

THE RISK MANAGEMENT ASSOCIATION

The Convergence of Reputation Risk with Cyber and Geopolitical Risk

Robert K. Gardner, New World Technology Partners

Doug Bond, Ph.D, Harvard University



Snowden Leak...

Caused U.S. Defense/Intel Agencies Significant Reputation Harm

Caused Congressional Oversight Committees to Reduce Authorities

Caused Appropriation Committees to Reconsider Funding

Caused Allies to Reconsider IP and Intelligence Sharing

Affected IC Workforce Recruitment and Retention

Assisted Adversaries' Recruitment and Financing



Which Materially Impacted Our Financial and Mission Capability

Agenda

Dilemma in the Boardroom

Reputation Risk Impact

Measuring Reputation Risk

Managing Reputation Risk

Dilemma in the Boardroom

- ▶ We must protect assets and shareholder value
 - Share Value = EPS x P:E Multiple**
- ▶ Result is dominated by P:E Multiple factors including Capital, **Reputation**, IP, etc.
- ▶ Yet we have no direct link between Cyber Risk and these risks, which affect current and future value



COSO pov of Enterprise Risk Management



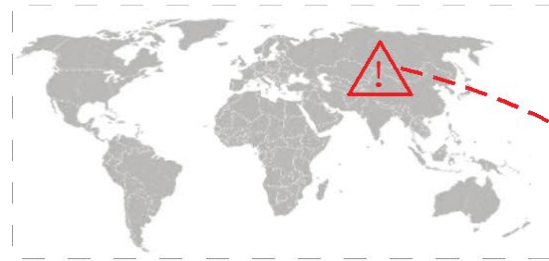
NIST Framework informs ERM and Reputation Risk

Integrating Cybersecurity and Enterprise Risk Management⁽¹⁾

- Pending publication acknowledges Reputation Risk as an Enterprise Risk Management element.
- Establishes an Enterprise Risk Register approach to connect Cyber Security analysis with ERM deliberations.
- Rolls up cyber risks to Quantify Financial, Mission (*i.e. Solvency & Valuation*) and Reputation Risk Exposure.

