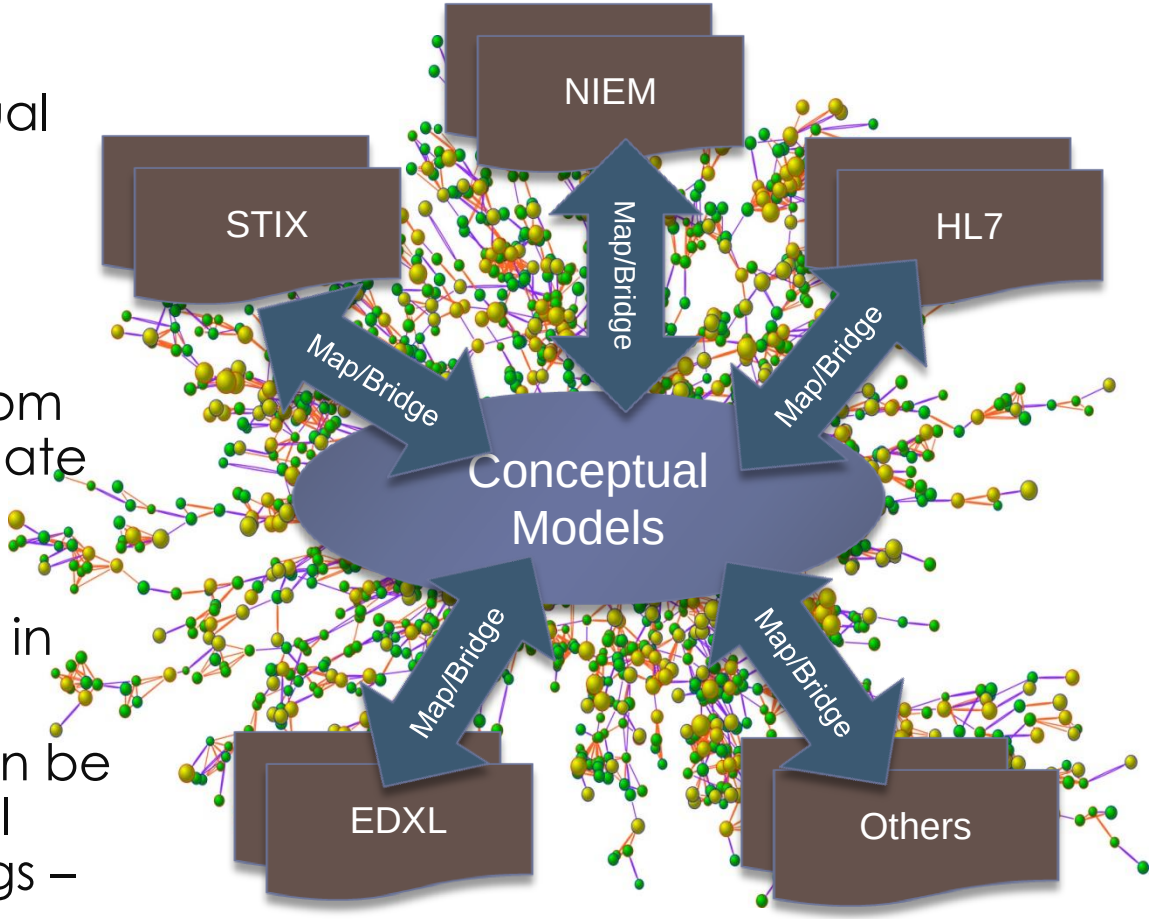
Approach to integrating domains

- Construct a conceptual model informed by existing domains, 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/organizational schema
- Make both models sufficiently precise that they can drive automated bridging between any mapped schema
- Use cases focuses scope and detail



At the technical level

- Define mapping rules between the conceptual models and various technology/domain specific models
- Automation can then federate information from multiple source or translate between them
- Of course translation is limited to the concepts in common!
- Conceptual models can be extended for additional concepts and mappings – it is an open system

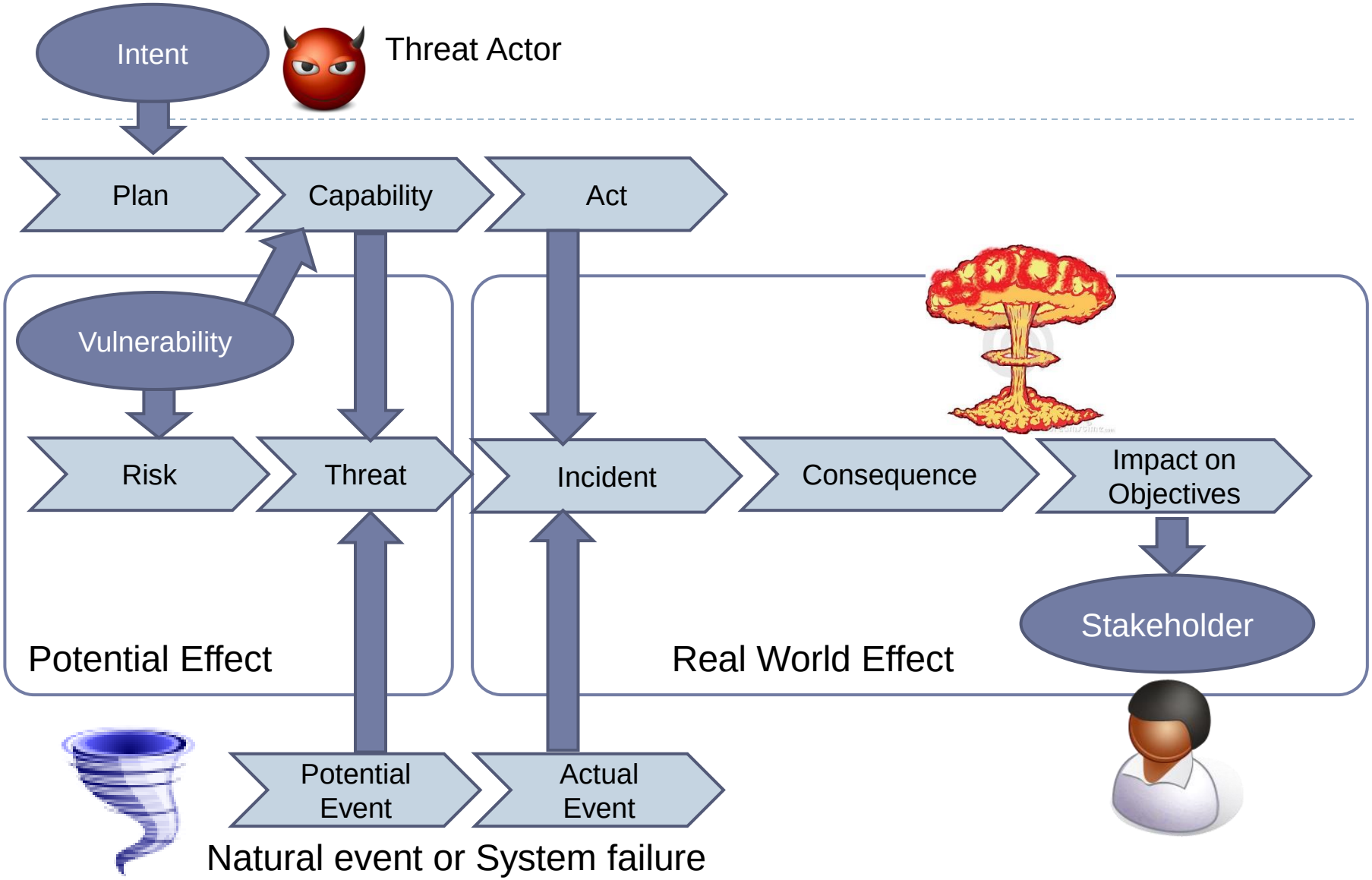


Concepts at the core

- The core to any communications or analysis is shared concepts
- Given a foundation in concepts there is a need for shared vocabulary and syntax – but there is a lot of variation in vocabulary and syntax
- The concepts are captured in a model, and then related to different vocabularies and syntaxes
- Concepts are about real world things, not data or technology
- Of course data then represents the concepts which can be manipulated by technology

