ERM identifies and manages Emergent Risks which threaten stakeholder interests

Law Enforcement plays a pivotal role

R. K. Gardner

10 November, 2020

New World Technology Partners

ERM
Establishes Enterprise Risk Policy & Manages Significant Breaches

1. Allocating Risk Management Resources *(expenditures, capital reserves, cash)* and Establishing Disclosure Strategies *(for Shareholders, Clients, Partners, Workforce, Regulators, Public and Adversaries)*, commensurate with enterprise exposure.

2. Mitigating Enterprise Peril from *Emergent Risks*(1) which directly *(often immediately)* threaten mission, value and solvency

which requires knowledge of the behavior of all players and elements of organizations' complex Cyber EcoSystem

federal & local law enforcement plays a pivotal role

(1) Behaviors and risks from unexpected, often overlooked sources

New World Technology Partners

Emergent, Systemic Risks

Reputation Risk

Affecting Shareholders, Sales, Partnering, Workforce, Regulators and the Public

- **Heartland** lost almost 50% of share value in one day
- **Snowden Breach** impacted NSA Authorities, Alliances, DIB trust, Public Trust

System Complexity Risk

Presenting channel conflicts, defect density & race conditions

- **2003 NE Power Outage** took down electric power, causing consumer, industry and government operations expense and peril – could be a cyber vulnerability

Embedded 3rd Party Risk

When partners are given direct access to core assets

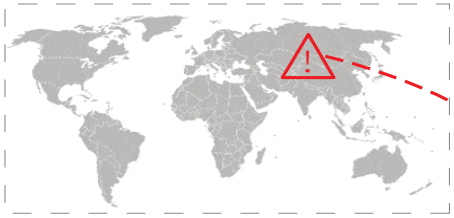
- Counterparty risk facilitated **Lehman Brothers** and **AIG** collapse during the 2008 financial crisis – could be a cyber vulnerability

Identify and Prepare

1. Determine configuration and dynamics of enterprise's complete cyber eco-system
2. Examine all Sources and Channels which may cause and propagate emergent breaches (accidental or intentional)
3. Instrument infrastructure
4. Alert and Coordinate with Law Enforcement (International, Federal and Local)

New World Technology Partners

Enterprise Risk Architecture enables Financial Consequence Analysis



Attack Scenarios

Adversary/ Threat Analysis

3rd Parties

Mathematical Behavior Analysis

- Information Assets and Ctl Signals
  - C, I & A coefficients
  - Latency & Duration time coefficients

Departmental Impact Analyses

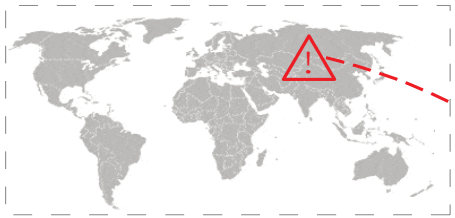
- Net Revenue
- Assets
- Ops/Mission

Prioritize Cyber Risk Expenditures

Aggregated Enterprise Risk

- **Financial** ✓EPS/Net Revenue ✓Capital ✓Free Cash Flow
- Reputation
- Mission

Then, Quantify and Analyze Reputation/Trust Consequences



Attack Scenarios

Adversary/ Threat Analysis

3rd Parties

Mathematical Behavior Analysis

- Information Assets and Ctl Signals
  - C, I & A coefficients
  - Latency & Duration time coefficients

Departmental Impact Analyses

- Net Revenue
- Assets
- Ops/Mission

Sentiment Analysis

Aggregated Enterprise Risk

- Financial
- **Reputation**
- Mission

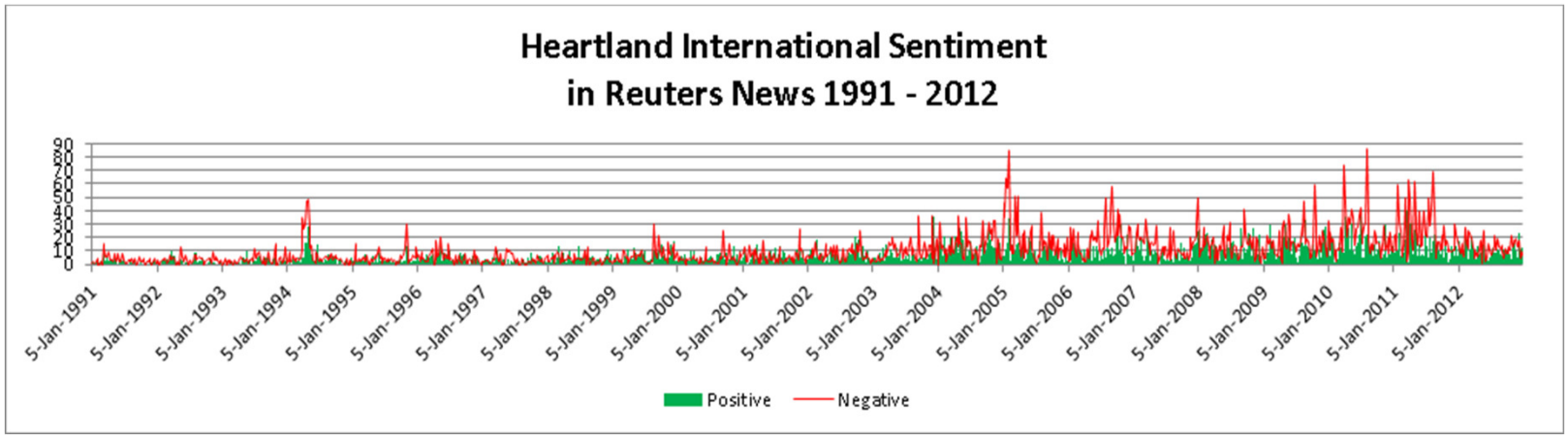
✓Investors
✓Public
✓Regulators/Congress
✓Allies/Partners
✓Workforce
✓Adversaries

