Crown Jewels Analysis (CJA): Criticality Analysis

*Helping Healthcare Address the Threat of Ransomware*

Joanne R. Fitzpatrick
3 Feb 2021
CJA at a Glance

Crown Jewels Analysis (CJA) is a MITRE-developed methodology for criticality analysis.

- Identifies an organization’s crown jewels, those cyber assets most critical to accomplishment of organization’s highest objectives.
- Allows healthcare organization to prioritize cyber assets and apply limited resources effectively for cyber resiliency, the ability to operate during a major cyber attack, such as ransomware, and still deliver highest objectives in some capacity.
- Asks senior management to confirm and prioritize healthcare and organization objectives.
- Should be done as part of Risk Management Plan.
- Combines expert input from healthcare SMEs with established, analytical techniques applied from engineering fields. CJA in active use for over 12 years with sponsors of all sizes serving in the public trust.
Understanding Crown Jewels

CJA identifies an organization’s *Crown Jewels*

- Cyber assets (hardware, software, data) *whose failure, or failure to operate or be accessed as intended,* causes failure of an organization’s major objective, e.g., deliver healthcare services
- Are *most* critical to the accomplishment of an organization’s objectives
- Many are already known by organizations. CJA confirms those known and reveals hidden, unexpected ones.

CJA Helps Healthcare Face a Ransomware Attack

*CJA’s purpose is not to prevent or detect a ransomware attack. It mitigates the risk posed by such major attacks. CJA serves an organization:*

- Before an attack, to better prioritize its cyber mitigations in protecting its most important assets
- During an attack, to more effectively respond in addressing most critical assets first
- During an attack, to know extent and impact of processes and systems affected and their relationship to top healthcare objectives
- After an attack, to provide supplemental protection to critical assets not yet involved in attack

CJA Identifies Most Critical Assets

Criticality Analysis

**Establish Highest Priorities**

- WHAT OBJECTIVES ARE MOST IMPORTANT TO THE ORGANIZATION?
- WHAT RESOURCES ARE MOST IMPORTANT? HOW DO WE KNOW?

**Identify Objectives’ Dependencies on Cyber**

**Mission Impact Analysis**

- WHAT ARE THE RISK/THREATS TO ACHIEVEMENT OF TOP OBJECTIVES? WHAT IS ROI FOR ADVERSARIES?
- HOW, WHERE & WHEN TO MITIGATE THE RISKS? WHAT IS ROI TO CYBER DEFENDER?

**Threat Susceptibility Assessment**

**Resiliency & Risk Remediation Analysis**

Healthcare Mission Objectives
Operational Tasks
System Functions

Cyber Threats & Intelligence

Mitigations

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED
APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED
CASE NUMBER PR 20-01867-3
Model Terminology

- **Healthcare Objectives (HO)**
  - Highest tier in model
  - Typical range: 3-6 nodes
  - Matrix 1 in tool

- **Operational Tasks (OT)**
  - Second tier in model
  - Typical range: 20-100 nodes
  - Matrix 2 in tool

- **System Functions (SF)**
  - Third tier in model
  - Typical range: 25-125 nodes
  - Matrix 3 in tool

- **Cyber Assets (CA)**
  - Fourth and lowest tier in model
  - Typical range: 40-200 nodes
  - Matrix 4 in tool
CJA: Five Step Process

1. **Collect Data & Build Initial Model**
   - Initial analysis using client-provided materials and discussions with senior management
   - Outcomes: Agreement on scope of analysis and draft build of model for Matrices 1 & 2

2. **Validate Initial Model**
   - Best done with senior management for HOs and senior healthcare SMEs for OTs
   - Outcomes: Validated build and scoring of Matrices 1 & 2. Leads to draft build of model for Matrices 3 & 4.

