TLP: GREEN

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

Energy Sector Risk Assessment Methodology

NASEO Energy Security Boot Camp

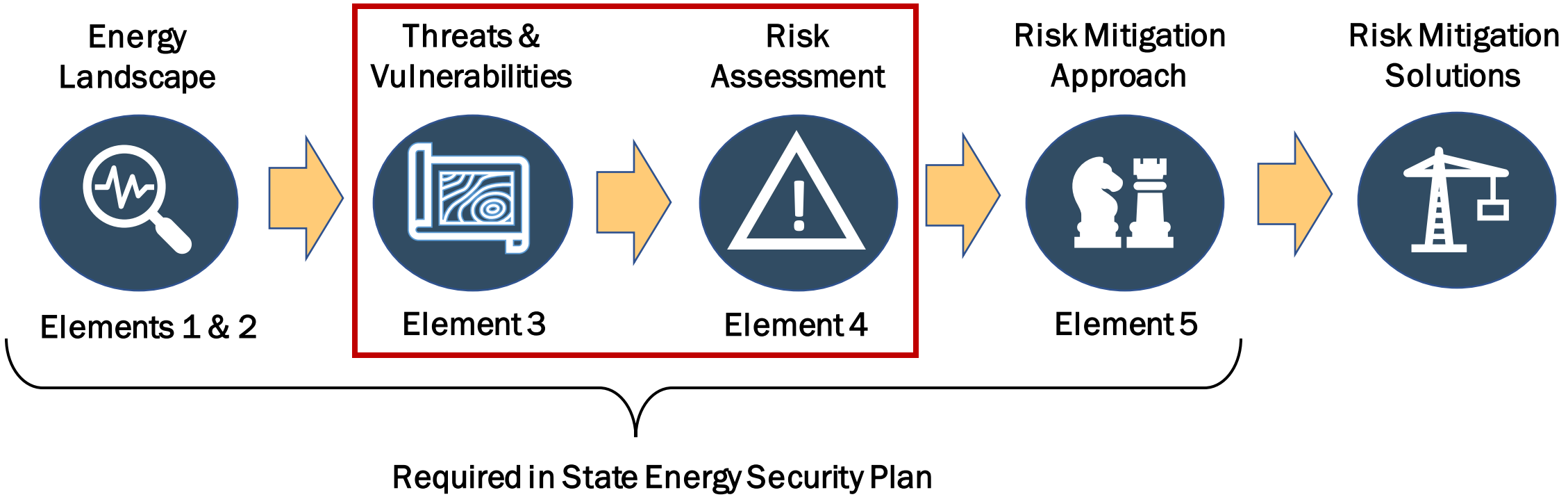
Kevin DeCorla-Souza, Senior Director, Energy Markets, ICF

April 2023

Why Do Energy Sector Risk Assessment?

- Requirement in State Energy Security Plans
- Informs preparedness activities
- Informs energy sector risk mitigation investment priorities

Risk Assessment & SESP Requirements



Requirements of Risk Assessments

Must:

- Take threat, vulnerability, and consequence into account
- Be informed by energy asset and event data
- Classify risks so that they can be compared with one another on a relative basis
- Follow a consistent, repeatable methodology

Need not:

- Be overly precise
- Consider every possible threat
- Evaluate every asset

Key Definitions

RISK

The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences

THREAT

Anything that can expose a vulnerability and damage, destroy, or disrupt energy systems, including natural, technological, manmade/physical, and cybersecurity hazards.

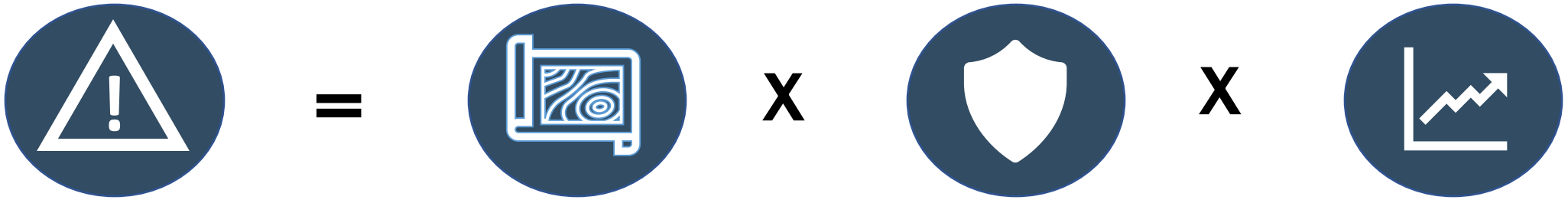
VULNERABILITY

Weaknesses within infrastructure, processes, and systems, or the degree of susceptibility to various threats. Vulnerabilities may be specific to the threat, energy type, and infrastructure component.

