6 Impact Assessment

An isolated vulnerability and an isolated threat are not enough to cause harm or damage to CI/CII. Rather, the convergence of a threat with a specific vulnerability, combined with the possibility of a *harmful impact*, produces the risk. Such impacts are disruptive challenges of different types, durations, and levels of severity, and can be measured using different parameters such as economic loss or social and political damage. The term "impact" is also used interchangeably with the terms "harm", "effect", or "consequence".

What is Impact Assessment?

Impact assessment is one step in the overall risk analysis process. Its aim is to determine the impact resulting from a successful threat exercise of a vulnerability. The grade of possible harm to an asset must be determined by a number of experts familiar with the assets, be they executives (such as experts within the administration), asset owners, or asset managers.

The adverse impact of a security event on IT-systems can be described in terms of loss or degradation of any, or several, of the →*IT-Security Objectives:* integrity, availability, and confidentiality. Other categories might be applied if risk analysis is conducted for more abstract systems: Some tangible impacts can be expressed quantitatively as lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, or damage to an organization's interest) cannot be measured in specific units. But they can at least be described qualitatively (e.g., using the impact categories "high", "medium", and "low").[103] However, in interdependent systems, assessing the impact of the loss of a critical asset becomes fairly complex.

103 Stoneburner, Gary, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800–30 (Washington, January 2002). http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, p. 22.

There are several quantitative and/or qualitative assessment approaches to impact assessment, which have both specific advantages and disadvantages:

- Quantitative Impact Assessment:
  - The major advantage of a quantitative impact analysis is that it provides a measurement of the impact's magnitude, which can be used in the cost-benefit analysis of recommended controls.
  - The disadvantage is that, depending on the numerical ranges used to express the measurement, the outcome of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Hence, additional factors must often be taken into account to determine the magnitude of impact.
- Qualitative Impact Assessment:
  - The main *advantage* of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
  - The *disadvantage* of the qualitative analysis is that because the magnitude of impacts cannot be measured in quantitative terms, a cost-benefit analysis of any recommended controls is not feasible.[104]

104 Ibid., p. 23.

Examples of Impact Assessment

Below, the following two examples are described:

- Example 1 (Canada) – OCIPEP Model for Impact Assessment (OCIPEP)
- Example 2 (United Kingdom) – NISCC Impact Model (NISCC)

Example 1 (Canada) – OCIPEP Model for Impact Assessment (OCIPEP)

The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) is developing a guideline aimed at assisting CI owners and operators in developing criteria for critical →*Assets* and to establish their relative criticality. CI owners and operators are asked to identify critical assets in infrastructures and assess the potential effects of loss of the asset.

The Canadian model for impact assessment distinguishes six impact categories (service delivery, public, economic, political, environmental, interdependency). The impact of the loss or disruption of the asset is assessed by the use of three impact factors: scope, magnitude, and effects of time:

- Scope: The loss of an asset is rated by the extent of the geographic area affected (impacted), usually "local", "provincial/territorial", or "national".
- Magnitude: The degree of the impact or loss is assessed in the context of the impact category using the →*Categories* "none", "minimal", "moderate", and "mjor".
- Effects of Time: The passage of time may have an affect on the loss of an asset's magnitude and scope of impact.

The following table (Table 6) is used to depict the information collected for a specific asset (e.g., a server) in a specific sector (e.g., telecommunications) for easier analysis.

Example 2 (United Kingdom) – NISCC Impact Model (NISCC)

The UK's *National Infrastructure Security Coordination Centre* (NISCC) is currently developing a procedure for impact analysis that will allow NISCC to compare disruptive challenges of different types, durations, and severities, by using a single model. This allows for the assessment of the significance or criticality of a single IT system, critical service, or attack scenario, using a common 'currency'. It is designed to produce a standard scale, or profile over time, of the impact of any 'disruptive challenge' to a country. The scale has three axes: area of impact, severity of impact, and time.

