QUANTIFYING EMERGING RISKS

Melissa Boudreau, FCAS

19 December 2018

What are “Emerging Risks”

Emerging risks are sources of potential injury, property damage, environmental damage, or other economic or non-pecuniary damage arising from causes that are either entirely new or materially changing in character.

What types of things constitute emerging risks?

Most emerging risks arise from innovation.

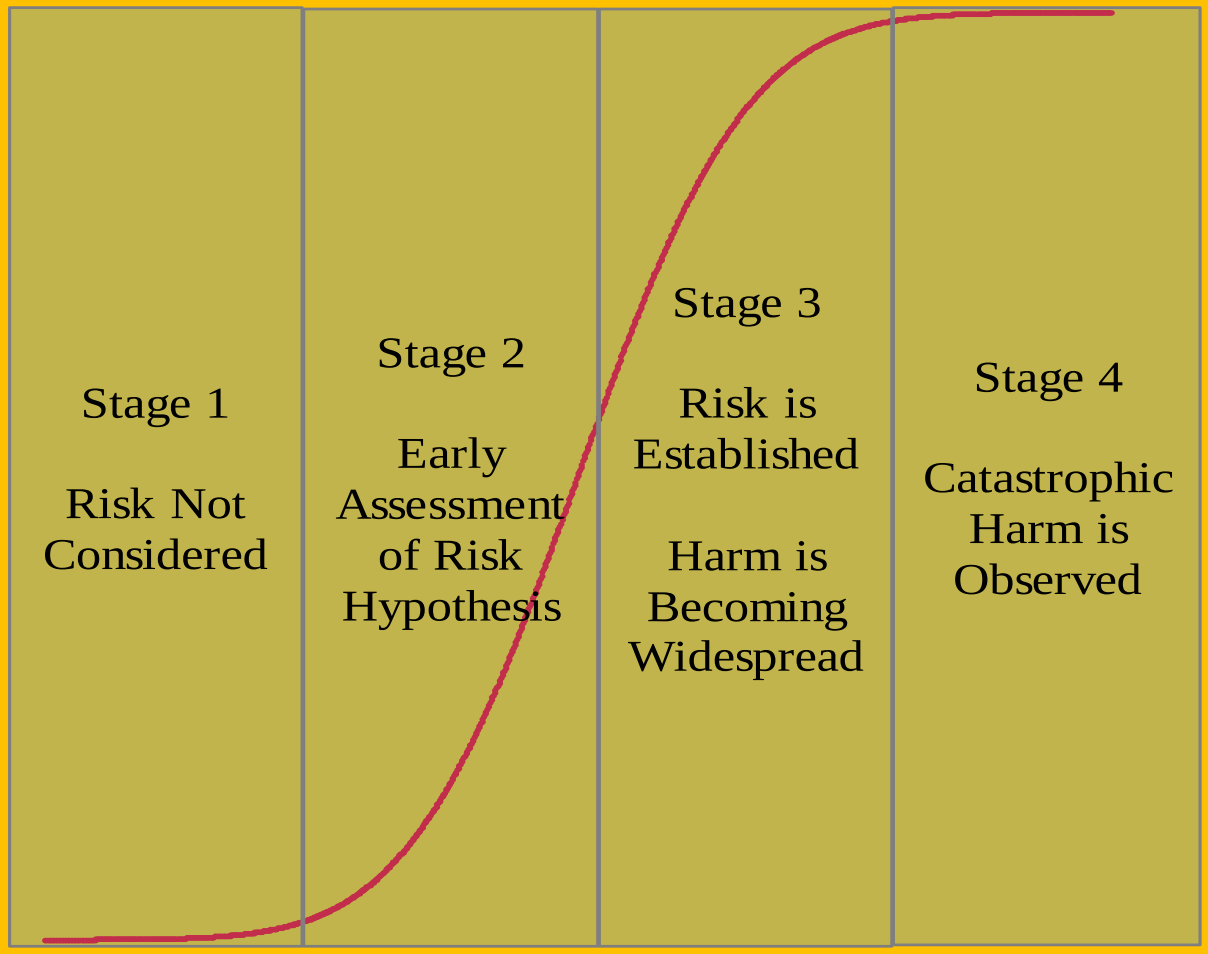
- Transformative technologies introduce entirely new categories of risks.
  - Cyber risks
  - Autonomous transport
- Innovation in existing fields often adds new risks with familiar patterns
  - Chemicals and pharmaceuticals
- Societal changes may cause familiar risks to change in character
  - Economic disruption
  - Demographic changes

The typical emerging risk process today…

Stages of Risk Emergence

There is often an element of latency in discovery or manifestation.

