IDA | Research Insights

August 2016

# Terminate, Tolerate, Transfer, or Treat*

Laura Odell, Institute for Defense Analyses (lodell@ida.org)

A cyber vulnerabilities risk management approach should offer decision makers several choices for responding when assets are assessed as vulnerable to or experiencing cyber exploitation. Rather than simply accepting risk or investing in a mitigation action, decision makers need a framework to help them manage the dynamic, accelerating pace of cyber intrusion incidents. A framework based on the choices of Terminate, Tolerate, Transfer, and Treat affords a deeper understanding of what could be gained or lost. These choices present opportunities and consequences. The framework applies equally well to early investments and fully operational systems. Specific considerations for fully operational systems include the following.

**Terminate – Opportunities and Consequences:**

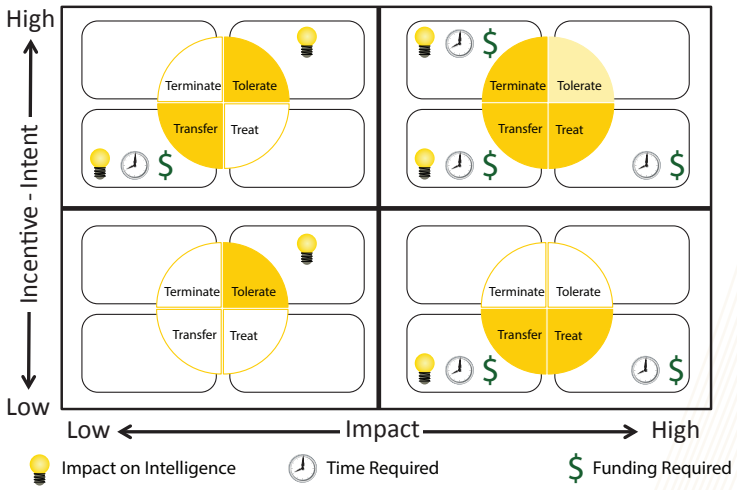
- Terminating a capability/technology may notify the adversary that he is discovered.
- There is no longer an opportunity to observe adversary targets and techniques.
- Although the incident is no longer a degradation to the system or environment, the capability/ technology is lost and may have to be replaced if there are no substitutes.

**Tolerate – Opportunities and Consequences:**

- Avoids investment in lesser priorities deemed low impact.
- Allows time to develop a more informed understanding of the adversary and defend against future attacks afforded by the opportunity to observe.
- However, observation takes time and resources.
- Degradation of current capability continues.

**Transfer – Opportunities and Consequences:**

- Requires a surgical knowledge of what alternatives are technically available and what is feasible.
- Funding and other resources may be required.
- May need cooperation and collaboration from stakeholders (sometimes difficult to coordinate) outside an organization or country.
- Time is needed for correction, socialization, and application of solution.
- May afford an opportunity to promote a solution from a singular platform to an enterprise-level application.




Source: Institute for Defense Analyses, 2015.

**Treat – Opportunities and Consequences:**

- Time and funding are required to treat and mitigate a risk.
- Know-how or knowledge is required that may not be contained in the original solution.
- There may be an opportunity to manipulate or create a false provenance or misinform the adversary (i.e., in cases of exfiltration).
- New opportunity to build in defensive design.

A decision to terminate, tolerate, transfer, or treat risk must include at a minimum: (1) what is known about (intelligence) the adversaries' current capabilities, (2) the incentive of the adversary to use those capabilities against a target of importance, and (3) an assessment of the impact level of the asset (priority to the organization).

NS D-8114

* Based on IDA NS D-8094, *Data to Decisions—Terminate, Tolerate, Transfer, or Treat*, July 2016.

Research sponsored by the Office of the Secretary of Defense, Chief Information Officer.


4850 Mark Center Drive
Alexandria, VA 22311-1882
www.ida.org