New World Technology Partners

NLP Sentiment Analysis Indexes Stakeholder Trust

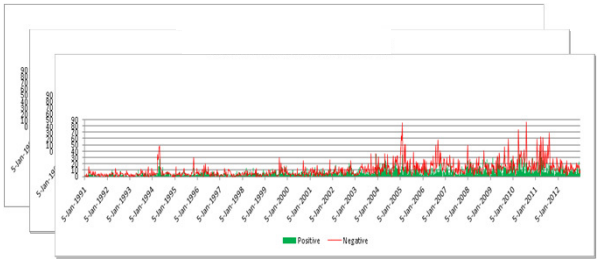
Measures subject-object-verb triads: indices reflect character & intensity of interactions between and among events, actors and organizations

When correlated against events, creates a histogram of reputation among shareholders, clients, partners, regulators, the public… *also adversaries!*

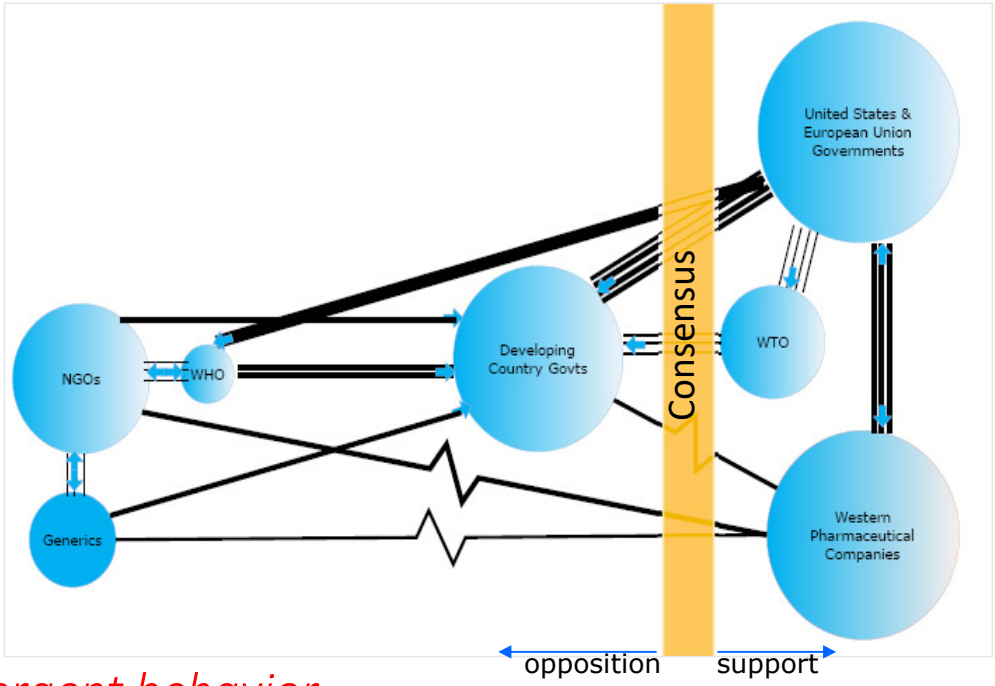


New World Technology Partners

Visualization of Collective, Consensus Attitude



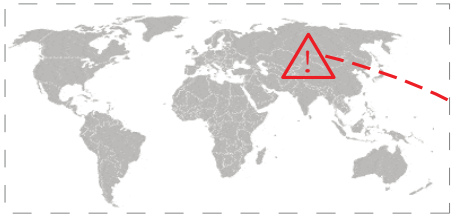
Map of Stakeholders' Positions



Provides clues to potential sources of emergent behavior…
…or strategies for influence

New World Technology Partners

Integrate to Quantify Enterprise Mission Consequences



Attack Scenarios

Adversary/ Threat Analysis

3rd Parties

Mathematical Behavior Analysis

- Information Assets and Ctl Signals
  - C, I & A coefficients
  - Latency & Duration time coefficients

Departmental Impact Analyses

- Net Revenue
- Assets
- Ops/Mission

Sentiment Analysis

Aggregated Enterprise Risk

- Financial
- Reputation
- **Mission**

✓Valuation
✓Solvency
✓Continuity

New World Technology Partners

Look for Potential Emergent Risks

See if/how 3rd party sources may present hidden behaviors and incidents

- Emergent Behavior Modeling (NPS/MP)
- Event Tree Analysis
- Covert Channel Analysis (NSA)
- FMECA(2)

(2) Failure Modes Effect and Criticality Analysis – system engineering practice attributed to Bell Laboratories

Anticipate Events to Deter, Protect or Respond

Inform and Consult with Government & Law Enforcement "WATCH" operations **(e.g. FBI, DHS, US-CERT, NYPD, LAPD, et al per U.S. Cybersecurity Information Sharing Act)**

Examine Dark Web, Securities Trading, Pulsing, Social Media,

Also collaborate with Peer Enterprises to share incident informaion (e.g. US Banks have successful info sharing policies)

New World Technology Partners

Be Prepared!

1. Examine enterprise's complete cyber eco-system

2. Examine all Sources and Channels for Emergent Behavior Possibilities

3. Alert and Coordinate with International, Federal and Local Law Enforcement

New World Technology Partners