



Trust Management: Business Impact - A Common Language

Problem

Back in the time when businesses were predominantly “local” and to a large extent insulated from each others operations, it really didn’t matter very much how we defined the Business Impact of Information Risks, for we knew what we meant in each business and we didn’t have much need to share that meaning with others. Collaboration and the business need for it back then was not a significant imperative for most businesses in a global or even national context, and certainly was not a requirement at the frequency and set-up speed that collaborations are demanded today.

Today, parties in a collaboration need more clarity over the controls that apply in their relationship. With the increased importance of collaboration, it is becoming more important to be able to share the implications of a risk in terms of the potential business impact. We need to do so in a manner that is universally understood. This paper recognises that there is no such commonly agreed scale available to communicate with sufficient granularity the impact of information risk on businesses.

Why should I care

Without a commonly agreed communications tool, enterprises will not be in a position to effectively share with their partners the implications of a particular information risk. With such a tool, it becomes possible to communicate in a manner that allows the collaborative management of information risks. Also it is not straightforward to automate the processes for managing risk if the impact is not commonly understood.

Recommendation/response

We need to promote development of a standard Business Impact Scale that would be associated with Information of different sensitivity, appropriate information controls, and trust levels.

Proposed set of terms and definitions for Business Impact Levels

This proposal defines six business impact levels, with the first unlikely to be used in a business context. It is assumed that there is no need to define “No Impact”.

- | | |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Disastrous | Significant loss of life, Collapse of multiple enterprises or a countries economy, significant global environmental incident |
| Catastrophic | Loss of multiple lives, Significant financial loss, Collapse of an enterprise, Significant countrywide environmental incident. |
| Material | Accidental loss of life, Financial loss of reportable sums of money, Significant brand impact, Significant local environmental incident. |

Major	Significant Injury, Significant financial loss, Brand impact, Local environmental incident
Minor	Injury, Financial loss, Local Brand Impact, Minor environmental incident
Insignificant	Negligible injury, Slight financial loss, Negligible environmental impact

These levels are directly equivalent to the UK Government's Business Impact Table: http://www.cesg.gov.uk/policy_technologies/policy/media/business_impact_tables.pdf. Other relevant references are available from the OECD, and from national standards organisations in many countries.

Background/rationale

Being able to quantify the impact in a qualitative frame enables understanding of impact and allows for dialogue and negotiation.

The four impact domains considered in this paper are:

- impact on human life
- financial impact
- brand impact
- environmental impact

Naturally, impact levels will vary greatly between different enterprises, based on their nature, their size, etc.

Examples of risk tools developed in the past to communicate the potential size of specific risks in nature include:

- Admiral Beaufort developed his Beaufort wind scale in 1805, allowing sailors to identify and communicate in a commonly understood manner the threat from wind force.
- Charles Richter and Beno Gutenberg developed a scale in 1935 (the Richter scale) to report Earthquake magnitudes (The levels for which were: Micro, Minor, Often, Light, Moderate, Strong, Major, Great, Devastating, Epic)

One important difference to understand with a Business Impact Scale is that it is not measuring the size of the risk event; a given information risk would NOT necessarily have the same business impact on each party in a collaboration. However the ability to be able to share in commonly understood terms the business impact that a given risk might have on both parties, allows for appropriate negotiation between those parties over the risk controls or mitigations that should be employed.

Similarly, it is also important to note that the financial implications of an event will not always be the same for each party. The impact of losing \$10,000 in a very small start-up will feel very different to the impact felt by a large corporate organisation losing the same amount. The important thing to consider is that the terms in a Business Impact Scale convey the true implications of a risk event for each party.

Conclusion

Recognition of the need for a Business Impact Scale of the nature described in this paper is a key first step. Those who do so can then work together to create and encourage global adoption of an Open Standard that will allow common understanding on business impact levels.

At this stage, we envisage that key attributes of a successful Business Impact Scale standard include:

- Sufficient Granularity (Some scales used today have just use 3 levels)
- Clear Understandable Definitions of Business Impact

A Business Impact standard is not of course a substitute for performing effective risk assessment/analysis evaluations¹ to enable business managers to understand what impacts their existing exposure to risk could have on their business operations, so they can take informed decisions on how best to manage (accept, mitigate) their exposure.

¹ See COA Process paper on Risk Management – available from www.jerichoforum.org/publications