4.6.5 ZCR 5.4: Determine unmitigated likelihood

4.6.5.1 Requirement

Each threat shall be evaluated to determine the unmitigated likelihood. This is the likelihood that the threat will materialize.

4.6.5.2 Rationale and supplemental guidance

In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as, a probability or a frequency over a given time period). A common method of estimating likelihood is to use a semi-quantitative likelihood scale that is defined by the organization as part of their risk management system (refer to Annex B for examples). Either qualitative or quantitative methods are allowed by this document.

A number of factors are considered when estimating unmitigated likelihood such as the motivation and capability of the threat source, the history of similar threats, known vulnerabilities, the attractiveness of the target, etc.

Existing cyber security countermeasures for the zone or conduit being evaluated should not be considered when determining unmitigated likelihood; they should be hypothetically eliminated. However, the likelihood determination recognizes countermeasures that are inherent to IACS components and any non-cyber independent protection layers (IPLs) such as physical security, mechanical safeguards (such as, pressure safety valves) or emergency procedures that are in place to reduce the likelihood.

Likelihood is evaluated twice during the detailed risk assessment process. It is initially determined without consideration for any existing countermeasures in order to establish the unmitigated risk. It will be re-evaluated in 4.6.10, taking into account existing countermeasures and their effectiveness in order to determine residual risk.

Consequence-only risk assessment methodologies may be used to meet the requirements of this document. These methodologies typically do not factor likelihood into the determination of unmitigated cyber risk and implicitly assume that likelihood is constant (such as, assuming the likelihood is ever present or quantitatively a ‘1’).

4.6.6 ZCR 5.5: Determine unmitigated cyber security risk

4.6.6.1 Requirement

The unmitigated cyber security risk for each threat shall be determined by combining the impact measure determined in 4.6.4, and the unmitigated likelihood measure determined in 4.6.5.

4.6.6.2 Rationale and supplemental guidance

Determination of unmitigated cyber security risk is often accomplished using a risk matrix that establishes the relationship between likelihood, impact and risk, such as a corporate risk matrix (refer to Annex B for examples).

4.6.7 ZCR 5.6: Determine SL-T

4.6.7.1 Requirement

A SL-T shall be established for each security zone or conduit.