Risk

Risk is knowable and quantifiable

Mike Dunn
Managing Director

My presentation today posits that:

- Risk does not need to be complicated.
- Effective risk management requires you to widen your perspective.
- The elements of the risk formula are profound but easy to understand when you have the key.
- Good risk management requires good scenario development.
- The consequence of getting consequence wrong is considerable.

Example 1: Canberra Bushfires - 2003

- Burnt into Canberra.
- Killed four people.
- Seriously injured hundreds.
- Destroyed or seriously damaged 400 homes.
- Cost millions of dollars.
- Unfortunately the holes in the cheese lined up:
  - Weather, temperature, dry vegetation, lack of undergrowth burn off and certainty it couldn't happen.

Volunteer Fire Brigade Captain's evidence…
"it is disturbing that a lightning strike on 8th January can develop into such a destructive blaze and destroy so much over a **week** later when you consider the knowledge and resources available for its control."

Example 2: Icelandic Volcanic Eruption: in 2010

Closed European airspace for almost a week and cost airlines operating in Europe hundreds of millions of dollars

- Did British Airways (BA) consider the possibility of UK airspace closure for a week.
- Yes? Why then didn't BA have strategic plans to locate part of its fleet in southern Europe and agreements with train and ferry operators to shift passengers between that location and London?
- Consider the Board of BA as the CEO reportedly advised them, they had no effective response to the closure of airspace except to attempt compensation from the UK Government.

Example 3: BP's Deepwater Horizon oil leak and explosion in the Gulf of Mexico - 2010

- Why didn't BP (the well owner) have tested plans and procedures to quickly cap the exposed well.
- BP has great risk management expertise.
- BP scrambled to develop any response to the unregulated flow of oil in the Gulf of Mexico that was negatively impacting their reputation and potentially costing billions of dollars to remedy.
- Press reports indicate that the dome built to try to cap the oil well had not been tested by BP at the required depth before.

BP has spent $71 billion on environmental clean-up, compensation, and defending its reputation.
It almost broke the company.

Example 4: JW Marriott Terrorist Attack - 2009

- Good risk management practices by staff.
- Knowledge of previous attack.
- New security measures and processes were implemented after the 2003 attack.
- Did the hotel's security preparedness after the first attack become vulnerable over the years.
- Did the hotel fail to conceptualise the type of scenario that eventuated in 2009

The JW Marriott Hotel in Jakarta was first attacked by terrorists using a vehicle bomb in 2003.
It was attacked for a second time in 2009 by a terrorist using a body bomb that was assembled in the hotel with insider support.

Possible control measures

- Searches for harmful substances including explosives are conducted on all people (including staff and vendors) entering the hotel.
- Searches of all vehicles entering the hotel precinct are conducted by professional security personnel.
- Searches for weapons are conducted on all people (including staff and vendors) entering the hotel.
- Training for staff includes identifying suspicious activity associated with planning and/or executing a terrorist act.
- Examination for harmful substances including explosives are conducted on all deliveries including mail to the hotel.
- Searches for harmful substances including explosives are conducted on all luggage brought into the hotel.
- Searches of all vehicles entering the hotel drop-off and car parks are conducted by professional security personnel.
- Enquiries are made by hotel security staff when a guest is not heard from or seen by hotel staff at least twice per day.
- Random searches for harmful substances including explosive matter are conducted daily by bomb detection teams with trained canines and explosives detection equipment.
- Security investigates all instances where a guest checks in without official ID or produces suspicious ID.
- Security investigates all instances where a guest unreasonably denies access by cleaners, room maintenance or other hotel staff to their room.
- Counter terrorist bodies monitor the sales of materials that could be used to manufacture improvised explosive devices in the country where the hotel is located.
- Counter terrorist bodies and law enforcement agencies are very effective in the country where the hotel is located.

Failure to conceptualise the risks and therefore a failure to identify a suitable response

- Firstly, foster a wide-ranging and uninhibited scenario generation regime.
- Secondly, import the scenarios into a simple risk assessment tool that supports the processing of the scenarios to identify changes in likelihood and risk.
- Thirdly, spend the money and effort to confirm you have a proven risk mitigation response to the risk.

How to foster a wide-ranging and uninhibited scenario generation regime

- Requires an organisation to engage its personnel in the study of its environment.
- Training on how to undertake scenario generation.
- Encouragement to think ‘outside the box’.
- Maintain your situational awareness.
- Remuneration for relevant scenario generation.
- Scenarios should identify signals, indicators, or events that indicate an organisation is entering or about to enter a period of change that signals either opportunity or threat.
- The organisation must have the flexibility to quickly add new scenarios for collective consideration with existing scenarios before the event is experienced (or in the least desirable outcome) as an event unfolds.
- The organisation should provide for simple and easily digested reports that can be communicated, preferably immediately via a medium like the Internet, to anyone responsible to input the scenario into the risk tool or to implement the risk mitigation response.