(1) NIST IR 8286 published for industry comment

1st Quantify Enterprise Risk *through a Wide-angle Lens*



Attack Scenarios

Adversary/ Threat Analysis



Behavior Analysis



Ops/Dept/Project Impact Analyses

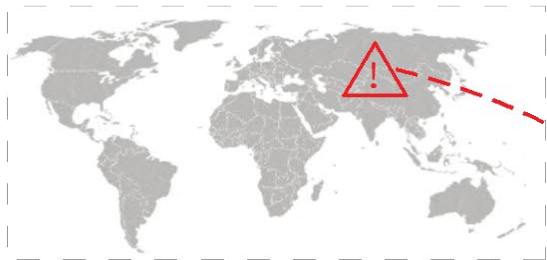
- Net Revenue
- Assets

Sentiment Analysis



Aggregated – Enterprise Risk

- Financial
- Reputation
- Mission



Attack Scenarios

Adversary/ Threat Analysis



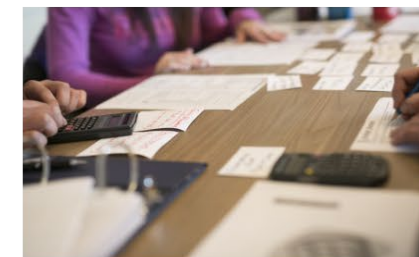
Behavior Analysis



Departmental Impact Analyses

- Net Revenue
- Assets
- Ops/Mission

Sentiment Analysis

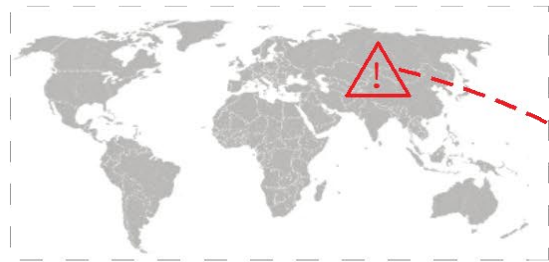


Aggregated Enterprise Risk

Prioritize Cyber Risk Expenditures

- ✓ EPS/Net Revenue
- ✓ Capital
- ✓ Free Cash Flow

- **Financial**
- Reputation
- Mission



Attack Scenarios

Adversary/ Threat Analysis



Mathematical Behavior Analysis



Departmental Impact Analyses

- Net Revenue
- Assets
- Ops/Mission

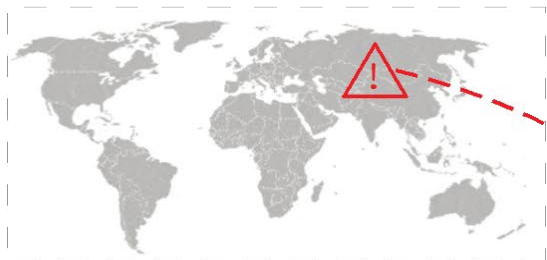
Sentiment Analysis



Aggregated Enterprise Risk

- Financial
- Reputation
- **Mission**

- ✓ Solvency
- ✓ Valuation
- ✓ Capability



Attack Scenarios

Adversary/ Threat Analysis



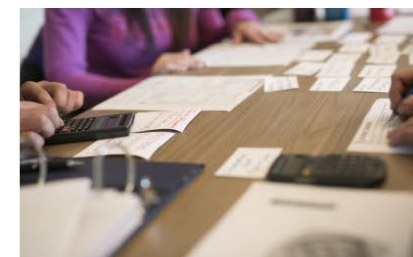
Mathematical Behavior Analysis



Departmental Impact Analyses

- Net Revenue
- Assets
- Ops/Mission

Sentiment Analysis



Aggregated Enterprise Risk

- Financial
- **Reputation**
- Mission

- ✓ Investors
- ✓ Clients/Constituents
- ✓ Public
- ✓ Regulators/Congress
- ✓ Allies/Partners
- ✓ Workforce

Consider the Full Impact of Reputation Risk

Public

- Customer Sales
- Constituent Votes
- Shareholders
- MktCap/Volatility

Workforce

- Recruitment
- Retention

Allies & Partners

- Shared Intelligence
- Shared Intellectual Property
- Cooperative Ops

Regulators

- Appropriations
- Authorities

Adversaries

- Recruitment
- Funding

Measuring Reputation Risk

Sentiment analysis (or opinion mining) is a **natural language processing** (NLP) technique used to determine whether data is positive, negative or neutral or ambivalent.

Often performed on textual data to help organizations monitor stakeholder **sentiment**, understand their needs, or anticipate their reactions.

Focus of the sentiment analysis,
typically:

Countries,
Corporations,
Markets, or
Individuals

Domains of relevance, for example:

Social, Political, and Economic sectors

May also be used with domains specific to financial risk analyses such as

Confidentiality, Integrity, and Availability

Affects analyzed include

Scope – singularity of the focus

Magnitude – lower to higher

Polarity –
positive
ambivalent / mixed / neutral
negative

Sample Output

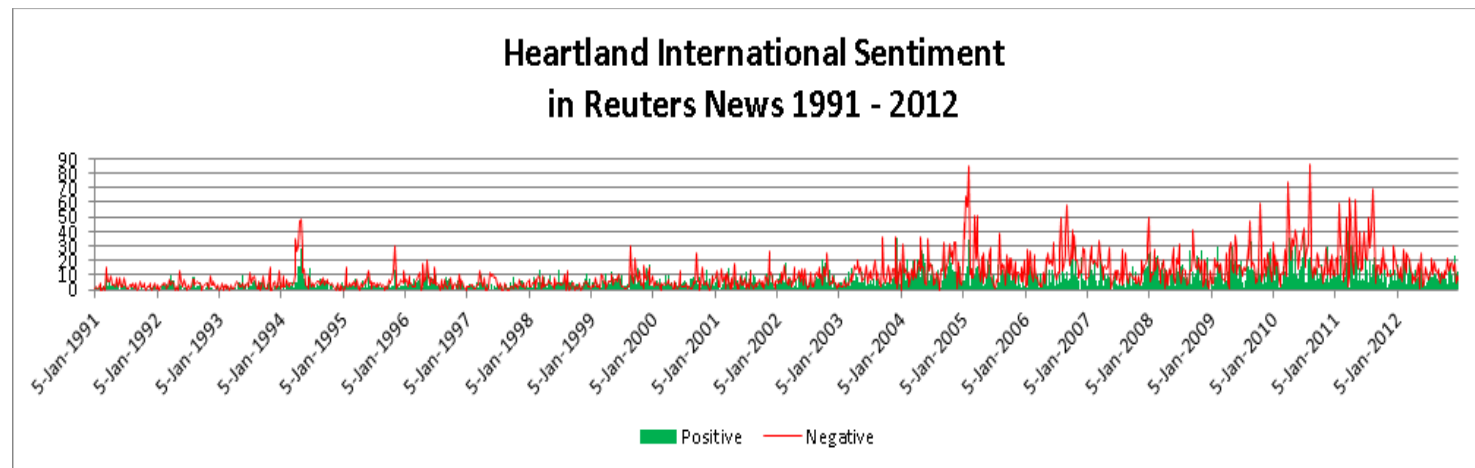
| Country | Week Ending | SOCIAL Score | ECONOMIC Score | POLTICAL Score | Overall Score | Positive Score | Negative Score | Overall Score Weighted |
|---------|-------------|--------------|----------------|----------------|---------------|----------------|----------------|------------------------|
| USA | 5-Jan-91 | 248 | 351 | 154 | 753 | 178 | 119 | 43.17 |
| USA | 12-Jan-91 | 557 | 739 | 257 | 1553 | 366 | 255 | 36.84 |
| USA | 19-Jan-91 | 687 | 704 | 251 | 1642 | 401 | 354 | 11.35 |
| USA | 26-Jan-91 | 645 | 615 | 185 | 1245 | 368 | 766 | 9.74 |
| USA | 2-Feb-91 | 666 | 657 | 326 | 1649 | 449 | 463 | 49.49 |

