Crown Jewels Analysis (CJA)
A Mission Criticality Analysis Technique Using Dependency Maps

A Presentation and Demonstration for Boston SPIN

20 February 2018
Jim Watters
Advanced Persistent Threats (APT) use sophisticated capabilities to attack, and maintain a presence in, our mission systems.

As a result, it is not realistic to use a defensive strategy based on stopping all threats at the boundary.

Instead, we must assume that the APT can penetrate, deny, and/or degrade our Cyber Assets (CA).

A defensive strategy based on that assumption is to harden mission-critical CA so we can operate through an APT attack.

Cyber resiliency techniques help us identify the mission-critical CA, evaluate the risks facing those CA, and develop mitigation strategies.
CJA As a Cyber Resiliency Technique

What do we care about?
Understand Mission & Threat Context
- CJA: Identify Mission Objectives and Priorities
- Identify Relevant Threat Classes and Representative Threats
- Identify Relevant Resources—Data Sources, Tools, Specialized Processes

What can we build on?
Establish Initial Cyber Resiliency Baseline
- Identify How Cyber Resiliency Is Already Being Applied
- Identify Cybersecurity Capabilities and Issues
- Assess Current Ability to Achieve Relevant Cyber Resiliency Goals

How do cyber risks affect missions?
Analyze Architecture & Mission Threads
- CJA: Identify Critical Resources
- Represent Adversary Perspective
- Identify Potential Architectural Applications of Cyber Resiliency Design Principles

What might we do to improve mission resilience?
Define and Analyze Specific Alternatives
- Define Alternatives in Terms of Technology and Operational & Development Processes
- Drill down into specific areas (e.g., SCRM) as per scope & purpose
- Analyze Individual Alternatives in Terms of Benefits, Effectiveness

What do we recommend?
Recommend Courses of Action
- Develop Alternative Courses of Action and Analyze in Terms of Cost, Schedule
- Structure Recommendations (e.g., time-phased)
- Identify Follow-on Activities (optional)

Ref: Structured Cyber Resiliency Analysis Methodology (SCRAM), by D. Bodeau and R. Graubart
What is CJA?

- MITRE-developed Mission Criticality Analysis technique
  - *First used during Operations Without Space deep-dive at 613\textsuperscript{th} Air and Space Operations Center (AOC) in 2009*

- CJA’s Dependency Map approach combines expert input with established techniques: *AHP, QFD, and FMEA*

- Definitions when applied to Cyber/IT systems
  - *“Cyber Asset” = A logic-bearing device including its hardware, firmware, software, and initialization/configuration data*
    - *We have also included non-logic bearing devices; e.g. comm links*
  - *“Mission-Critical Cyber Asset” = A Cyber Asset whose failure or degradation causes mission failure; a “Crown Jewel”*
How do failures here . . . translate into impacts here?
We Start by Identifying the Tasks That Support Each Mission Objective
Next, We Identify the System Functions That Support Each Task
Finally, We Identify the Cyber Assets That Support Each System Function
Dependency Mapping - Refinery Example

Mission Objectives
- Stay Safe
- Stay Profitable
- Stay in Compliance
- Supply Customers Well

Operational Tasks
- Acquire Gas for Heaters
- Report Flow Rate
- Report Pressure

System Functions
- Plant LAN Router
- Corporate Router

Cyber Assets
We Use the Dependencies to Predict the Impact of Cyber Asset Failures
Greater Dependency Means Greater Impact from Cyber Asset Failure
How Do We Evaluate a Dependency?