CONSEQUENCE

Effect of an event, incident, or occurrence, including immediate "direct" impacts and cascading "indirect" impacts

Risk Assessment Formula



RISK

- Risk scores are given to combinations of specific assets and specific threats

THREAT

- Probability of occurrence on an annual basis, typically on a scale of 0 to 100%
- Specific to location
- Informed by climate data (NOAA, USGS, etc.) and Hazard Mitigation Plan

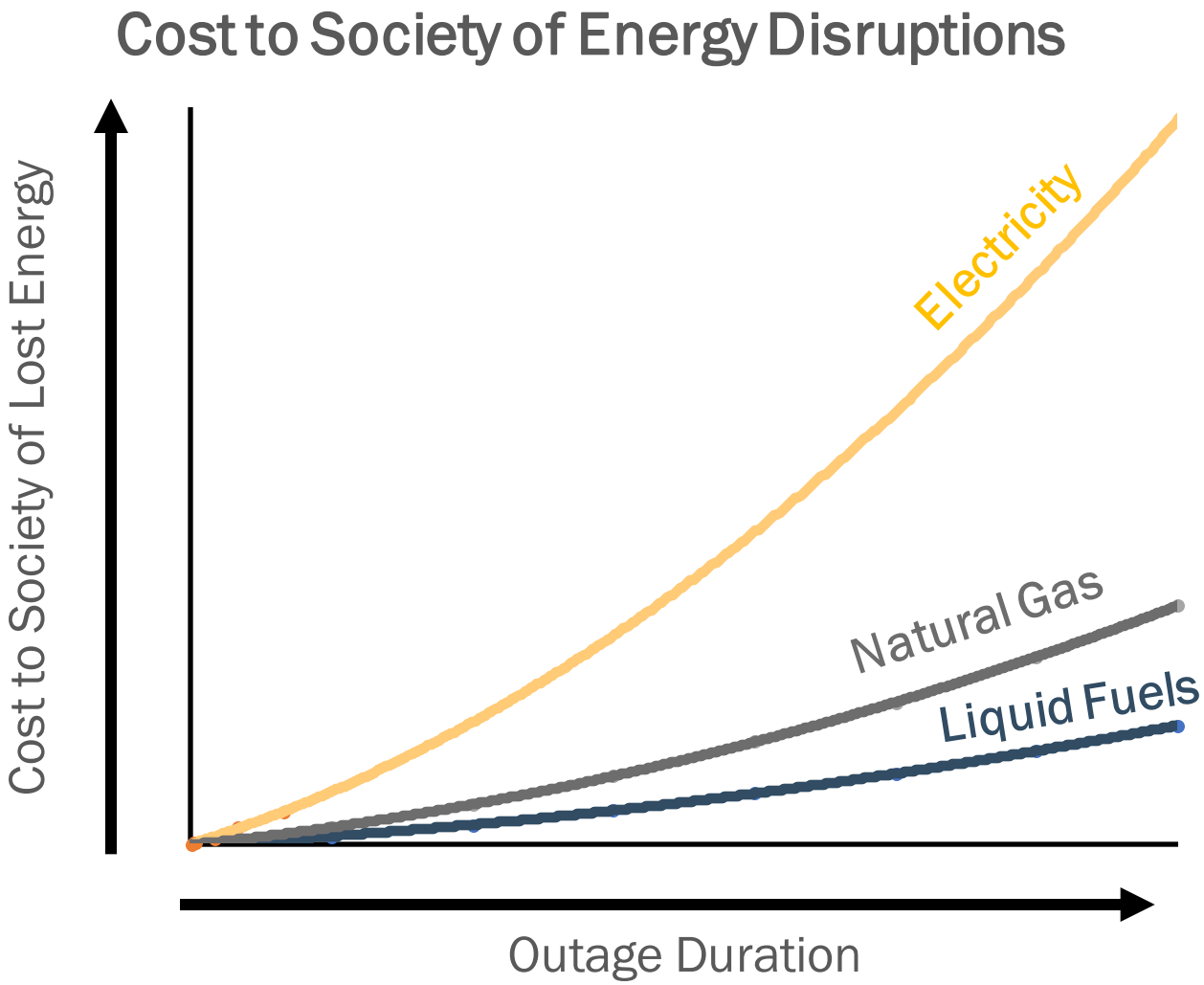
VULNERABILITY

- May be interpreted as the expected outage duration from exposure to a given threat
- Specific to asset type and region
- Should include inter-dependency considerations
- Informed by subject matter experts and discussions with operators

CONSEQUENCE

- Specific to asset and market
- Direct consequence = lost energy supply
- Indirect consequence = cost to society of lost supply
- Informed by analysis of asset and market data

Indirect Consequence: Cost to Society



Risk Assessment Formula - Expanded

RISK = **THREAT** x **VULNERABILITY** x (**DIRECT CONSEQ.** x **INDIRECT CONSEQ.**)

RISK	THREAT	VULNERABILITY	DIRECT CONSEQ.	INDIRECT CONSEQ.
Exp. Annual Impact ($)	Annual Probability (% per Year)	Outage Duration (days)	Energy Lost per Day (MWh, bbls, MMcf, etc.)	Cost per Unit Lost ($/MWh, $/bbl, etc.)

DISCLAIMER

The following walk-through is presented as an example of risk assessment methodology. The example utilizes "dummy data" that are NOT scientifically derived and are presented only for the purpose of explaining the methodology.

Example: 1-in-100 Year Threat to 500 kV Substation

RISK	=	THREAT	x	VULNERABILITY	x (	DIRECT CONSEQ.	x	INDIRECT CONSEQ.)
Exp. Annual Impact ($)		Annual Probability (% per Year)		Outage Duration (days)		Energy Lost per Day (MWh)		Cost per Unit Lost ($/MWh)
$2.4 mn	=	1%	x	5 days	x	12,000 MWh	x	$4,000

$240 million

How do I implement this in practice?

- Where do I get threat information (% per year)?
- How to I estimate vulnerability (outage days)?
- Where do I get consequence information (energy lost)?
- How do I estimate indirect impacts ($/energy lost)?
- How do the resulting risk scores feed into the Risk Mitigation Approach (Element 5)?
- How can this approach be used for Cost-Benefit Analysis?

Risk Assessment Guidebook Coming Soon!

Discussion