3. **Query SMEs for Scores & Relationships**
   - Best done with IT staff and operators for SFs and CAs.
   - Outcomes: Builds and scorings of Matrices 3 & 4.
   - Leads to Dependency Maps

4. **Perform Impact Analysis. Identify Crown Jewels**
   - Initial deliverables

5. **Conduct What-If Analyses & Present Findings**
   - Best done with senior management (objectives’ owners) and system owners
   - Outcomes: Explored options. Allows for better resource management through priorities. Provides focus for future risk analyses and mitigation strategies.
Functional Decomposition

- CJA determines its dependency mappings and ultimate impact analysis by performing decomposition of healthcare IS modules
- Healthcare IS broadly divided into two major areas: Patient Care IS and Managerial IS. Both are comprised of numerous, likely targets for attacks
- Patient Care IS of particular importance. Likely contains most crown jewels. Notionally, comprised of:
  - Patient Mgt System (PMS) – e.g., registration, appointments and scheduling, charging and billing
  - Clinical Information System (CIS) – e.g., patient care plans, clinical decisions, medical order entry, clinical data management
  - Clinical Support Systems (CSS) – e.g., labs, imaging, pharmacy, blood bank, operating room schedules

Ref: Dr. Dollah, 2019 https://drdollah.com/hospital-information-system-his/Information Systems in Health Care | Health Care Service Delivery (drdollah.com)
Sample, Partial Healthcare Decomposition

Healthcare Objectives
- Provide Fair Access to Healthcare
- Deliver Healthcare Services
- Stay Cost-Effective
- Meet or Exceed Estab. Stds of Quality & Care

Operational Tasks
- Manage Patient Admissions

Information Assets
- Past Admittance History
- Current Clinical Profile

Cyber Assets
- Unique Patient ID
- Attending MD ID

Patient Mgt. System (PMS)
Clinical Information System (CIS)
How Dependency Tree Relates to CJA Matrices for Scoring (1 of 2)

Matrix 2 captures HO/MO (parent) to OT (child) relationships.

Matrix 3 captures OT (parent) to SF (child) relationships.

Matrix 4 captures SF (parent) to CA (child) relationships.
Start with Matrix 1. Use AHP to prioritize Healthcare Objectives.

- In model, children nodes become parent nodes
- In tool, columns become rows

Forms candidate Crown Jewels

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-3
## Healthcare Objectives:
### What Might Matrix 1 Look Like?

Notional

<table>
<thead>
<tr>
<th></th>
<th>Deliver Healthcare Svcs</th>
<th>Meet/Exceed Standards</th>
<th>Provide Fair Access</th>
<th>Stay Cost Effective</th>
<th>Sums</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver Healthcare Svcs</td>
<td>1</td>
<td>1.25</td>
<td>1.75</td>
<td>2</td>
<td>6.000</td>
</tr>
<tr>
<td>Meet/Exceed Standards</td>
<td>0.8</td>
<td>1</td>
<td>1.4</td>
<td>1.5</td>
<td>4.900</td>
</tr>
<tr>
<td>Provide Fair Access</td>
<td>0.571</td>
<td>0.714</td>
<td>1</td>
<td>1.14</td>
<td>3.429</td>
</tr>
<tr>
<td>Stay Cost Effective</td>
<td>0.6</td>
<td>0.625</td>
<td>0.875</td>
<td>1</td>
<td>3.000</td>
</tr>
</tbody>
</table>

- Based on the Analytic Hierarchy Process (AHP)
- Inputs only required in the white cells – all others auto-calculated
- Result is a set of normalized Relative Weights

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-3
Healthcare Objectives: Sorted by Relative Weights

Notional

- Deliver Healthcare Services
- Meet or Exceed Standards
- Provide Fair Access
- Stay Cost Effective

- Allows senior management to refine their inputs, to adjust relative priorities of objectives
- Provides a visual means of validating the model at this point in the process
Healthcare Objectives and AHP