Measured Stakeholder Sentiments

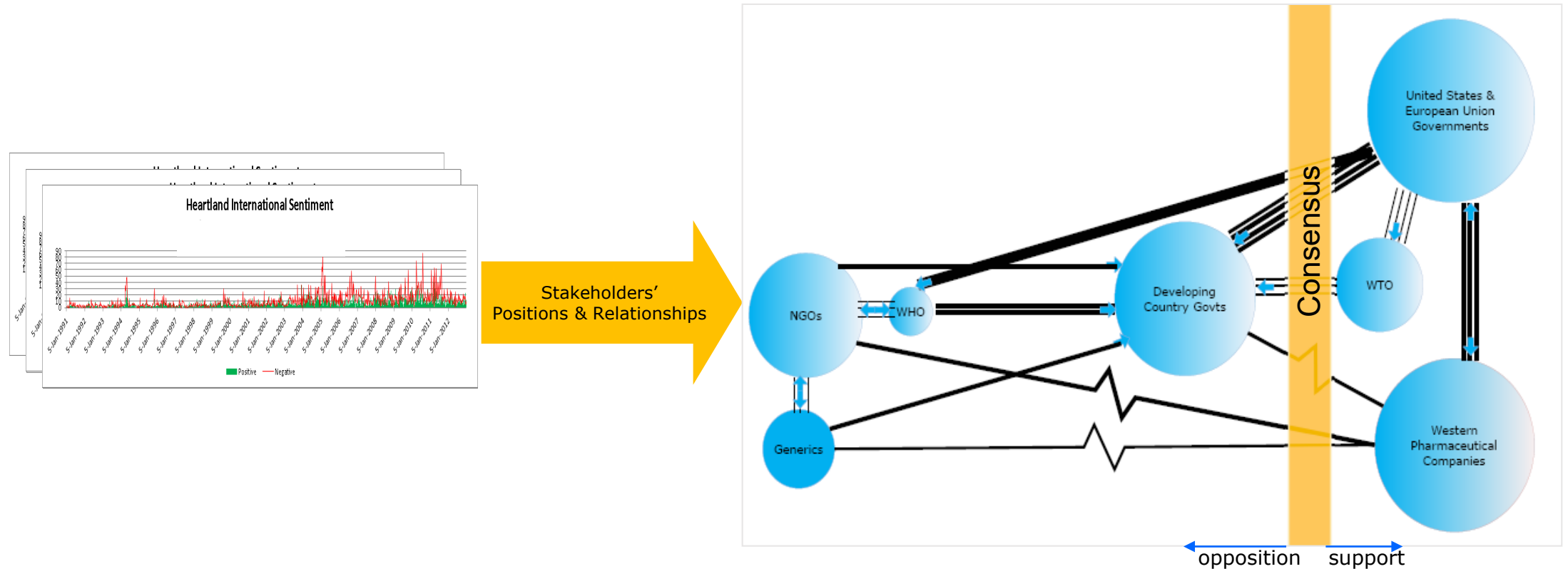
NLP measures subject-object-verb triads.

Reflects polarity & intensity of actors' (people or organizations) sentiments pursuant to (cyber) events.

When correlated with previous attacks, it creates a histogram of shareholder, client, regulator/government official and public sentiment



Landscape of All Significant Stakeholders



Bubble Size, Position and Connection = Intensity, Attitude and Relationships... resulting in net consensus