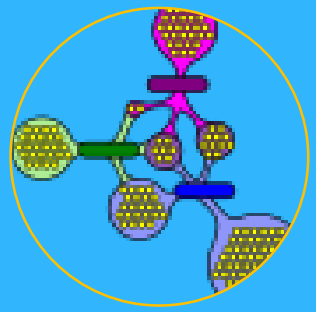
Sometimes the duration of latency is extreme.



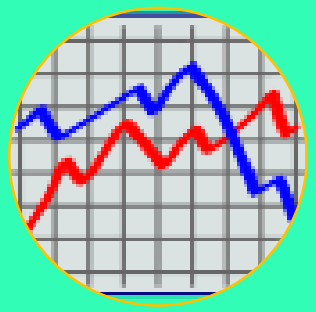
Key Features of Emerging Risk Models

Structural models	Capture relationships, correlation and causes
First principles	Model the underlying processes
Forward-looking	Model the leading indicators
Exposure-based	Overlay exposure of interest over granular “universe” model

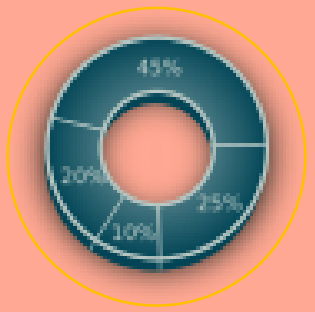
Modelling Process Overview



Research and Submodule Creation



Simulate Future Outcomes



Analyze Effects

Building the Model

Process for Quantifying Risk

Identify risks

- Natural phenomena – are they changing in frequency or character?
- Technological innovation – identify leading indicators
  - Substance toxicity – has toxicology literature started, increased in pace, or obtained positive findings?
  - Disruptive technology – what unforeseen consequences are possible?
- Societal – what is changing, how, and why
  - What effect will these changes have?

Identify drivers of event frequency

Building the Model

Process for Quantifying Risk

Estimate severity of possible events

- Bodily injury harm – what are direct medical costs and indirect costs (loss of productivity / quality of lift / wrongful death)?
- Property or environmental harm – what is cost of remediation?
- Economic injury – what is the range of damages?

Evaluate correlation

- Are events contagious? Positively or negatively?

Reflect dynamic response

A Multidisciplinary Effort

Consider the question of quantifying property losses from two effects of climate change – inundation and more frequent and/or more powerful storms.

This involves several specialties:

- Climatologists review seminal literature exploring the magnitude and trajectory of change, and what the likely contributing causes are.
- Data scientists collaborate with the client scientists to identify the characteristics of literature supporting or refuting hypotheses, and analyse the entire corpus of literature.
- Meteorologists model the incidence of atmospheric and oceanic conditions conducive to cyclogenesis, and simulate wind and precipitation fields.
- Hydrologists analyse precipitation runoff and storm surge.
- Engineers model the effect of winds on buildings and model partial or total failures.
- Economists estimate the replacement or relocation costs from property and infrastructure damage, including the "mesoeconomic" effects of abrupt demand increase and supply chain disruption.
- Actuaries estimate the overall loss and its effect on insurers.

Example: Cyber Risk

Economic Consequences

First-Party Damages

- Theft
- Business Interruption
- Reputation Damage
- Equipment Damage

Third-Party Damages

- Breach of Privacy
- Misuse of Data
- Slander/Defamation
- Harmful Content
- Notification / Remediation

Example: Cyber Risk

Underlying Processes

Breaches – What Causes Them?