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



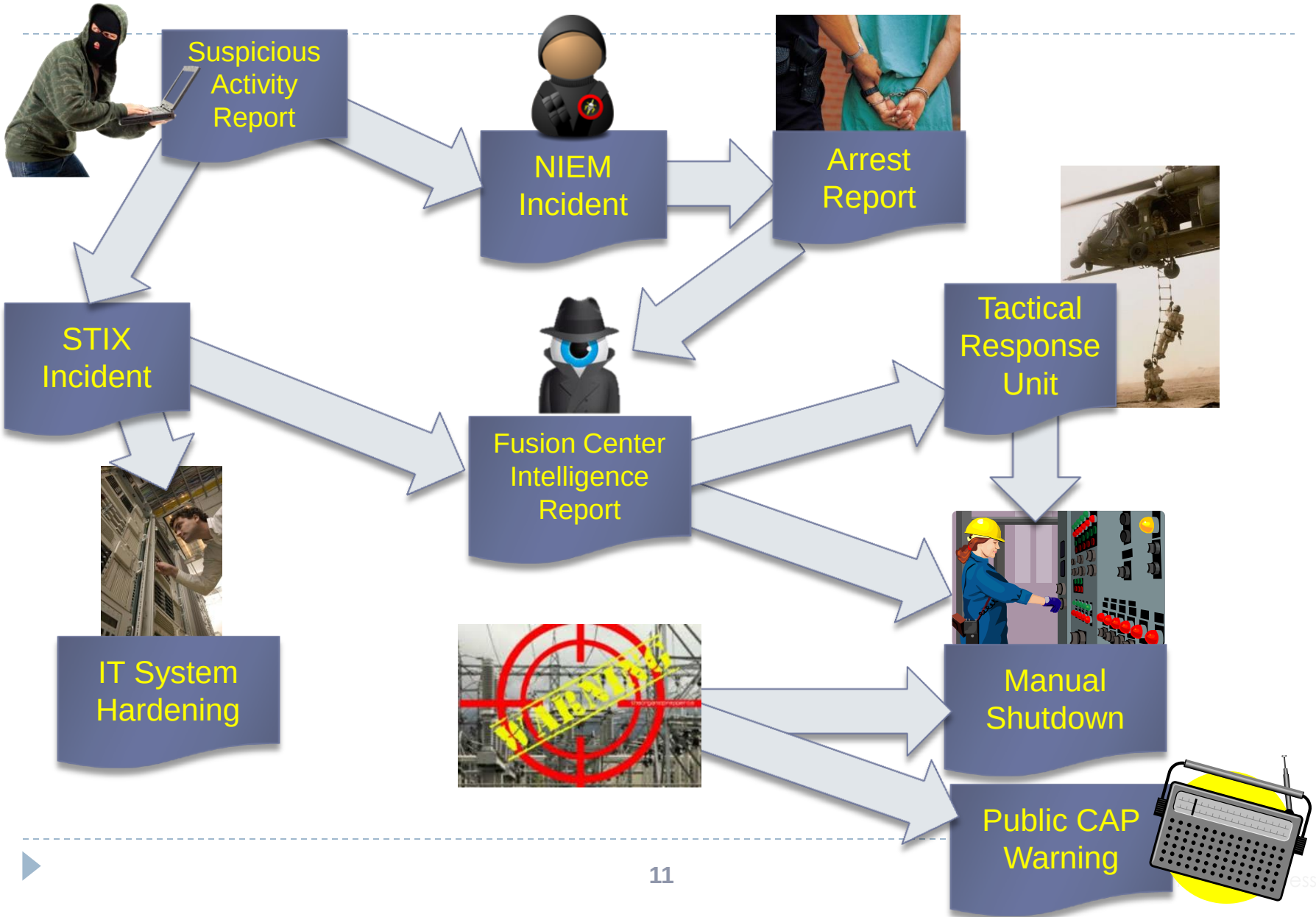
Core Concept: Attacker/Defender Symmetry

- 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

Example Scenario: Coordinated Power Grid Attack

- Attack
  - Laptop with access credentials is stolen
  - Grid industrial control system is compromised in Cyber attack
  - Physical attack on substation disrupts power
  - Compromised system cascades failure
  - Physical infrastructure damaged
- Potential Mitigations
  - Law enforcement recovers laptop
  - Compromise is recognized by Cyber defense, system is hardened
  - Law enforcement notified and arrests attackers
  - Preparation is identified and defense forces put in place
  - Real-time notification of systems going down initiates manual shutdown

Cross-domain Information Flows

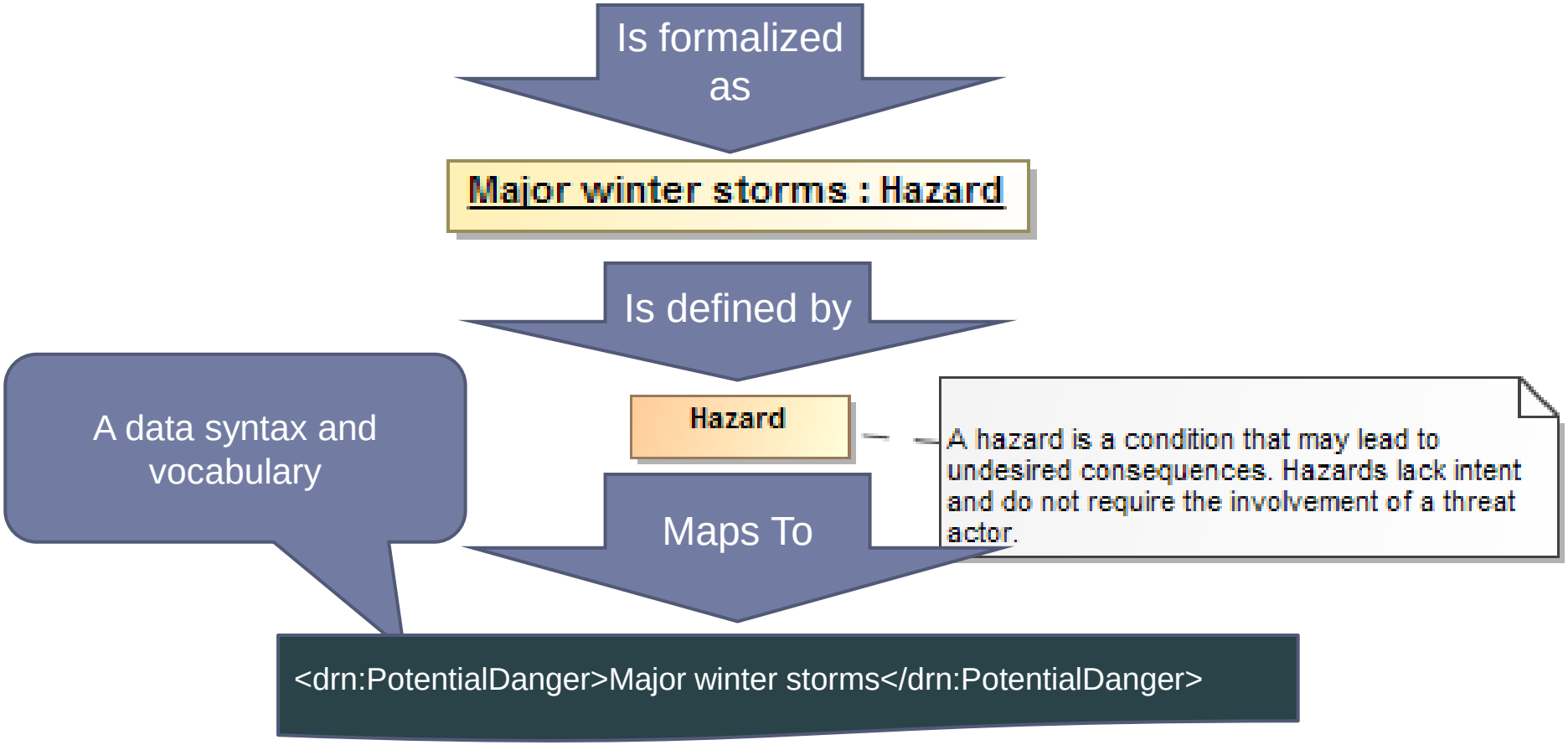


In January 2015 Massachusetts faced the Hazard of major winter storms across the region. Potential Harm from blizzards and winter storms includes negative economic impact, limited road accessibility, restricted emergency management, non-availability of utility, property damage, personal injury and death,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

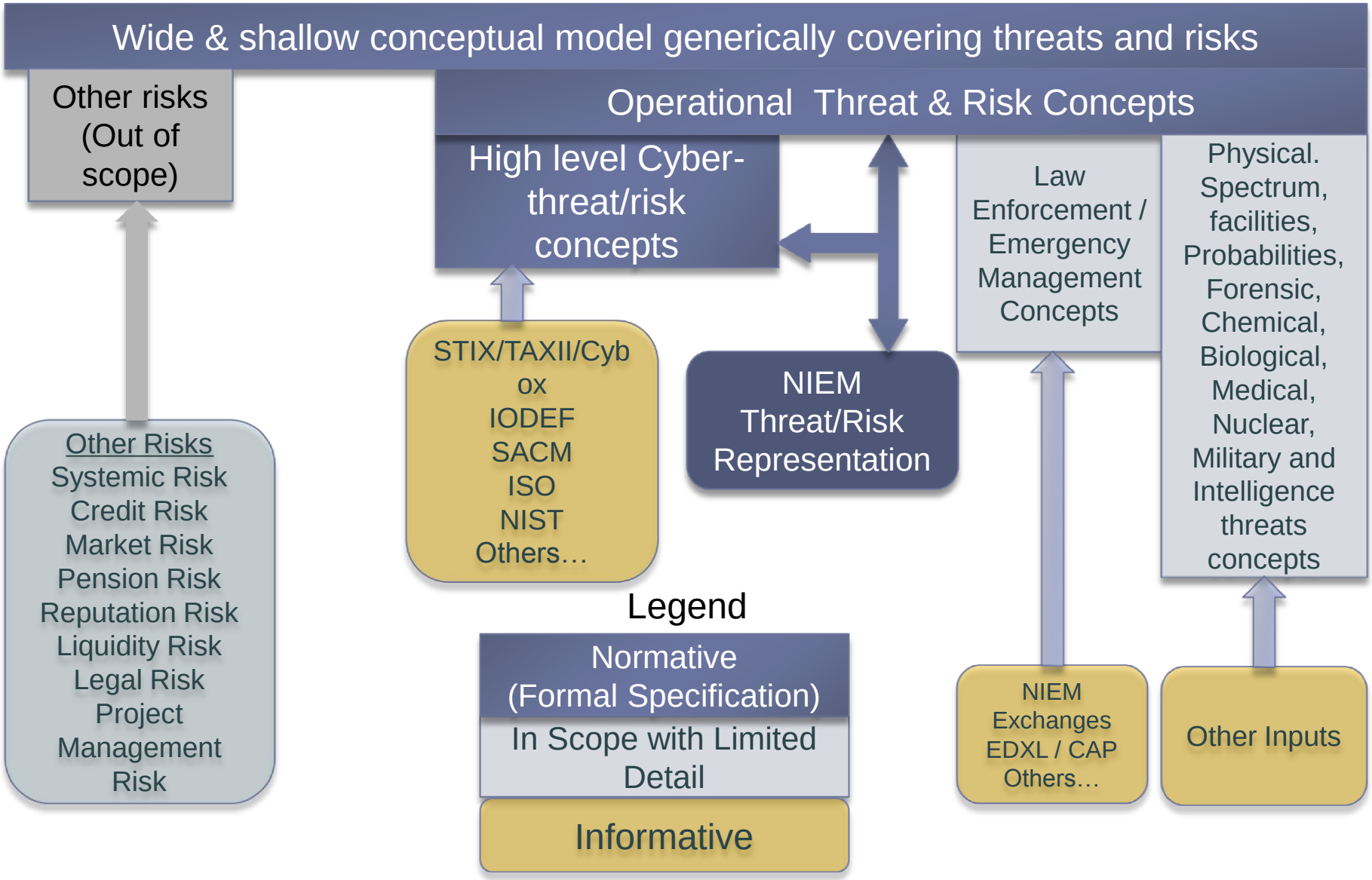
The onset of a winter storm or blizzard was predicted by the National Weather Service (NWS).

