COLLABORATION, COORDINATION AND COMMUNICATION: BUILDING RESILIENCE

Anne Strauss-Wieder

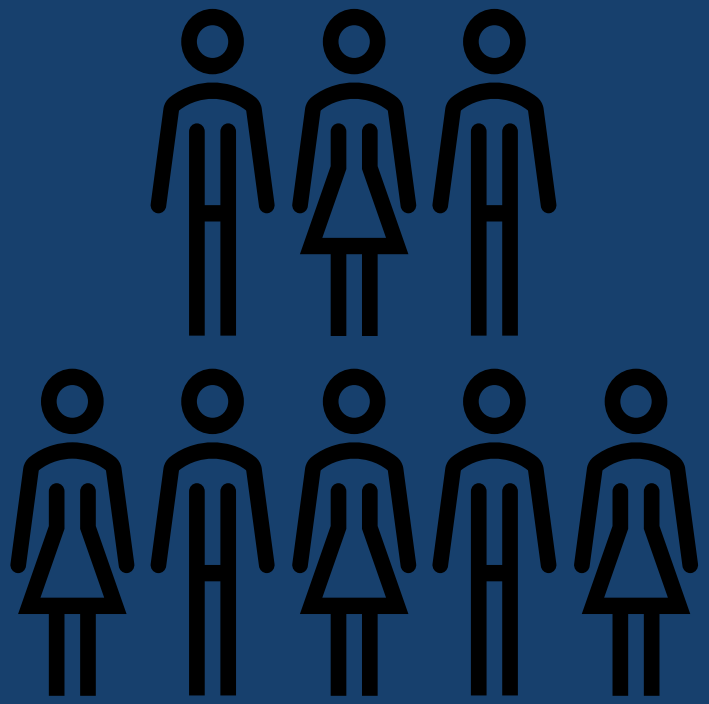
DEFINING SUPPLY CHAINS AND RESILIENCE

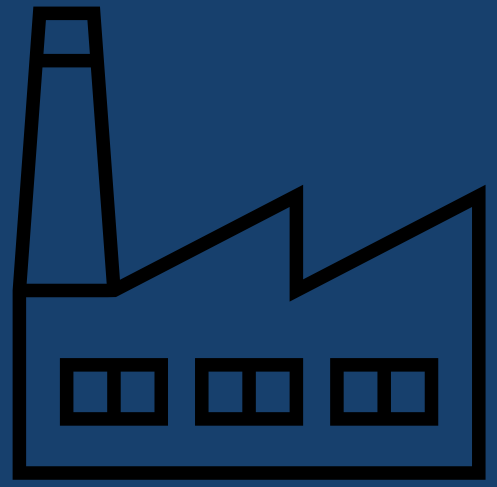
How goods move starting from materials sourcing to where production occurs and then to where they are consumed.

Business continuity refers to the capacity to continue to delivery products or services after a disruptive event.

COMMUNITY CONTINUITY

Community continuity refers to the capacity to continue to support the area's population and secure its economic base after a disruptive event.





Definition Source: Anne Strauss-Wieder

THE IMPORTANCE OF BUSINESS & COMMUNITY CONTINUITY

TR News 311 September-October 2017, p. 14.

- 30 percent of all companies that experience a catastrophic loss fail with in the first two years after the event.
- Another 29 percent shut down after this time.
- Severe and potentially permanent economic losses for communities.

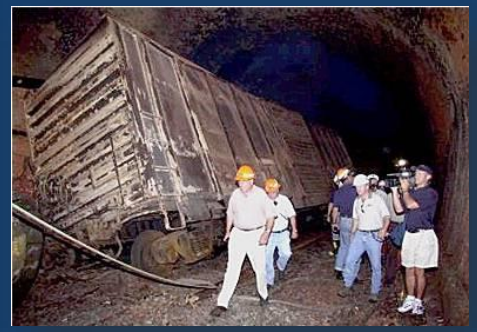
Statistics source: https://www.nado.org/lessons-from-the-storm-case-studies-on-economic-recovery-and-resilience/

SUPPLY CHAIN RISK CATEGORIES

- Natural Disasters
- Human Caused Disruptions
- Supplier Risks
- Cybersecurity and Information System Failures
- Transportation Failures
- Quality Failures