- Analytical Hierarchy Process (AHP) determines relative importance among healthcare objectives and used to form CJA Matrix 1
- Provides a means of measuring *intangible* properties, e.g., importance of objectives to senior management, when no direct measurement scale is possible
  - Employs pairwise comparisons using a fundamental scale
  - Comparison values are summed up and the sums normalized
  - Result is a set of relative weights
- Developed by Thomas L. Saaty (1926 - 2017)
  - Very-well respected approach used across numerous domains
  - “Decision Making with the Analytic Hierarchy Process,” 2008
Healthcare Objectives:
Matrix 1 Relationships

<table>
<thead>
<tr>
<th>Objective 1</th>
<th>Objective 2</th>
<th>Objective 3</th>
<th>Sum of Row</th>
<th>Relative Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objective 1</td>
<td>1</td>
<td>$m_{12}$</td>
<td>$m_{13}$</td>
<td>$1 + m_{12} + m_{13}$</td>
</tr>
<tr>
<td>Objective 2</td>
<td>$\frac{1}{m_{12}}$</td>
<td>1</td>
<td>$\frac{m_{13}}{m_{12}}$</td>
<td>$\frac{1 + m_{12} + m_{13}}{m_{12}}$</td>
</tr>
<tr>
<td>Objective 3</td>
<td>$\frac{1}{m_{13}}$</td>
<td>$\frac{m_{12}}{m_{13}}$</td>
<td>1</td>
<td>$\frac{1 + m_{12} + m_{13}}{m_{13}}$</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td>$\frac{(1 + m_{12} + m_{13})(m_{12} + m_{13} + m_{12}m_{13})}{m_{12}m_{13}}$</td>
</tr>
</tbody>
</table>

### Operational Tasks - Matrix 2

**Notional**

- **Purpose:** to determine IMPACT of each task failure on each Healthcare Objective (HO)
- **Sample question and answer:** *What is the impact on the HO Deliver Healthcare Services if Task 1 fails, or fails to operate as intended?*
- **Shadings of orange:** provide a quick visual cue to the highest values on the screen

#### Healthcare Objective Impact of Task Failure/Degradation

- 0 = No Impact on HO achievement
- 30 = HO is achievable using a documented work around
- 75 = HO is degraded even using a work-around
- 95 = HO is not achievable at all

<table>
<thead>
<tr>
<th>Task Criticality to Healthcare Objective</th>
<th>Task 1</th>
<th>Task 2</th>
<th>Task 3</th>
<th>Task 4</th>
<th>Task 5</th>
<th>Task 6</th>
<th>Task 7</th>
<th>Task 8</th>
<th>Task 9</th>
<th>Task 10</th>
<th>Task 11</th>
<th>Task 12</th>
<th>Task 13</th>
<th>Task 14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver Healthcare Services</td>
<td>0.348</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
</tr>
<tr>
<td>Meet of Exceed Standards</td>
<td>0.279</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
</tr>
<tr>
<td>Provide Fair Access</td>
<td>0.199</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
</tr>
<tr>
<td>Stay Cost Effective</td>
<td>0.174</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.30</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
<td>0.70</td>
</tr>
</tbody>
</table>
Operational Tasks - Pareto View

- Based on QFD method
- Calculation produces a weighted average. Relative Weights provide a quick means to visually validate the model
- Caveat: relative weights reflect general importance but do not constitute impact on their own
Operational Tasks, System Functions, Cyber Assets and QFD

- **Quality Function Deployment (QFD) used to form CJA Matrices 2 - 4**
  - Uses series of matrices rather than single “House of Quality”
  - Adds cardinal scale for developing relative weights

- **Decomposes top-level product requirements into underlying qualities and functions. Used to identifies dependencies.**

- **Originally intended for manufacturing setting**

- **Developed by Dr. Yoji Akao (1928 - 2016)**
  - Original work appeared in the 1960’s shipyards in Japan. Brought to U.S. by Don Clausing of MIT
Values in CJA Matrices 2 - 4

- Represent criticality. Four levels.
  - High (failure). Default is 95.
  - Medium (degradation, even with work-around implemented). Default is 70.
  - Low (a documented, trained-to work-around is required). Default is 30.
  - None (no impact). Default is 0.
- Used to calculate relative weights
- Provide a sense of placement within each matrix level
Failure Modes and Effects Analysis (FMEA)