Example of structuring risk information

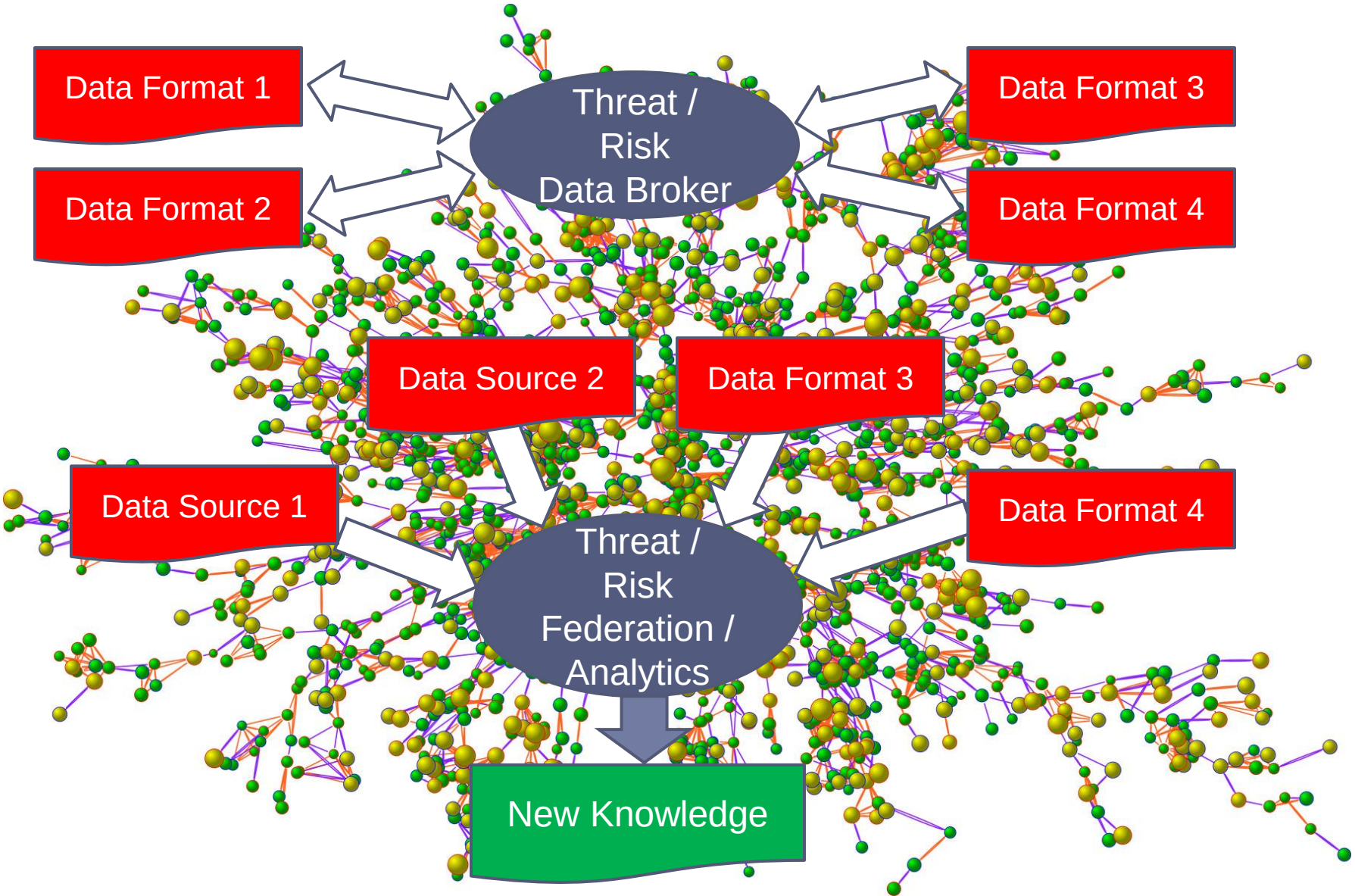
In January 2015 Massachusetts faced the Hazard of major winter storms across the region.



Scope



Primary Use Cases



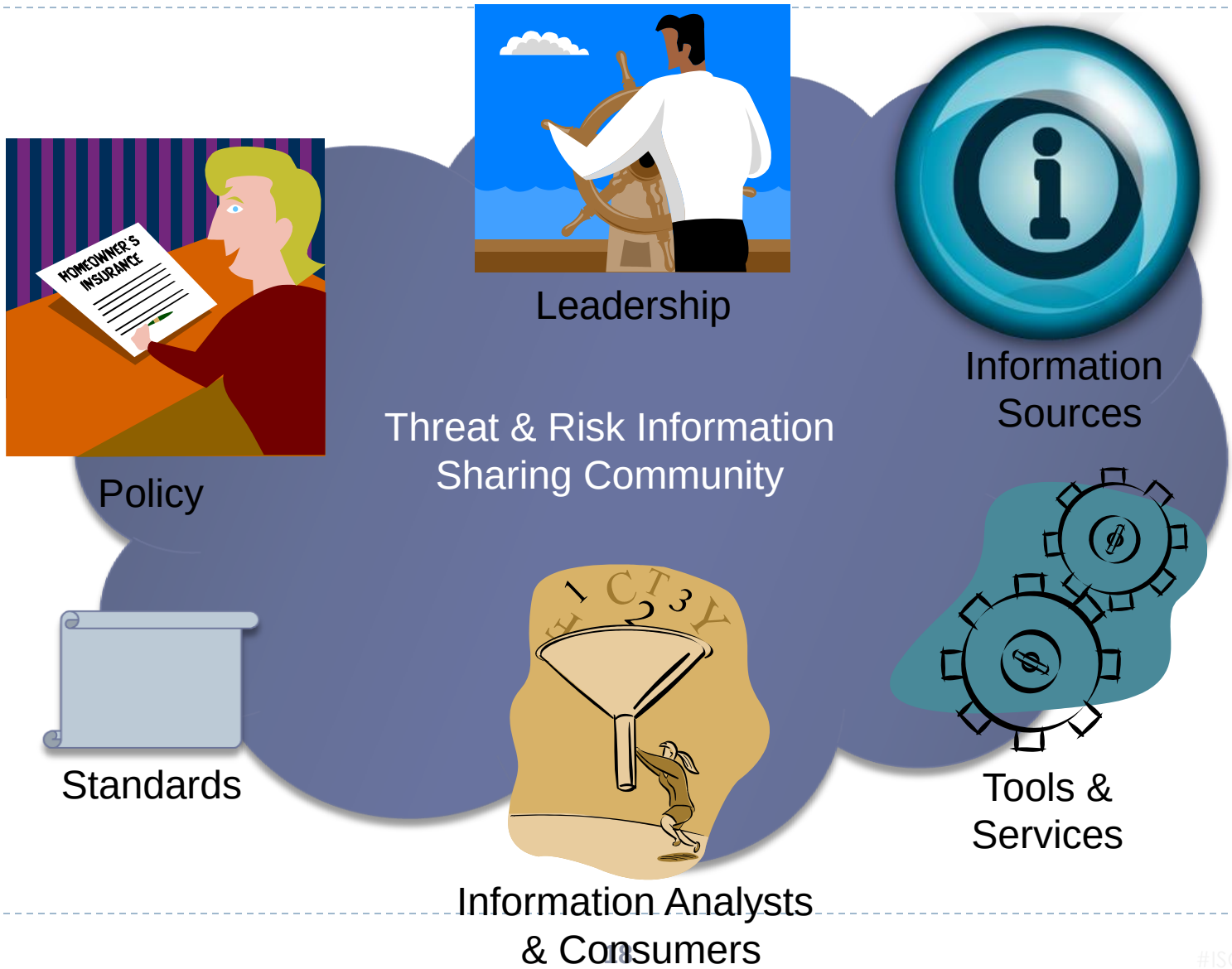
Why this is important

- To make sense of data from many sources
- To deliver information to secure supply chains
- To allow diverse organizations to collaborate and share information
- To protect critical assets and sensitive or private data
- To provide threat and risk analytics across domains
  - Cyber and physical
  - Safety and security
  - Health, Intelligence, biological, retail, military, finance
  - Private and public sector– internationally

