IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

Multi-Asset and System Assessment

BACKGROUND

The Multi-Asset and System Assessment (MASA) is a voluntary assessment process applicable to infrastructure systems, large campuses, and clusters of infrastructure. The MASA process collects data at the enterprise and asset levels and provides infrastructure owners and operators with the following: a ranked list of assets based on their relative criticality, an overview of applicable attack types by asset, and security vulnerabilities and options for consideration. The final product is an integrated resource that includes geospatial information, interactive dashboards on security and dependencies factors, and a written report.

PROGRAM DESCRIPTION

CISA conducts a MASA in collaboration with the infrastructure owner. The Protective Security Advisor (PSA) leads the coordination and data collection in the field and involves regional partners, such as fellow PSAs and regional analysts, as needed to complete all phases of the MASA. The criticality phase of the assessment is conducted through a series of webinars or onsite meetings and generates an asset ranking. The ranking assists in the determination of which assets warrant an onsite security site visit. Typical owner involvement includes the equivalent of 3-8 days often dispersed over a period of a couple months, but this commitment is flexible based on the needs of the organization and availability of personnel required for the assessment.

MASA PROCESS

TABLE 1: MASA PHASES

PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5
▪ Approval and Preparation ▪ Schedule and Pre-assessment ▪ Preliminary Asset Identification ▪ Background Research Materials	▪ Enterprise-level Assessment ▪ Facilitated Criticality Discussion	▪ Security Site Visits ▪ Identification of Vulnerabilities	▪ Development of Options for Consideration ▪ Draft Report	▪ Final Products Development and Delivery

In most cases, engagement with the following enterprise personnel (or similar titles) is required:

- Facilities manager or engineering
- Chief information officer or representative from information technology
- Security manager, may include onsite law enforcement
- Human resources
- Business continuity or risk manager

Asset Criticality

The asset criticality index characterizes the criticality of each asset by considering five categories of impacts and two additional factors that affect, or modify, those impacts.

FIGURE 1.–Sample Asset Criticality Ranking Graph.

Impacts

- Operational
- Service
- Safety
- Economic
- Reputation

Modifiers

- Ease of access
- Symbolic importance

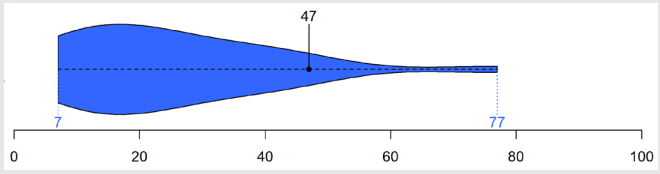


FIGURE 2.–Example Criticality Distribution.

Attack Types

17 Pre-defined Attack Types | **8** Natural Hazards

Attack types are automatically assigned to each asset based on infrastructure type and can be adjusted based on information gathered during the security site visits if needed.

Vulnerability

- Assets are evaluated during an onsite visit, for vulnerability to each applicable attack type
- Options for consideration provide opportunities to mitigate vulnerabilities

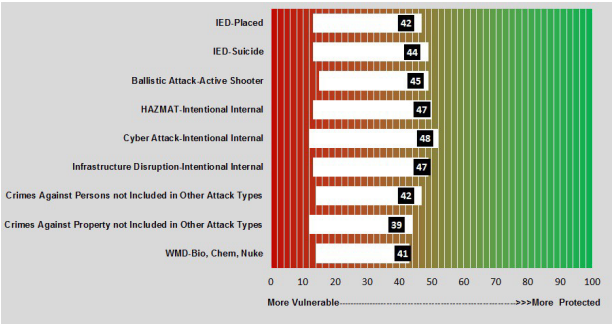
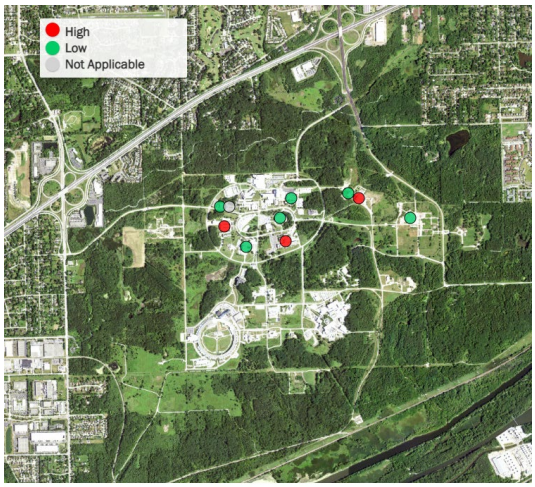


FIGURE 3.–Sample Security Level Indices per Attack Type.

Final Product

Integrated resource containing the following:

- Enterprise- and asset-level data
- Ranked list of assets based on relative criticality
- Vulnerabilities and options for consideration
- Asset susceptibility to different attack types
- Security and dependency dashboards
- Interactive maps



Notional Data - For Example Purposes Only

FIGURE 4.–Active-shooter Threat Susceptibility.

For more information or to submit a MASA proposal, contact Felix Pomponi at felix.pomponi@cisa.dhs.gov.