- Technical "arms race" – even the careful application of "best practices" does not immunise an organisation from risk
- End users and system administrators may fall prey to clever "social engineering"
- Carelessness or cost-limiting measures elevate hacking risk
- Malicious or questionable management decisions

- Dynamic Elements
  - Detection
  - Mitigation

Example: Cyber Risk

Analyze Exposure and Results

- Model each attack vector
- For each insured enterprise, enumerate exposures
  - Servers, networks, devices
  - Less obvious: HVAC controls, building security
  - Controlled data entry/exit points
- Simulate effect of a successful attack at each point

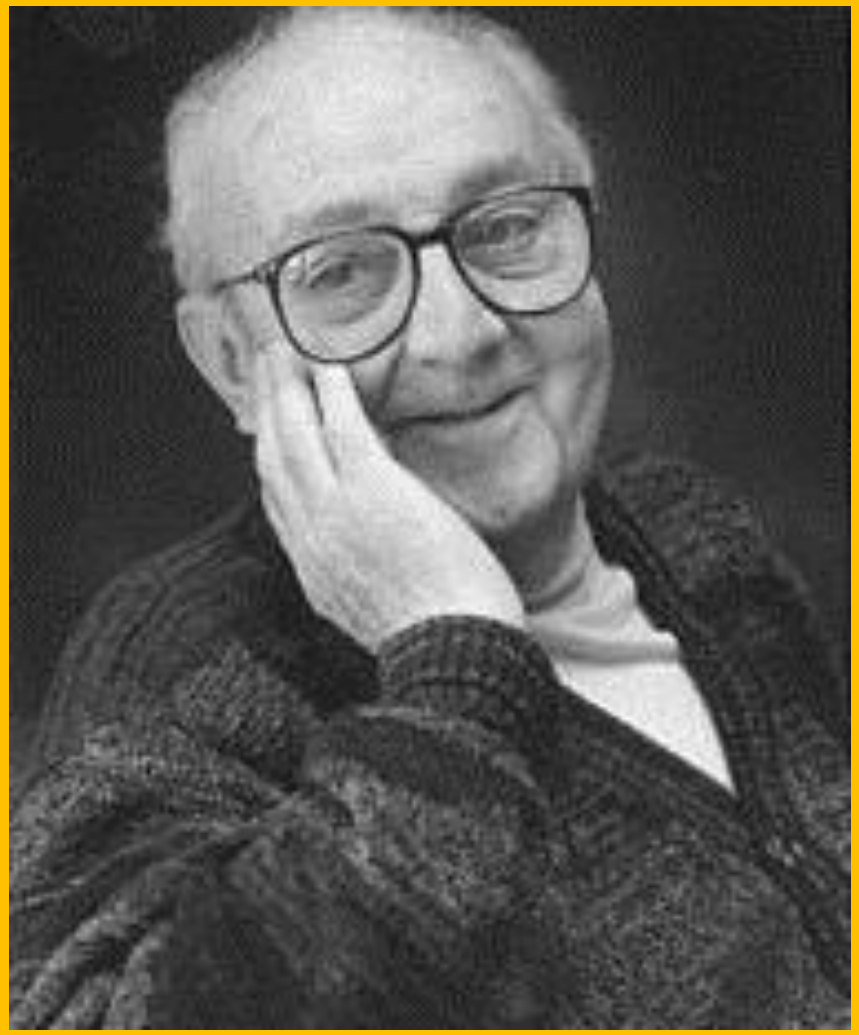
Validating Emerging Risk Models

Emerging risk models may include assumptions derived with little to no prior historical information.

So how can we determine whether they're right?

“All models are wrong, but some are useful”

- George Box (1978)



Validating Emerging Risk Models

- Some aspects of the model forecasts can be compared to known results
  - Goodness-of-fit metrics
  - Retrospective scenario back-testing
- Other projected elements can be compared to external assessments or benchmarks for direction and level
- There are other aspects for which there is no representative history. Traditional rigorous validation techniques cannot be applies in these cases.
  - A systematic approach can still be taken to quantify model risk

Validating Emerging Risk Models

- Test the model for sensitivity to changes in parameters
  - How much do results change given fixed movements in key parameters?
  - Do these movements represent a realistic range of possibilities for key parameter values?
  - Are there meaningful bounds on any parameters? Can we assert that the result is “at least X” or “at most Y”?

Validating Emerging Risk Models

- Are benchmark values available for any model components. For example, do econometric forecasts diverge materially from those of government economists?
- Are alternative models available as benchmarks?
- Know the model's limitations, and keep them in mind when applying the model results to business problems.
  - We can still create useful models, even if some aspects are fundamentally "unknowable".

Questions