Example use cases

- Protection of critical infrastructure through information sharing and analytics. Specific use cases for the electric grid (Duke Energy)
- Large company understanding and acting on its threat/risk landscape
- Fusion center “connecting the dots” by federating multiple data sources
- California Governor’s Office of Emergency Services fusing BioWatch and other data for better decision making
- Integration of STIX (Cyber) data with physical threats and risks for all-hazards
- Retail Sector Point of Sales Attack
- Securing the supply chain for Air Force avionics
- Physical attack on Transformer Yields Cyber and Kinetic Effects
- Threat to electronic healthcare records
- DoD Information Sharing Portal
- Federating information for evaluating the trust of individuals and organizations
- Victim information compromise
- Theft of laptop exposes credentials resulting in loss of confidential information
- State Cybercrime Investigation
- Aligning risk models along the dependencies between systems

It takes a community



Threat and Risk Community

Home | Use Cases | Standards Process | Articles | Upcoming Events | Resources | About the Community | Contact Us

Executive Order -- Promoting Private Sector Cybersecurity Information Sharing

On February 13th 2015 U.S. President Barack Obama issued an executive order "Promoting Private Sector Cybersecurity Information Sharing".

1 2 3

Thinking About Joining?

Great! Once you submit a request to create an account, we will get in contact with you shortly. Please let us know who you are and why you wish to join the site. We can't wait to speak with you.

User login

Welcome to the Threat and Risk Community

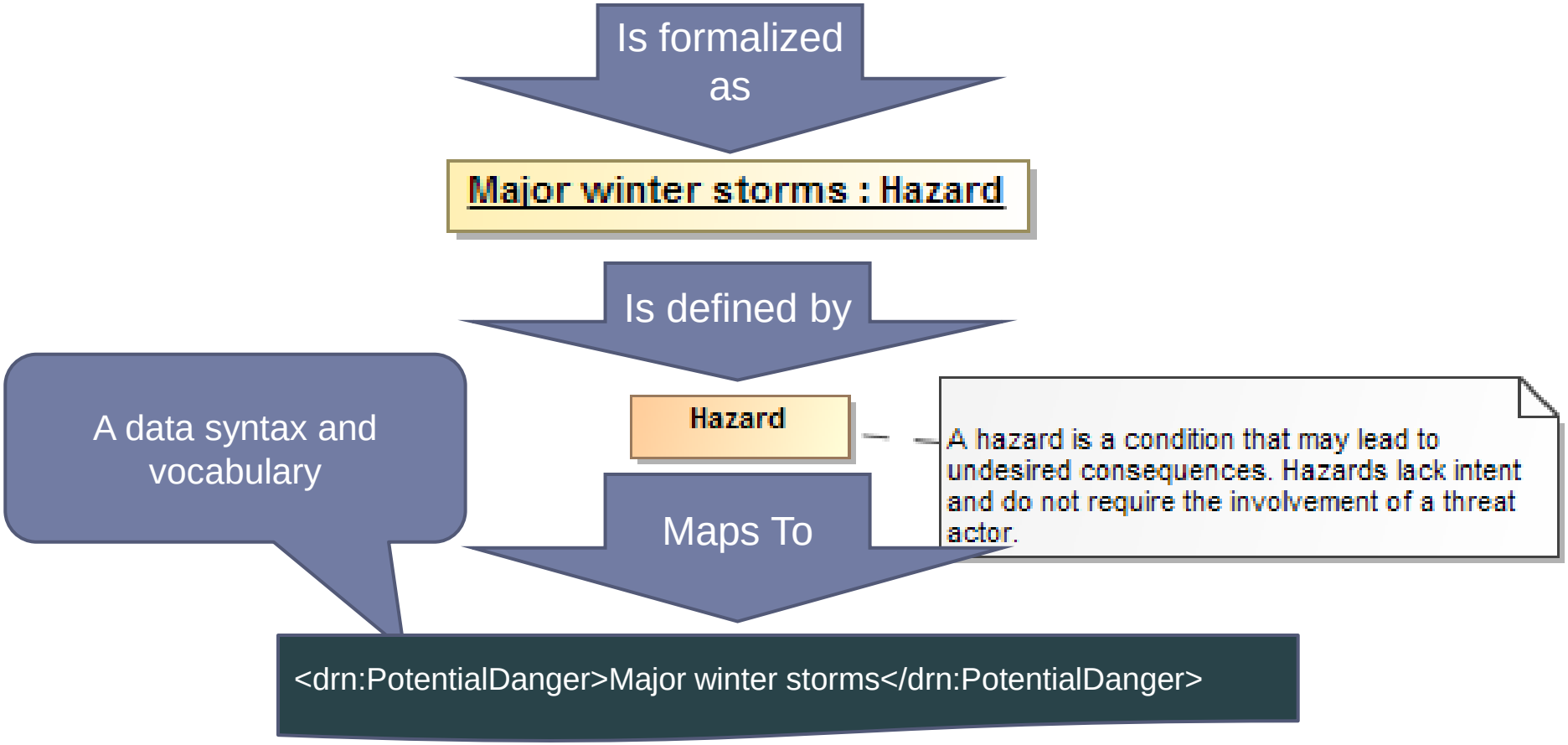
Introduction

Threats and risks are increasingly multi-dimensional in nature – spanning both physical and cyber space. Only by analyzing, federating, and sharing information across multiple domains (i.e. critical infrastructure, cyber, health and human services, public safety), can we effectively counter multi-dimensional threats. This community initiative is focused on driving the federation and secure sharing of threat, risk and provenance information across multiple domains, technologies and data formats. Domains of interest include but are not limited to cybersecurity, law enforcement and public safety, counter terrorism, critical infrastructure, health and emergency management.

