A Practical Framework for Assessing Emerging Risks

John Bowman, MBCI
Enterprise Business Continuity Management

My objectives for this session…

- Share one approach to assess the current level of business continuity risk in your organization.
- Consider the factors (“drivers”) that will change the level of risk.
- Consider how the drivers affect the rate of change to risk over time.

Real life: This is the approach being used by my department.

Desired outcomes…

- Learn a process to identify and rate the relative impacts of risks to your organization, and show how and why they are expected to change over time.
- The outcomes of the process are:
  - Identification of factors that most influence increased risk (that is, emerging risk), and
  - A commonly understood process for identifying and rating risk.
- The results of the assessment are:
  - Easy to display on a heat map and support with (brief) rationale;
  - Scalable – equally useful from a business unit level to a global level; and
  - Transferrable - the same method could also be used for other risk types.

Why bother?

“Why bother?”

“‘You’ll know you’re doing risk assessment right when leaders at every level use the information to make decisions regarding value.’

“How can you ensure that your BCM programme and resources are allocated in a way proportionate to the current and potential threats that the company is and will be facing?”
Lee Glendon, BCI: Big picture – long picture: the value of horizon scanning
We provide the structure by following a risk assessment process... *a little “BCM 101”*

- Identify risks.
- Develop assessment criteria.
- Assess risks.
- Assess risk interactions, including “drivers”, and
- Prioritize risks ... which then enables us to

  - Respond to risks...
  - and then Repeat, so we can consider what’s changed / changing.

In the first step – “Identify Risks” – we want to cast a broad net...

**Goal** = develop a long list of potential hazards / threats.

- Natural
- Technological
- Human

Many sources exist to help get started.

For example, here’s a (short) starting list...

<table>
<thead>
<tr>
<th>Human</th>
<th>Technological</th>
<th>Natural</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical attacks (e.g., bomb, chemical, biological, radiological)</td>
<td>Hazardous material spill or release</td>
<td>Earthquake</td>
</tr>
<tr>
<td>Cyber attack</td>
<td>Explosion / fire</td>
<td>Tsunami</td>
</tr>
<tr>
<td>Sabotage</td>
<td>Transportation disruption</td>
<td>Volcano</td>
</tr>
<tr>
<td>Intoxication</td>
<td>Energy / power failure</td>
<td>Landslide, mudslide, subsidence</td>
</tr>
<tr>
<td>Deformation</td>
<td>Fuel / resource shortage</td>
<td>Glacier, iceberg</td>
</tr>
<tr>
<td>Criminal activity (e.g., vandalism, arson, theft, fraud, data theft)</td>
<td>Air / water pollution, contamination</td>
<td>Food, flash flood, tidal surge</td>
</tr>
<tr>
<td>Physical or information security breach</td>
<td>Water control structure / dam / levee failure</td>
<td>Drought</td>
</tr>
<tr>
<td>Civil disturbance, public unrest, riot</td>
<td>Water supply failure</td>
<td>Fire (e.g., forest, urban, wild fire)</td>
</tr>
<tr>
<td>Internal strike or labour dispute</td>
<td>Communication system interruption</td>
<td>Snow, ice, hail, snow avalanche</td>
</tr>
<tr>
<td>External (supplier) strike or labour dispute</td>
<td>Other Critical Infrastructure Failure (e.g., food, food safety, public safety &amp; government services, health services)</td>
<td>Windstorm, tropical cyclone, hurricane, tornado, water spout, dust / sand storm</td>
</tr>
<tr>
<td>Information Systems / IT Failure</td>
<td>Extremes: temperatures</td>
<td>Disease epidemic / pandemic</td>
</tr>
<tr>
<td>Supplier failure / supply shortage</td>
<td>Lightning strikes</td>
<td>Animal / insect infestation or damage</td>
</tr>
<tr>
<td>Electromagnetic pulse</td>
<td>Geomagnetic storm</td>
<td></td>
</tr>
</tbody>
</table>

Next, develop the base assessment criteria – that is, to assess your current state...