The Risk Formula

- You guys confront risks in your boarding houses daily.
- The risk models deployed by your boarding houses will differ in detail, complexity, style and technology.
- The formula is usually Likelihood x Consequence = Risk.
- Some organisations undertake vulnerability assessments.
- The Australian Standard AS ISO 31000:2018 Risk Management Guidelines provides great information for anyone wanting to understand and implement good risk management.
- You want to get in front of risk.
- Retrofit of risk management is difficult and expensive.
- Once you begin risk assessment your only action can be to continue to the end.

Inanimate risk formula

- Risk you think about every day in your boarding house.
- The great majority of risks will be these types of risks.
- No intent to target you, your people or your facility.

Animate

- Risk you think about infrequently in your boarding house.
- You will confront this type of risk occasionally.
- Active intent to target you, your people or your facility.
- Decompiling likelihood into any sub-elements is difficult so why do it?
- It's worth doing because the quality of risk analysis being provided to organisations in the guise of likelihood assessment is often poor.
- A probability number on its own is often opaque to a non-risk trained business manager and appears to make as little sense to many risk consultants.
- how do we improve the product, educate risk consultants, and provide a value likelihood service to our clients? We start by identifying the sub-elements of likelihood.
- There could be any number but let's concentrate here on three sub-elements: intent; capability; and vulnerability.

Likelihood sub-elements: intent

- Intent to undertake a risk scenario is hard to discern.
- It's easy if the scenario has been conducted against you before or if an organisation has threatened to undertake the scenario against you.
- Given the JW Marriott attacks, the hotel's risk team would be imprudent not to identify a high level of intent for terrorist organisations to attack the hotel in the future.
- You must undertake systematic collection and analysis of information to identify actual intent.
- If your analysis can't confirm actual intent, you should not assume an elevated level of intent.
- Be honest and say intent is unknown.
- When analysing intent, don't assume your actions can reduce intent.

Likelihood sub-elements: capability

- Capability is more easily identified and assessed.
- It will usually revolve around modus operandi, relationships, personnel, training, finance, and experience.
- Find these threads and you will tell a compelling capability story.
- Capability to implement a risk scenario against you can be undermined by addressing any vulnerabilities that your organisation exhibits.

Likelihood sub-elements: vulnerability

- Vulnerability relates to our exposure to the risk scenario.
- If we have correctly identified the scenario and then assessed the capability of the threat source to carry out the scenario, we can easily review our current defence measures and then identify any additional mitigation we might require.

Opportunity

- We think of a positive risk as an opportunity.
- How likely is it to occur and what will be the benefit if it does occur.
- It will often revolve around timing. Pertinent examples might be:
  - Should we expand our boarding house now?
  - Should we increase our staffing levels now?
  - Should we consider amalgamating with boarding house X?

The consequence of getting consequence wrong (slide 1)

- A confession: I once thought consequence was the easy part of risk but the four risk examples today (and much of my career) have taught me differently.
- You must work hard with a client to assess likelihood.
- But the client usually has a basic understanding of consequence that can be informed by your knowledge and experiences to obtain a very good result.
- If a client organisation doesn't have a formal grasp of consequence definitions, you can work with their understanding of their business to develop them.
- What's easy about consequence is developing the consequence definitions.
- And you cannot mitigate a risk if you haven’t considered the risk scenario.

The consequence of getting consequence wrong (slide 2)

- What’s hard is mitigating the consequence of a risk event – particularly a strategic risk event that could threaten your organisation's existence.
- We practitioners always say mitigating consequence is expensive – and it’s true.
- But getting a client to agree firstly, on the potential consequences of a strategic risk event like the oil spill, and secondly, on the requirement to spend large amounts of money on identifying workable mitigation, isn't always easy.
- But think of the changed circumstances that BP would be facing in the world today if it had identified this risk scenario when conducting its risk workshops in 2004, spent the necessary funds to test and identify a viable solution, and had that solution ready to implement when the rig exploded and finally the blow out preventer failed to cap the well.
- Hopefully, none of you will face disasters like this one. But even operations on a lesser scale should look again at their risk processes and review their consequence actions because the consequences of getting consequence wrong are increasing all the time.

Strategic Risk

- All risk is a challenge but biggest challenge posed to any organisation is strategic risk.
- You will not understand the components of strategic risk if you don’t understand the range of scenarios that will eventually confront your organisation.
- By integrating your risk process into complicated business practices, you potentially lose the perspective on what really counts in strategic risk management: informed early warning; easily understood risk processes; and well understood and effective risk mitigation.

Questions please?

Contact details

- Email: mike.dunn@iog.com.au
- Mobile: 0418468364
- Web site: www.iog.com.au