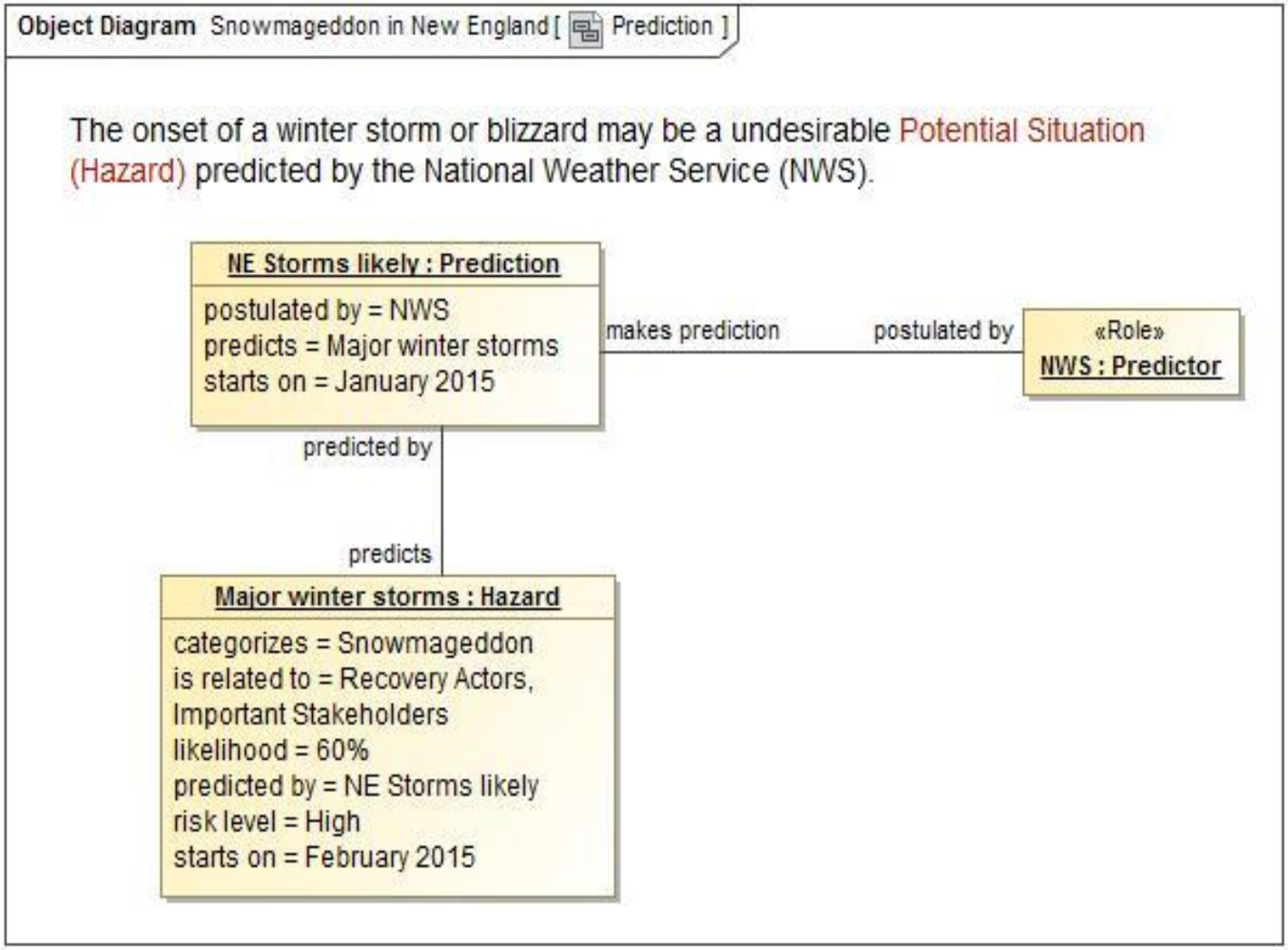
Community Building

Example of structuring risk information

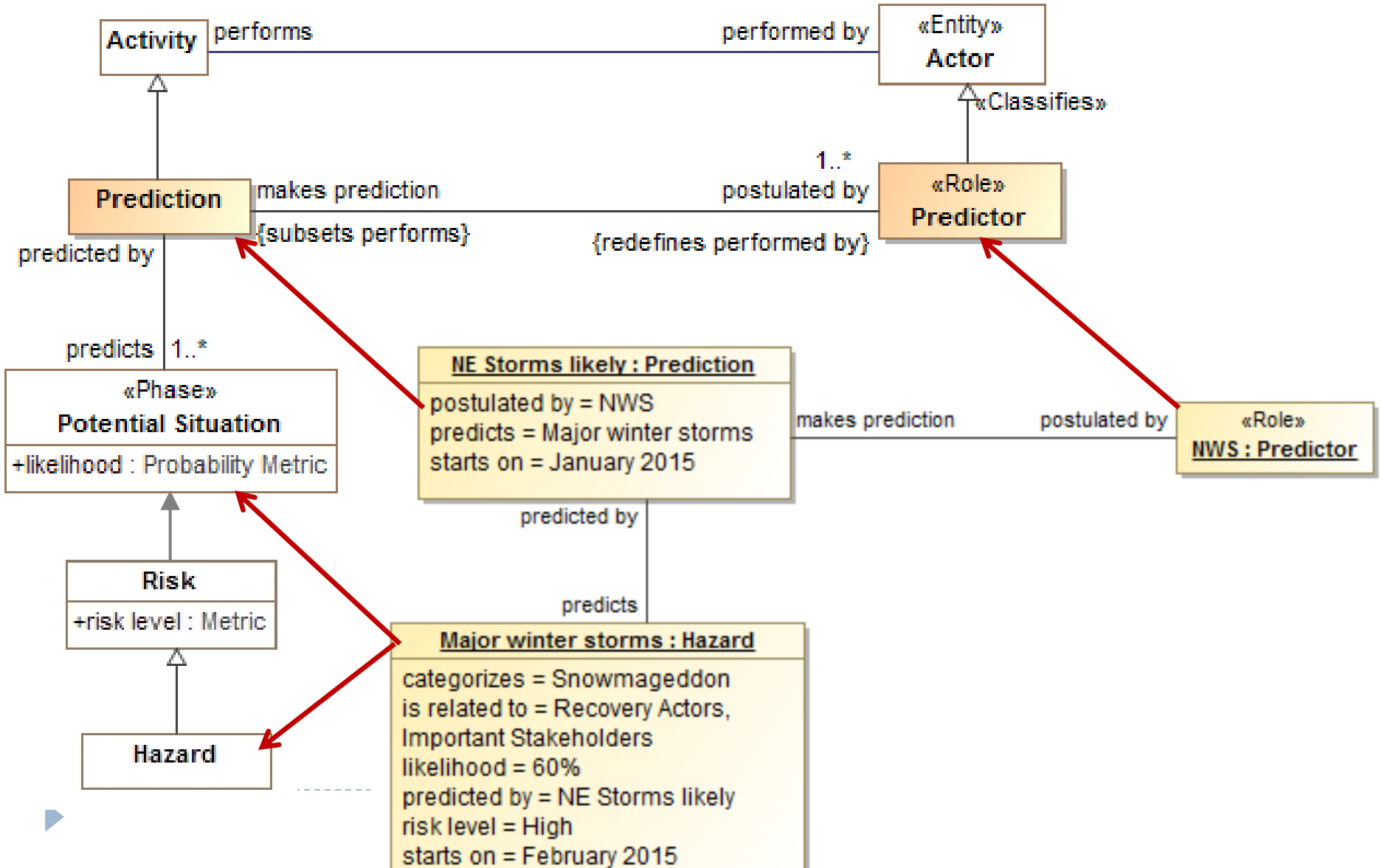
In January 2015 Massachusetts faced the Hazard of major winter storms across the region.



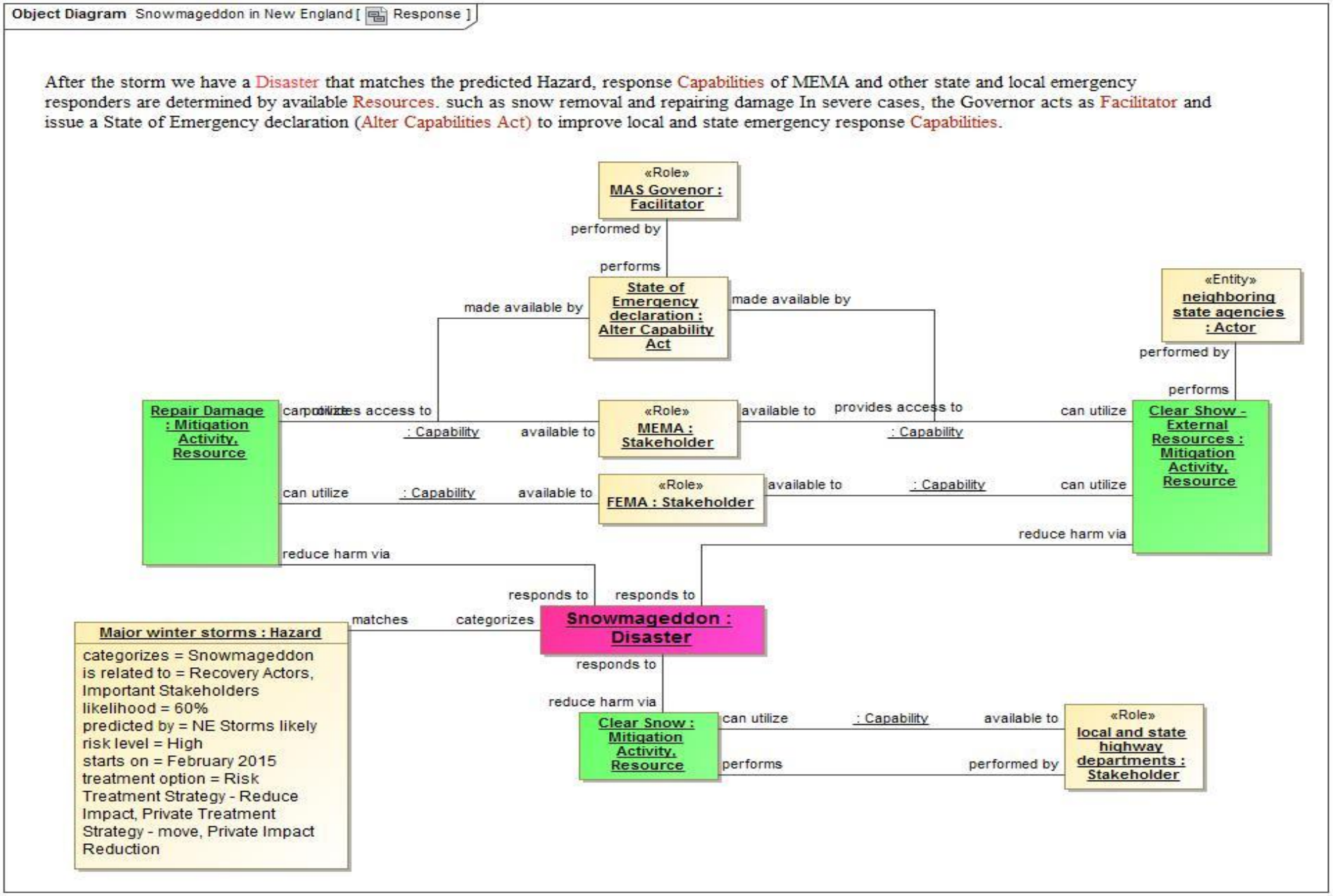
A Potential Storm? Who said this?



