March
2025

COUNTERINTELLIGENCE: DRIVING DISCUSSIONS ABOUT CRITICAL ASSETS

JOB AID

CDSE Center for Development of Security Excellence

INTRODUCTION

Organizations in Government, industry, and academia are persistently targeted by motivated adversaries seeking to steal, exploit, manipulate, or sabotage sensitive or valuable information, infrastructure, and/or assets. While counterintelligence (CI) professionals are responsible for identifying and mitigating these organizational risks, doing so can be a challenge without a clear understanding of what each organization deems most vital.

HOW DO CRITICAL ASSETS INFORM COUNTERINTELLIGENCE EFFORTS?

Foreign adversaries don't just focus on obtaining classified Government information. Instead, they conduct sophisticated analysis to systematically identify which organizations are most critical to advancing their specific objectives.

Similarly, critical assets are the essential guide for CI professionals to align their mission priorities, allocate often-limited resources, and effectively mitigate the most risk possible.

While some organizations may have already conducted a criticality analysis to determine their critical assets, many have not. For organizations that haven't identified critical assets (or don't see the need), CI professionals champion the need and support stakeholder-led criticality analysis across the enterprise.

A common pitfall for CI professionals is to attempt to identify and prioritize critical assets themselves. Instead, their focus must be to acquire the buy-in and cooperation of stakeholders to make those value determinations. The assets determined critical by stakeholders inform and guide subsequent counterintelligence efforts.

DEFINITION: ***Criticality analysis*** **is a methodology for identifying, assessing, and prioritizing assets based on the impact each would have if negatively affected in some way.**

The following elements are foundational to critical assets and inform related discussions with key asset stakeholders.

WHAT IS A CRITICAL ASSET?

- Not all assets are equally important. A critical asset is one that is essential to – or has the greatest impact on – an organization's mission, operations, and overall success.
- They can be tangible and intangible (proprietary design vs. singular role).
- Specificity is important. Is an entire asset critical or is there a specific component within that makes it critical?
- They can fall into any number of categories, including but not limited to:
  - **Sensitive information/data:** classified information, intellectual property (IP), proprietary research, patents, trade secrets, or sensitive designs
  - **Operational or business information:** supply chain data, project plans, schedules, internal processes, financials, or employee information
  - **Human capital:** key personnel with critical skills or knowledge
  - **Technology or physical infrastructure:** information technology (IT) systems, software, or facilities

WHAT IS CRITICALITY ANALYSIS?

- **Criticality analysis** is a strategic initiative to identify an organization's assets and develop a ranking based on risk of hypothetical loss or compromise.
- Some key risk variables include **likelihood**, **vulnerability**, or **impact/consequence**.

CRITICALITY IS ORGANIZATION DEPENDENT

- Organizations can have very different priorities. For example, any one of the following can be the top factor behind how an organization identifies and prioritizes what is critical:
  - Maintain technological edge.
  - Effect on future revenue.
  - Uphold brand/reputation.
  - Ensure competitive advantage or market differentiation.
  - Sustain national security objectives.

STAKEHOLDER ENGAGEMENT

- Establish a **cross-functional review team**. Expect and ensure a collaborative process with leadership, IT, human resources (HR), legal, and operational teams to understand organization values, mission, and objectives as well as asset values.
- Ensure a standardization while inventorying assets, assigning values, and calculating overall priority rankings.
- Keep momentum by ensuring stakeholders understand the importance of the initiative, both for CI objectives as well as high-level risk management.
- Plan on periodic, iterative efforts to reassess criticality of assets.

A critical asset list strengthens CI efforts. By knowing what matters most to an organization, CI professionals can develop more impactful objectives, better allocate resources, and mitigate more risk.

PRIORITIES

- Without identified critical assets, attention is spread thinly across all assets, where over-protection of low-priority assets diverts attention from true risks, and under-protected critical assets become prime targets.
- With critical assets being identified, CI professionals know where to focus efforts, to include starting on the highest probability/impact risks.

RESOURCE OPTIMIZATION

- Prioritization ensures protection efforts are focused on the "right" assets, whereas resource optimization ensures budget, infrastructure, and personnel deployments match priorities.

EFFECTIVE RISK MANAGEMENT (PROACTIVE & REACTIVE)

- Misaligned risk mitigation strategies lead to a reactive posture with inconsistent protections and ineffective incident response.
- By anticipating risks to critical assets, organizations can:
  - Assess efficacy of existing mitigation mechanisms, if any.
  - Analyze known and emerging risks posed by adversaries, both directly and via insiders.
  - Evaluate exposure levels or historical incidents.
  - Implement proactive mitigations.
  - Conduct targeted, reactive due diligence.
  - Address any deficiencies in risk assessment processes, response procedures, or workflows involving cross-functional support.

ADDITIONAL RESOURCES

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

- Counterintelligence Awareness/Supply Chain Risk Management Toolkit
- Job Aid: Counterintelligence Awareness for Defense Critical Infrastructure
- Asset Identification Guide

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC)

- Protect Your Organization from the Foreign Intelligence Threat
- Protect Your Organization from the Inside Out
- Secure Innovation Scenarios and Mitigations

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

- Identifying Critical Assets for Risk Management

NOTE: If the URLs in this document do not open upon clicking, right-click on the hyperlinked text, copy link location, and paste into a browser. Alternatively, you can open the PDF in a browser.