THE DISRUPTION SPECTRUM

Planned Disruptions	Predictable Disruptions	Rapid Disruptions	Abrupt Disruptions	Continuing Disruptions
Columbia River Closure, Road Closures	Winter Weather, Labor Actions	Hurricane Katrina, Superstorm Sandy, Pandemic	9/11, Howard Street Tunnel Fire, 2017 Cyberattack, 2024 Dali	Ukraine War, Middle East Conflict, Ongoing Humanitarian Relief



Source of Chart: Anne Strauss-Wieder
Photos from various sources

2017 MAERSK CYBER ATTACK

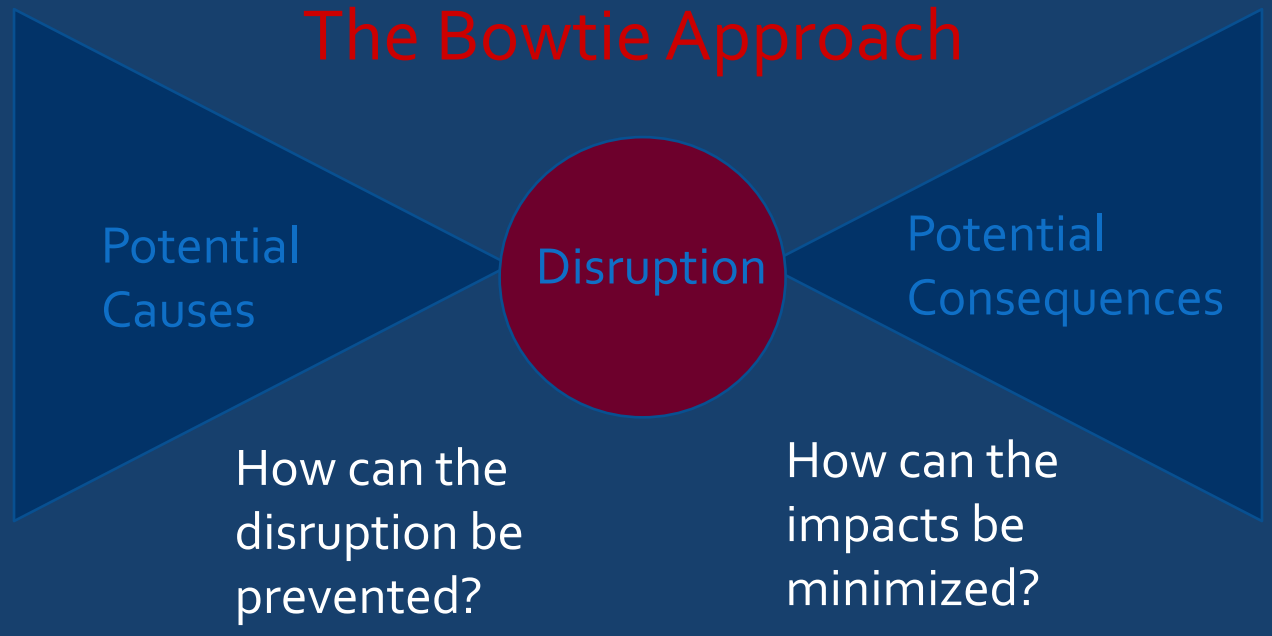
Characteristics	Information Disruption: 2017 NotPetya Cyber Attack
Geographical Scope Affected	• Global – All information systems went down
Freight Facilities Affected	• Vessels, terminals and company infrastructure around the world.
Commodities and Shipments Affected	• Multiple commodities and shipments affected
Recovery Time from Disruption	• 10 days involving “a complete new infrastructure of 4,000 new servers, 45,000 new PCs, and 2,500 applications.” • Estimated cost to company of the attack: $250-300 million.

Source on Recovery Information:
https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

UNDERSTANDING THE CAUSES

Analyze using the "Bowtie Approach."

Develop a "Risk Register."



ANALYZING YOUR FREIGHT SYSTEM AND SUPPLY CHAINS

- Determine what the most important commodity movements are from community and business continuity perspectives.
  - *Now and in the future*
- Identify the key freight system elements (road, rail, waterborne, air cargo, and facilities) most necessary to keep these goods flowing.
- Consider emerging trends, technologies and public goals.
- Ascertain freight movement alternatives and undertake scenario analyses.
- Identify and develop working relationships with the key partners.

MOVE FORWARD TOGETHER

THANK YOU

Anne Strauss-Wieder

- Anne.strausswieder@rutgers.edu

Sources: UPS, ShareAmerica, USCIB (Gettty Images), Amazon