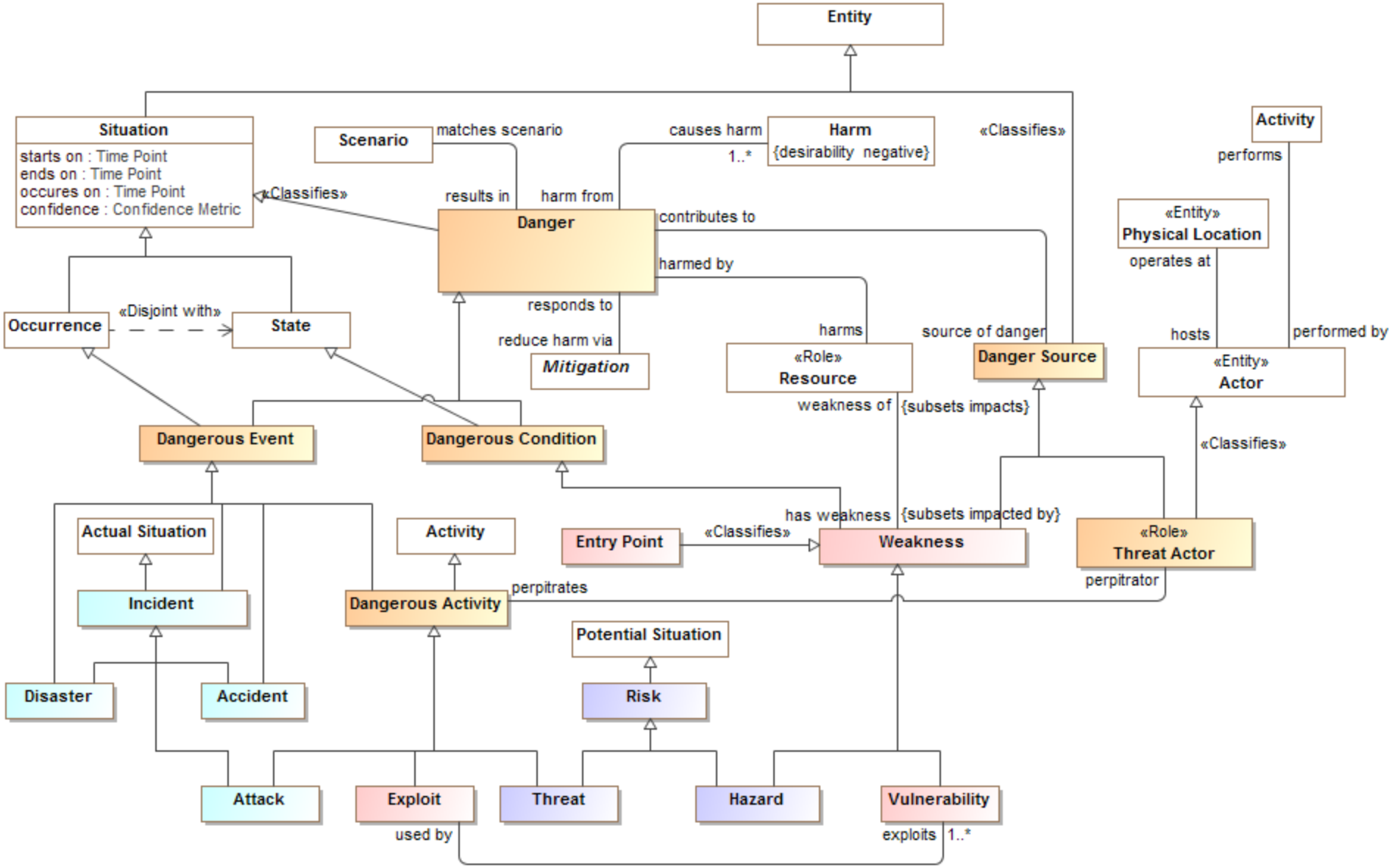
Real-world events relate to the concepts