Asset Name:	**Impact Factors**		
Sector:			
Impact Categories	**Magnitude**	**Scope**	**Effects of Time**
Service Delivery			
What will be the impact of the loss of this element/asset on the delivery or level of the particular service/product within the respective sector?			
Public			
Could the loss of this asset result in death, serious injury, or displacement of people?			
Could the loss of this asset result in low morale, panic, rioting, or civil disorder?			
Economic			
What economic impact would arise from the loss or degraded services of the asset?			
Political			
What impact could the loss of this asset have on public confidence, either directly or through related service degradation or loss?			
Will the loss of this asset significantly reduce the ability of government to deliver basic government services in the areas of public health, safety, and economic security, or to provide essential services?			
Environmental			
What would be the environmental impact of the loss or degradation of service of this asset/element?			
What would be affected by the loss or degradation of service of this asset/element (insert all that apply in the Scope box)?			
Interdependency			
Are assets/elements within the sector dependent upon this asset?			
Are assets/elements outside the sector dependent upon this asset?			

Table 6: Canadian Impact Analysis Table

- Area of Impact: The four areas of impact for the model are derived from the definition of the UK critical infrastructures:[105]
  - Loss of life,
  - Economic consequences,
  - Social consequences,
  - Political consequences.
- Severity of Impact: Severity is measured on a →*Logarithmic Scale* up to a maximum of 10. For each of the four areas there is a logical ceiling – corresponding to a score of 8 or 10, depending on the area. The impact scales in the four areas are designed to be of approximately equivalent severity. The ceilings for each of the four impact areas are shown in Table 7.

Impact Area	Scale Max	Impact Severity
Loss of Life	10	Death of 10% to 100% of population of country
Economic	8	Loss of between 10% and 100% of annual GDP
Social	8	Complete collapse of society; anarchy and chaos
Political	8	Total failure of political machine

Table 7: Ceilings for each of the four Impact Areas

The logarithmic scale allows for much greater granularity at the lower end of the axis: for example, for 'economy', the full scale for the UK, with a population of about 60 million and a GDP of £1 trillion, runs as shown in Table 8. Gradations in the scale for social and political impacts can also be set out. Social and political scales will be more subjective, using examples rather than number ranges.

105 "Those parts of the United Kingdom's infrastructure for which continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening serious economic or other grave social consequences for the community, or any substantial portion of the community, or would otherwise be of immediate concern to the Government." Barry, Ted. "Critical Information Infrastructure Protection in the United Kingdom". Paper presented at the Critical Infrastructure Protection (CIP) Workshop (Frankfurt, 29–30 September 2003). →See Part I for more detail.

Scale	Economic range	
	from…	to…
10	greater than total UK GDP	
9		
8	£100’000’000’000	£1’000’000’000’000
7	£10’000’000’000	£100’000’000’000
6	£1’000’000’000	£10’000’000’000
5	£100’000’000	£1’000’000’000
4	£10’000’000	£100’000’000
3	£1’000’000	£10’000’000
2	£100’000	£1’000’000
1	£10’000	£100’000

Table 8: Scale for Economic Range

- Time: The duration of a disruptive impact is measured by again using a logarithmic scale. For some events (such as electronic attacks), occurrence, detection, and remedial action may all take place within a matter of days. Others will have a much longer time-frame: for example, the impact of global warming will be felt over decades and centuries.

An event or scenario can be represented in a three-dimensional graph. The example shows a terrorist attack, which may cause short-term loss of life, longer-term economic damage, and medium-term social and political consequences (Figure 31):

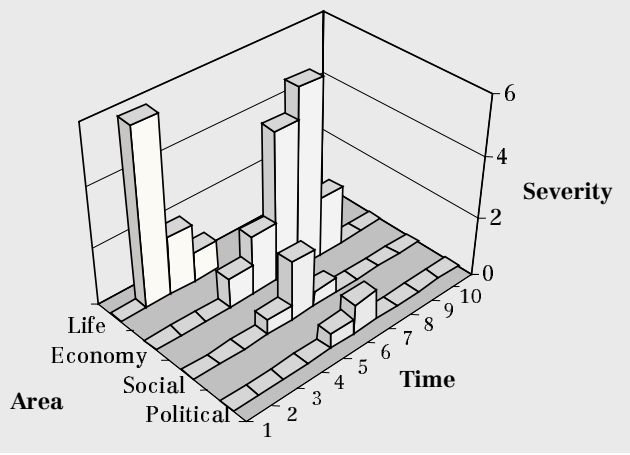

Figure 31: UK Impact Three-Dimensional Graph