- For our purposes, a dependency is a need
  - Achieving a Mission Objective depends on one or more Tasks being performed as intended
  - Performance of a Task depends on one or more System Functions executing as intended
  - Execution of a System Function depends on one or more Cyber Assets operating as intended

- We express the degree of dependency in terms of criticality
  - Criticality describes the impact of loss of an asset, based on the effect the loss would have on operations and the ability to fulfill the mission
  - We define four levels of impact: Failure, degradation, a workaround is required, and none
Where Does the Information Come From? (Option 1)

Mission Objectives (MO) & priorities come from managers

Operational Tasks (OT) & Mission dependencies come from managers & operators

System Functions (SF) & Task dependencies come from operators & engineers

Cyber Assets (CA) & System Function dependencies come from engineers

Combined model grows from a series of on-site interviews with organizational & technical Subject Matter Experts (SMEs).
Where Does the Information Come From? (Option 2)

Mission Objectives
- MO validation & priorities come from managers

Operational Tasks
- OT validation & Mission dependencies come from managers & operators

System Functions
- SF validation & Task dependencies come from operators & engineers

Cyber Assets
- CA validation & System Function dependencies come from engineers

Model starts prior to on-site discussions using data gleaned from reference documents and MITRE team member expertise. Site SMEs provide validation & completion of data.
How Do We Limit Subjectivity?

1. We use structured question-and-answer sessions with the operational and technical experts on the system
   a. Managers/Operators: What is the impact on Mission Objective “MO1” if Task “T1” is not performed as intended?
      – No impact? Work-Around Required? Degradation? Failure?
   b. Operators/Engineers: What is the impact on Task “T1” if System Function “SF1” does not execute as intended?
      – No impact? Work-Around Required? Degradation? Failure?
   c. Engineers/Administrators: What is the impact on System Function “SF1” if Cyber Asset “CA1” is not operating as intended?
      – No impact? Work-Around Required? Degradation? Failure?

2. Scoring tables provide a reference, to ensure consistency
   – We define “as intended” to mean no failures and no degradation
How Do We Identify the Mission-Critical Cyber Assets?

1. From the dependency identification, we know the following:
   a. If Task “T1” fails, the impact on achieving Mission Objective “MO1” is one of the following:
      ▪ No impact, work-around required, mission degradation, or mission failure
   b. If System Function “SF1” fails, the impact on performing Task “T1” is one of the following:
      ▪ No impact, work-around required, task degradation, or task failure
   c. If Cyber Asset “CA1” fails, the impact on the performance of System Function “SF1” is one of the following:
      ▪ No impact, work-around required, function degradation, or function failure

2. We can use these “if-then” statements to predict the impact at each level in the dependency map
   – We call this step in the CJA the Mission Impact Analysis (MIA)
In the MIA We Consider Each CA As Failed, Starting with CA1
CA1’s Failure Causes Several SF and Tasks to Fail, Causing MO1 Failure
CA2’s Failure Degrades SF1, Causing Task T1 to Fail, Causing MO1 Failure
CA3’s Failure Has an Effect Like That of CA2’s Failure – Causing MO1 Failure
Because CA4’s Failure Degrades SF2 and T1, It Causes MO1 Failure
CA5’s Failure Has an Effect Like That of CA4’s Failure – Causing MO1 Failure

Mission Objective
- MO 1

Tasks
- T 1
- T 2
- T 3
- T 4
- T 5
- T 6
- T 7
- T 8
- T 9
- T 10
- T 11
- T 12
- T 13

System Functions
- SF 1
- SF 2
- SF 3
- SF 4
- SF 5
- SF 6
- SF 7
- SF 8
- SF 9
- SF 10
- SF 11
- SF 12
- SF 13

Cyber Assets
- CA 1
- CA 2
- CA 3
- CA 4
- CA 5
- CA 6
- CA 7
- CA 8
- CA 9
- CA 10

Dependency Legend:
- Black line: Failure
- Gray line: Degraded

Impact Legend:
- Red: Failure
- Orange: Degraded
- Green: Work-Around
- Blue: Nominal

Approved for Public Release: Case 11-2827
© 2018 The MITRE Corporation. All rights reserved
CA6’s Failure Requires a Work-Around for SF2 and SF10 – No MO1 Impact
CA7’s Failure Has an Effect Like That of CA6’s Failure – No MO1 Impact
CA8’s Failure Has an Effect Like That of CA6’s Failure – No MO1 Impact
CA9’s Failure Has an Effect Like That of CA6’s Failure – No MO1 Impact