- Are you assessing inherent risk, residual risk, or both?
- Probability / Likelihood
- Impact

If assessing residual risk, what are the mitigants (actions taken to reduce either likelihood or impact)?
Several often overlooked factors affect the scope and quality of your risk assessment...

- **Range of threats considered** – What is responsibility of BCM department vs. other departments?

- **Geographic scope** – company wide? Site specific? Business line?

- **Time horizon** – how far into the future? Link to company’s strategic planning timeframe?

---

Key question: *Who will use the information to make what decisions?*

---

The risk assessment is useful because it helps us take action...

- Prioritize risks.
- Develop response plans.
- Develop and implement additional mitigation plans.

However, we also want to consider how the threats will change over time, and what new risks might emerge.

---

After conducting the risk assessment, the results might look something like this...

<table>
<thead>
<tr>
<th>HAZARD</th>
<th>VULNERABILITY</th>
<th>IMPACT</th>
<th>MITIGATION</th>
<th>RELATIVE RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health-related chemical, biological, radiological</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Cultural</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Cyber⋅⋅⋅</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Electromagnetic pulse</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Earthquake</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

There are many models available. This one was first adapted for use by Indian Health Service from a tool designed by Kaiser-Permanente and has been further adapted by my department.

---

We need to identify and understand the “drivers”, and consider how they interact...

That is, what are the factors that will influence:

- Likelihood.
- Severity.
- Velocity (speed of change).
FEMA’s Strategic Foresight Initiative identified five dimensions that have significant influence in the world...

Looking at each in turn, consider how these drivers will affect the risks to and opportunities for your organization...

Social and Technological drivers...
- Demographics:
  - Aging population;
  - Concentration – changes in where people are located.
- Technological innovation and dependency:
  - Exposure to cyber threat;
  - No viable manual workarounds;
  - Access / opportunity for distributed work.
- Universal access to and use of information.

Environmental Drivers...
- Climate and weather change
  - Frequency and intensity of extreme weather events.

An example of interdependencies...How will climate change affect demographics: concentration; where people live?
Economic and Political Drivers...

- Global Interdependencies / Globalization
  - Supply chain / outsourcing;
  - Off-shoring.
- Evolving Terrorist Threat
  - Cyber and physical threat;
  - Civil disturbance.
- Budgets
- Critical Infrastructure – reliance on:
  - Transportation;
  - Communication;
  - Energy;
  - Other?

Factoring these drivers into your assessment expands its usefulness...

- Add a measure of “Velocity” – speed of change.
- Re-assess the “long” list of hazards to **identify emerging risks**.

Requires that you “reframe” your thinking from “what is” to “what is likely”

So now your assessment changes, and starts to look like this...

<table>
<thead>
<tr>
<th>ID</th>
<th>HAZARD</th>
<th>LIKELIHOOD</th>
<th>IMPACT</th>
<th>VULNERABILITY</th>
<th>SPEED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physical attacks</td>
<td>3</td>
<td>11</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Cyber attack</td>
<td>3</td>
<td>10</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Civil disturbances, public unrest, riot</td>
<td>3</td>
<td>7</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Strike of labour disputes (Internal)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>Electromagnetic pulse</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>Earthquakes</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>n</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

And the results can be displayed in an easy to understand, impactful heat map...

![Heat Map Diagram]
Another option is a MARCI chart (Mitigate, Assure, Redeploy, and Cumulative Impact) plotting impact and vulnerability.

To recap...

- Identify risks.
- Develop assessment criteria.
- Narrow the list.
- Define the scope.
- Expand list of potential hazards.
- Plan.
- Respond.
- Assess the risks.
- Likelihood, impacts.
- Measure of Cumulative Impact.
- Prioritize risks.
- Communicate.
- Heat map.
- MARCI
- Identify and assess the drivers.
- Identify emerging risks.

For more information, here’s a starting reading list...


Thank you.