Response Concepts

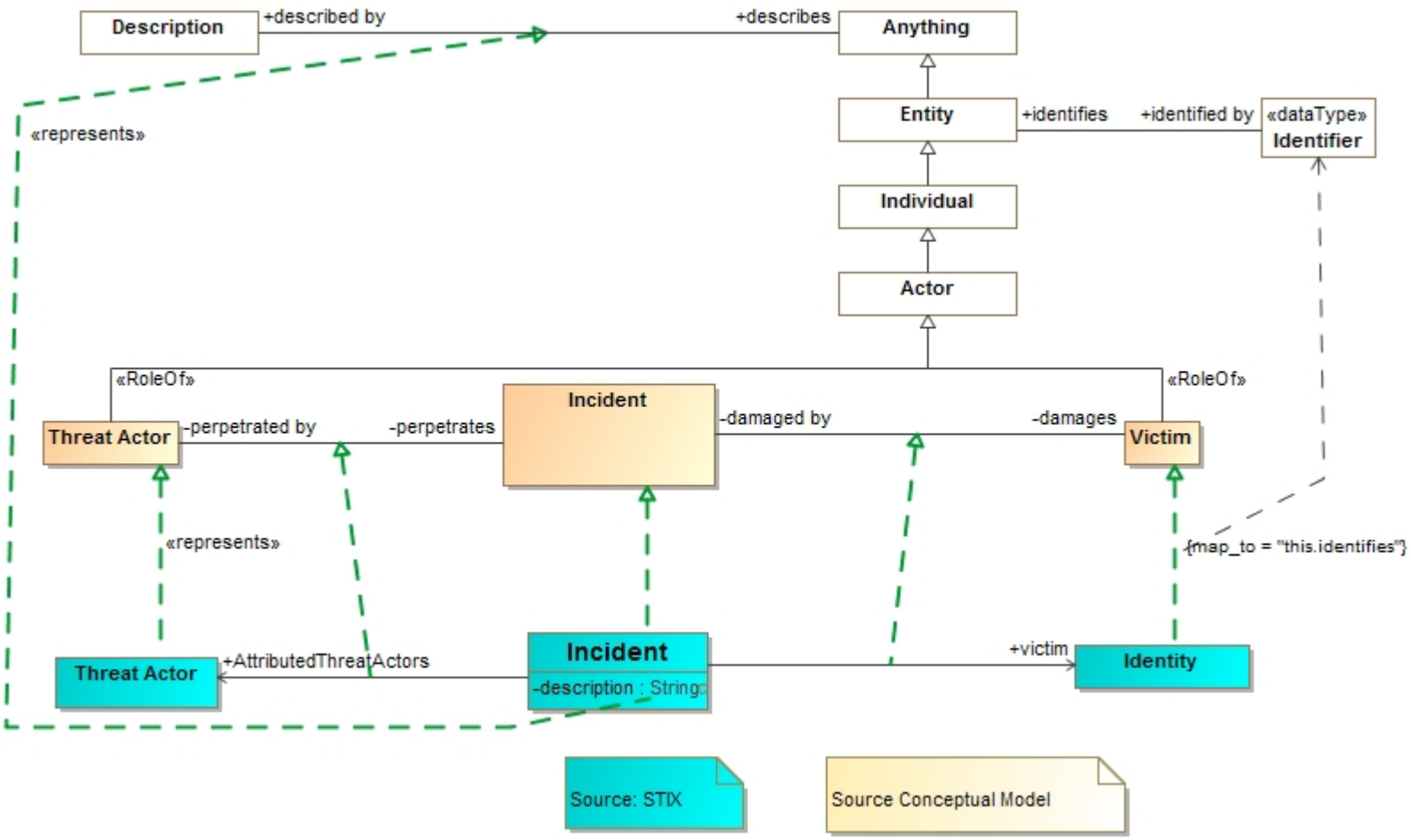


How concepts relate



Mapping

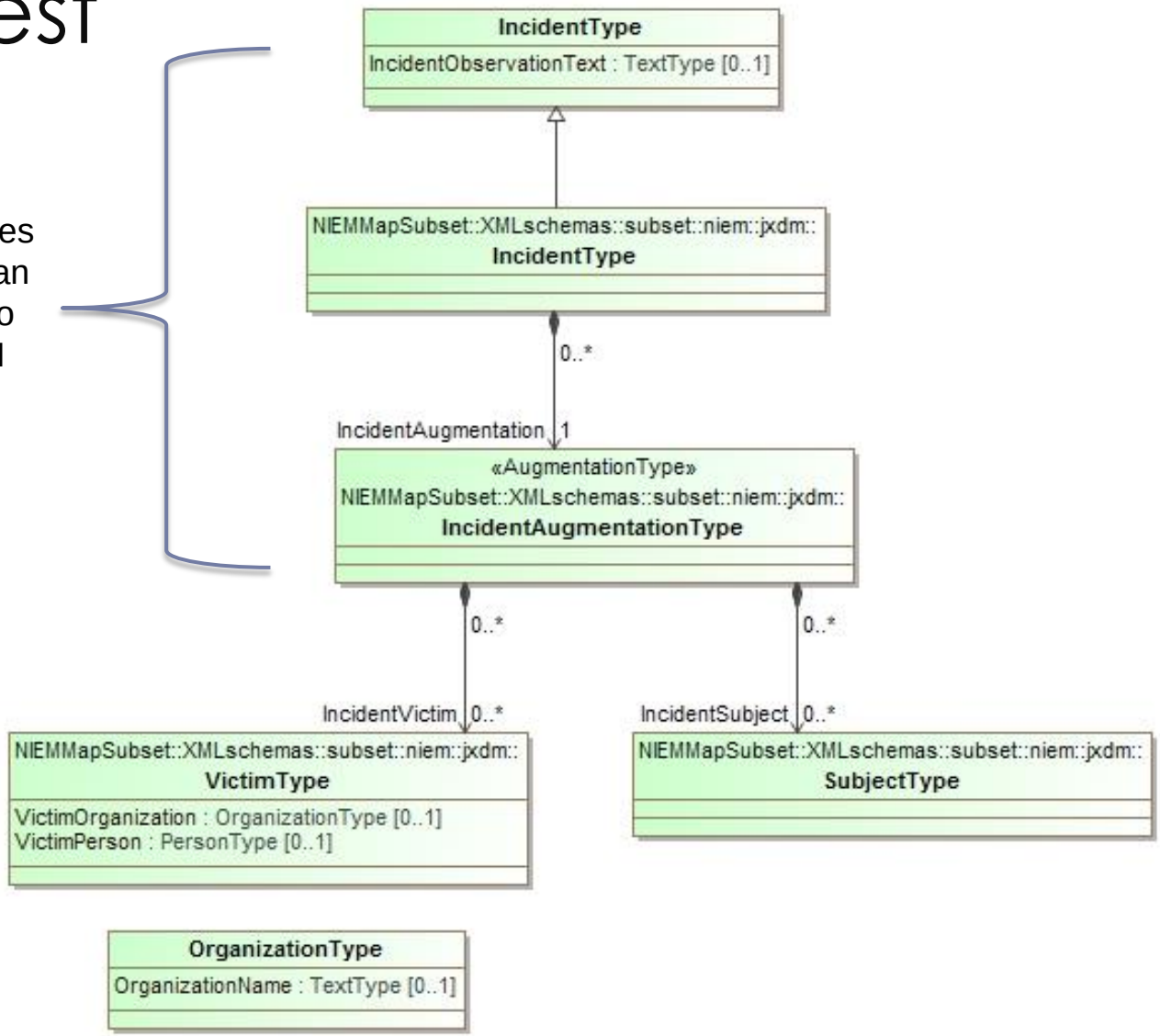
STIX Mapping fragment



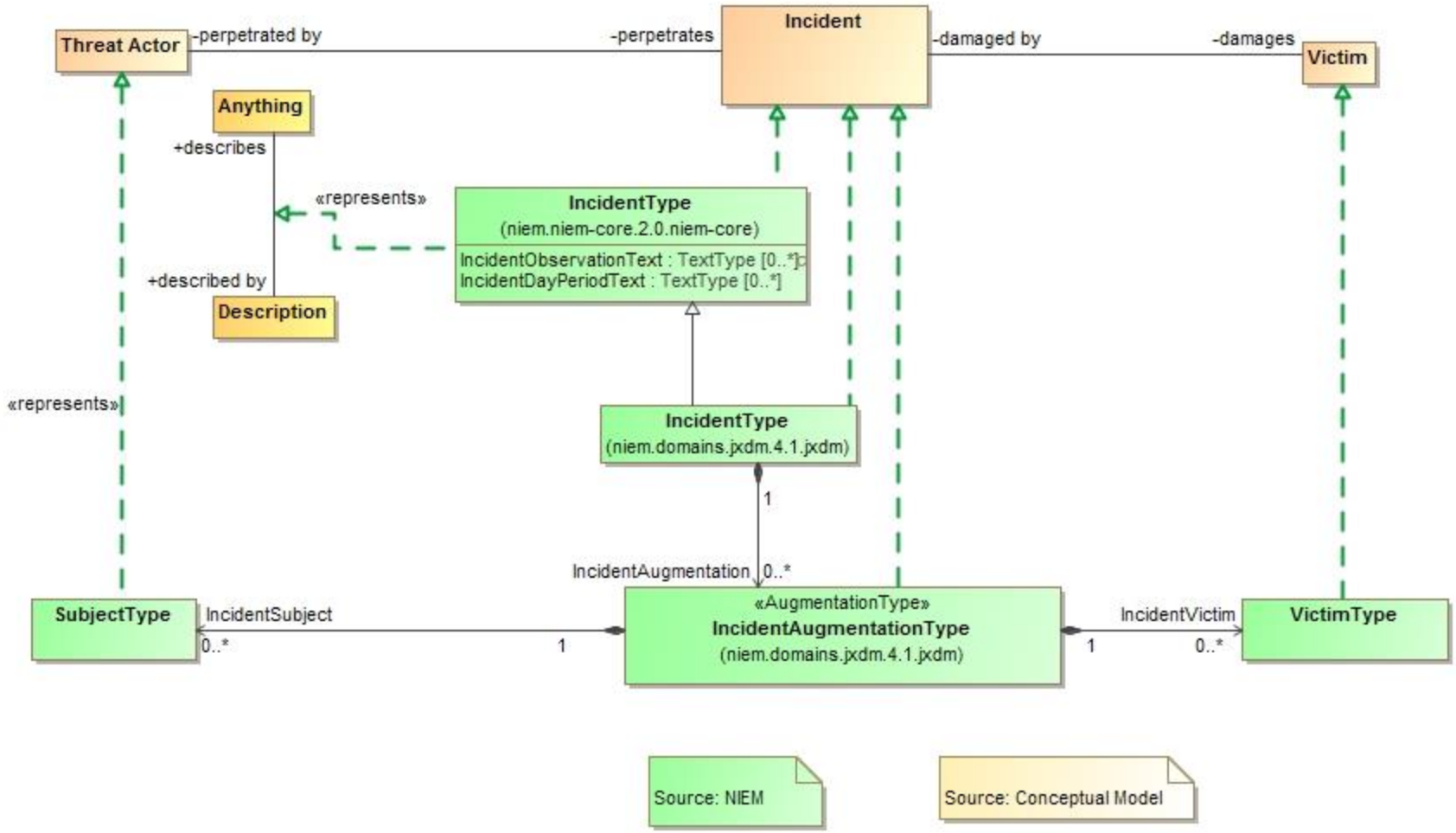
Note: Complete mapping rules are more complex

Corresponding NIEM Subset of interest

Multiple classes representing an incident due to the way NIEM segments domains



NIEM Mapping Fragment



Example STIX data


```
<stix:Incident id="example:incident-fd56fb34-af59-47b3-95cf-7baaaa53fe93" timestamp="2014-08-28T16:42:52.859547+00:00"
xsi:type='incident:IncidentType' version="1.1.1">
        <incident:Title>Breach of Canary Corp</incident:Title>
        <incident:Time>
                <incident:Incident_Discovery precision="second">2013-01-
13T00:00:00</incident:Incident_Discovery>
        </incident:Time>
        <incident:Description>Intrusion into enterprise network</incident:Description>
        <incident:Reporter>
                <stixCommon:Description>The person who reported it</stixCommon:Description>
                <stixCommon:Identity id="example:Identity-5db269cf-e603-4df9-ae8c-51ff295abfaa">
                        <stixCommon:Name>Sample Investigations, LLC</stixCommon:Name>
                </stixCommon:Identity>
        <stixCommon:Time>
                <cyboxCommon:Produced_Time>2014-03-11T00:00:00</cyboxCommon:Produced_Time>
        </stixCommon:Time>
        </incident:Reporter>
        <incident:Victim id="example:Identity-c85082f3-bc04-43c8-a000-e0c1d0f2c045">
        <stixCommon:Name>Canary Corp</stixCommon:Name>
    </incident:Victim>
        <incident:Impact_Assessment>
        <incident:Effects>
                <incident:Effect xsi:type="stixVocabs:IncidentEffectVocab-1.0">Financial Loss</incident:Effect>
        </incident:Effects>
    </incident:Impact_Assessment>
        <incident:Confidence timestamp="2014-08-28T16:42:52.859570+00:00">
        <stixCommon:Value xsi:type="stixVocabs:HighMediumLowVocab-1.0">High</stixCommon:Value>
    </incident:Confidence>
</stix:Incident>
```

Notional Model Mapping Instances

STIX Data

Note: Conceptual instances are “virtual”, no actual instances are necessarily created.

NIEM Data

STIX

STIX-Canary_Corp : Identity

victim

STIX-Breach of Canary Corp : Incident

description = "Intrusion into enterprise network"
victim = STIX-Canary_Corp

Conceptual

damaged by

Breach of Canary Corp : Incident

describes

described by

Intrusion into enterprise network : Description

damages

Canary Corp : Victim

{property}

NIEM

NIEM-Breach of Canary Corp. : IncidentType

IncidentAugmentation = NIEM-Breach of Canary Corp
IncidentObservationText = "Intrusion into enterprise network"

IncidentAugmentation

NIEM-Canary Corp : VictimType

IncidentVictim

«AugmentationType»
NIEM-Breach of Canary Corp : IncidentAugmentationType

Derived NIEM Data

```
<Q_:Incident >
    <nc:IncidentObservationText>Intrusion into enterprise network</nc:IncidentObservationText>
    <j:IncidentAugmentation >
        <j:IncidentVictim >
            <j:VictimOrganization  xsi:type="nc:OrganizationType">
                <nc:OrganizationName>Canary Corp</nc:OrganizationName>
            </j:VictimOrganization>
        </j:IncidentVictim>
    </j:IncidentAugmentation>
</Q_:Incident>
```

Note that only elements of interest that have a correspondence between STIX and NIEM are mapped. However, this kind of summary may be what is needed by, for example, law enforcement.