- CJA uses FMEA-like approach to predict impacts to objectives due to failures in system “components”
  - System or information dependencies identified through system decomposition
  - Impacts of failures predicted during Impact Analysis (IA)
  - Comes from reliability discipline within engineering

- Tied to Failure Modes, Effects and Criticality Analysis (FMECA)
  - FMECA extends FMEA by introducing likelihood of failure
  - Prescribed in military standards where loss of life is highest risk. Adopted by NASA and as US/European airworthiness standards
Impact Analysis (IA)

- Occurs after model is built, data is entered, and matrices are scored
- Performed by encoded algorithms in CJA tool. Uses what-if technique to sequentially fail each cyber asset for each healthcare objective
- Results in simulated impacts percolating upwards

Dependency Map for one objective

After Impact Analysis, from first failed asset

© 2021 THE MITRE CORPORATION. ALL RIGHTS RESERVED APPROVED FOR PUBLIC RELEASE DISTRIBUTION UNLIMITED CASE NUMBER PR 20-01867-3
When is an Asset a Crown Jewel?

- **Definition**: a cyber asset whose failure, or failure to perform as intended, causes a major healthcare objective to fail
- Typically a physical, system, or information asset an organization cannot afford to lose, i.e., operate without
- Likely candidates for adversaries, especially in ransomware attacks

**Diagram Note**: CA1 fails and **is** a Crown Jewel

**Diagram Note**: CA6 fails but **is not** a Crown Jewel
CJA Results: Portrayal Table

- Available as part of Impact Analysis
  - Shows relative weights of each cyber asset as a whole. Allows for healthcare SME reality checks
- Impact view option
  - Sorts by impact to bring Crown Jewels to the top.
  - Assists in prioritizing resources for follow-on assessments and/or resiliency mitigations
- Intermediate option
  - Allows an intermediate Portrayal Table to view after Matrices 1 & 2, before populating Matrices 3 & 4
  - Good way to solidify model before going forward, especially if model is large, complex
- Propagation option
  - Allows a force of all degraded scores in tables to impact as failures
  - Commonly used in scenarios where human life and safety are paramount, e.g., manned spaceflight
High relative weights confirm already-suspected cyber assets

Relative weights provide a means of prioritizing among crown jewels

Impact analysis reveals little-used cyber assets that are nonetheless healthcare critical
Dependency Maps & Impact Maps

- Available after model build and data entry, like Portrayal Table.
- Part of Impact Analysis (IA)
  - Reading **down** a map shows dependencies. Look at weight of lines
  
  ![Dependency Legend](image1)

  - Reading **up** a map shows impact (criticality)

  ![Impact Legend](image2)

- Map for an entire system can be large. Usually does not fit on one slide in readable way. Can display/print one HO at a time for further analysis by healthcare organization
Dependency Map Example

- Full dependency map for 4 objective example. Can zoom and isolate for clear displays of branches and nodes.
- All OT, SF and CA are represented, not just those thought to be critical at the outset
- Overall map provides context and insights to organization
- Provides a visual opportunity to validate the data in an overall sense
How Can CJA Help?
Conclusions for your Healthcare Organization

- CJA identifies an organization’s **crown jewels**, using prioritized healthcare objectives, as determined from an organization’s senior team, as its foundation
- CJA creates a model that is **organization and architecture agnostic**, working for any size organization employing any types of hardware, software, and data
- Upon completion, an organization gains **architecture and functional decompositions** of their HIS, with CJA Dependency Maps and Impact Analysis. The model is reused by an organization as situations necessitate
- CJA offers a **strong component to Cyber Resiliency and Risk Management Planning**, especially when faced with top-tier adversaries capable of executing advanced persistent threats (APTs), such as ransomware
- CJA has been employed in serving our nation’s top, critical, federal sponsors **for over 12 years**. CJA SMEs have deep reachback