Dependency Legend:
- Fail/Deg → Failure
- Fail/Deg → Degrade
- Fail/Deg → Work-Around

Impact Legend:
- Failure
- Degrade
- Work-Around
- Nominal

Mission Objective

Tasks

T1 T2 T3 T4 T5 T6 T7 T8 T9 T10 T11 T12 T13

System Functions

SF1 SF2 SF3 SF4 SF5 SF6 SF7 SF8 SF9 SF10 SF11 SF12 SF13

Cyber Assets

CA1 CA2 CA3 CA4 CA5 CA6 CA7 CA8 CA9 CA10
CA10’s Failure Has an Effect Like That of CA6’s Failure – No MO1 Impact
The Results Can Be Compacted For Easy Viewing

- Cell color indicates the Mission Objective’s Impact resulting from each CA failure

- Red means that MO1 fails, and Blue means that MO1 is nominal

- In this example, CA1 through CA5 are Mission-Critical Cyber Assets since their failure would cause MO1 to fail

- Cyber Assets CA1 through CA5 are Mission-Critical Cyber Assets – the “Crown Jewels”

<table>
<thead>
<tr>
<th></th>
<th>MO 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA 1</td>
<td>Red</td>
</tr>
<tr>
<td>CA 2</td>
<td>Red</td>
</tr>
<tr>
<td>CA 3</td>
<td>Red</td>
</tr>
<tr>
<td>CA 4</td>
<td></td>
</tr>
<tr>
<td>CA 5</td>
<td>Red</td>
</tr>
<tr>
<td>CA 6</td>
<td>Blue</td>
</tr>
<tr>
<td>CA 7</td>
<td>Blue</td>
</tr>
<tr>
<td>CA 8</td>
<td>Blue</td>
</tr>
<tr>
<td>CA 9</td>
<td>Blue</td>
</tr>
<tr>
<td>CA 10</td>
<td>Blue</td>
</tr>
</tbody>
</table>
A Typical Case Shows Mission-Critical CA for Several Mission Objectives

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue = Mission Nominal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Green = Mission Work Around</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yellow = Mission Degrade</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Red = Mission Failure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- A single CA in a highly integrated infrastructure will affect more than one MO
- The total mission impact of each CA is shown across each row
- For each MO, the column below it shows the CA that are critical to its achievement
The CJA Methodology Allows For Flexibility

- The preceding slides show a CJA based on the 4-tier model shown here:
  
  ![4-tier model diagram]

  - Different models are also used, depending on the reference information available to the CJA team

- Alternative 4-tier models:
  
  ![Alternative 4-tier models diagram]

  - An Information Asset is operational information needed to perform a task
Alternative Model Using Information Assets - Refinery Example

Mission Objectives
- Stay Safe
- Stay Profitable
- Stay in Compliance
- Supply Customers Well

Operational Tasks
- Acquire Gas for Heaters

Information Assets
- Flow Rate
- Pressure

Cyber Assets
- Corporate Router
- Plant LAN Router

Approved for Public Release: Case 08-0490
© 2018 The MITRE Corporation. All rights reserved
We Use the CJA Tool to Help Build the Dependency Map

Objective Weights

Task Weights

Info Asset/ Sys Funct Weights

Cyber Asset Weights

Mission-Critical CA Candidates

Identify Dependencies on Tasks

… and on Info Assets or System Functions

… and on Cyber Assets

Prioritize Mission Objectives

Identify Dependencies on Tasks

… and on Info Assets or System Functions

… and on Cyber Assets
Next, The CJA Tool Automatically Completes the Mission Impact Analysis (MIA)

- **Task Criticality**
- **IA/SF Criticality**
- **CA Criticality**
- **Propose CA Failures/Degrades**

**Scenarios**

**Tasks**

**Mission Impact**

**Roll-Up Rules Utilize User-Input Criticality Scores**
Tool Demonstration
For More Information:

CJA article in MITRE’s Systems Engineering Guide:


Contact the following at MITRE Bedford:

- Jim Watters - jwatters@mitre.org
- Peter Kertzner - kertzner@mitre.org