Threat / Risk and data

- The threat risk specification does not create yet another data format
- It maps to and from existing data, such as STIX, NIEM, EDXL and others
- Remember – our goal is federation and interoperability *across* domains, disciplines and technologies.
- Each concept we want to share or federate is mapped, but we do not try and map the details of interest to those “inside” the domain – they are fine where they are.

Implementation Patterns

- Technology implementations make the specification real – create the capability
- Multiple technologies could be used
  - Big data
  - Semantic Web
  - Ontologies
  - Rules
  - Information Brokers
  - Analytics Engines
  - Simulation Engines
  - Graph, XML and/or Relational Database

Where are we

Conceptual Model

- Synthesizes Input from NIEM, STIX, OGC and others
- Multiple use cases
- Results in a solid draft foundational model

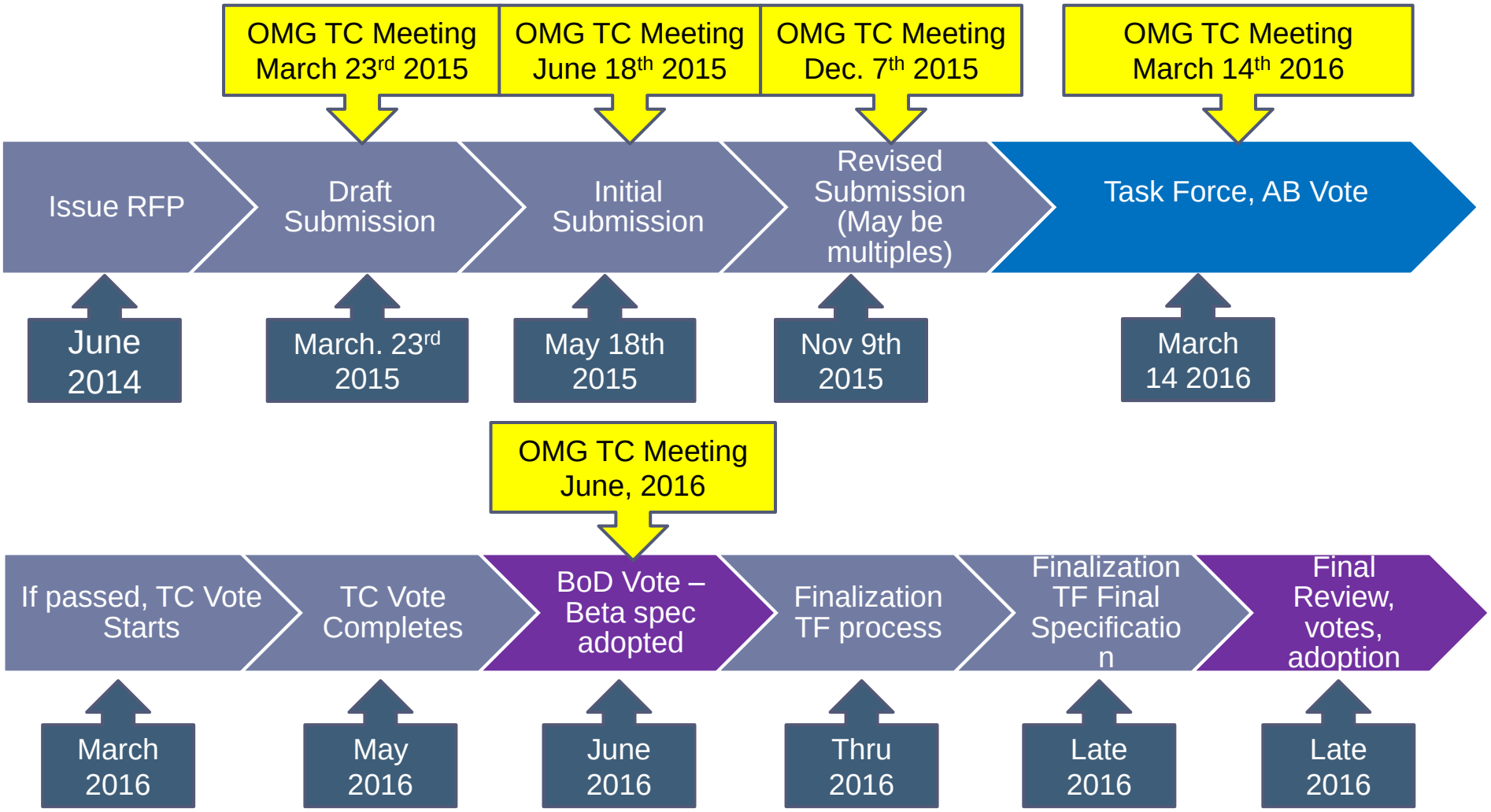
Mappings

- Mappings are in-progress
- Most are information
- STIX has early prototype

Specification

- Draft initial specification is available on threatrisk.org
- Initial proposals will be submitted to OMG in May 2015

OMG RFP Process Time Line



Who are we

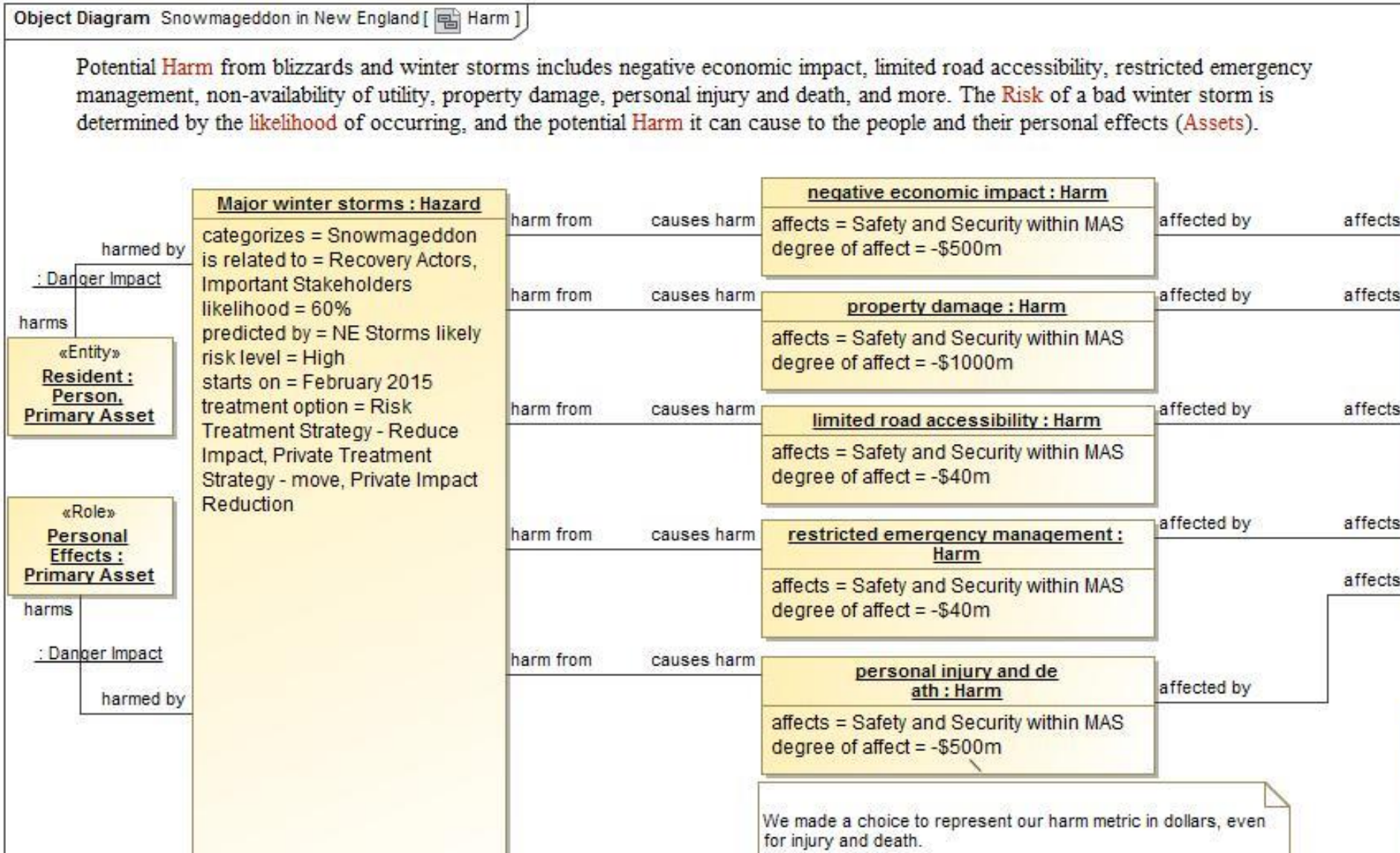
- Demandware
- Model Driven Solutions
- KDM Analytics, Inc.
- LEADing practice, Inc.
- RSA, The Security Division of EMC
- U.S. Information Sharing Environment PMO
- U.S. National Information Sharing Model (NIEM) PMO
- U.S. Air force
- U.S. Defense Security Services
- California Public Safety

Join us!

- We are an open community focused on sharing and federating cross-domain threat and risk information
- Participate deeply or just follow and review
- We welcome use cases, existing schema, models, data sources, data consumers, vendors…

- Talk to us!
- Or, see: http://www.threatrisk.org

Each concept of our scenario is captured



Treatment concepts