Compare Response/Influence Strategies

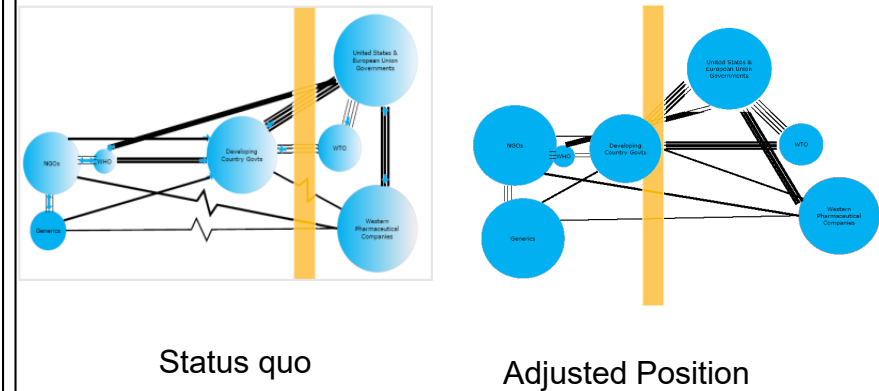
Focus attention on pivotal actors

Explore mitigation options

1. Disclosure
2. Investment
3. Diplomacy
4. Other

Illustrate potential consensus change when individual attitude shifts occur

Explore
"what-if" scenarios



Geopolitical Business Example

American company pursued privatizing electric power in the Republic of Georgia

- Analysis of multiple stakeholders' support/opposition opinions (Georgia Gov't, Industry, Consumers; Russia; World Bank; US; etc.)
- Highlights negative impact of lost corporate support and increasing Russian hostility
- Supported decision to sell to Russian utility UES



Managing Reputation Risk

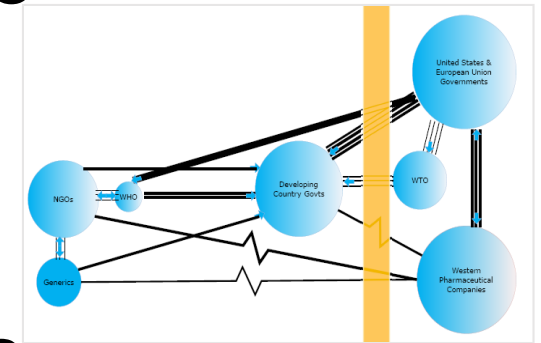
- Maintain Reputation Situation Awareness
- Post Required Disclosures
- Produce Proactive Disclosures
- Other

Establish Reputation Situation Awareness

Aggregate and track diverse stakeholders' individual and collective sentiments to understand and manage consequences

Connect the silos:

- Marketing contacts with consumers and partners
- Investor Relations contacts with Analysts & Investor Groups
- CFO contacts with Banks and Money Managers
- General Counsel contacts with Regulators



Required Disclosures

Periodic



Out-of-Cycle



Voluntary Disclosures Maintain Trust

- Public - Press, Newsletters
- Investors - IR Partner Communications, Earnings Calls
- Workforce - Internal Cyber Training, Special Communication
- Strategic Partners – Executive Calls
- Regulators - Contact Before Other Stakeholders
- Law Enforcement - Periodic Local, State, FBI Contact

Conclusion

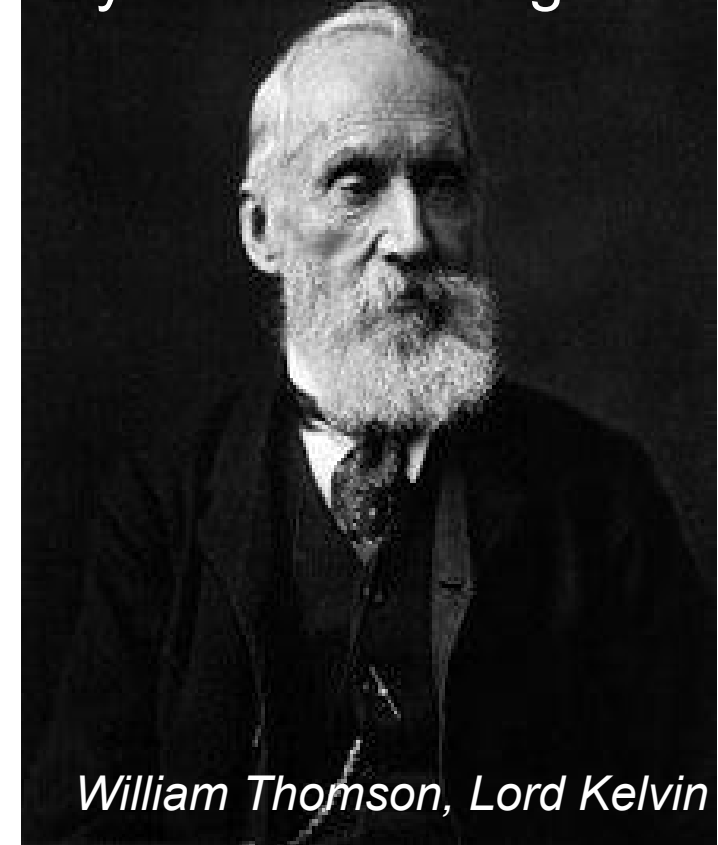
Know Stakeholders' Opinions

- Measure each and all groups
- Update changing sentiments

Provide Prudent Disclosures

- As Required
- Periodically, Proactively
- Strategically

If you can't measure it,
you can't manage it



William Thomson, Lord Kelvin