RISK ANALYSIS

Mikhail Sosonkin

Overview
Introduction
OCTAVE
Characteristics
Criteria
Methods
Large
Small
Choosing
Minimal
Example
Homework

OCTAVE:
Operationally Critical Threat, Asset and Vulnerability Evaluation

Mikhail Sosonkin
mike@isis.poly.edu

Polytechnic University
CS996: Information Security Management

April 27, 2005
OVERVIEW

1. **Introduction**

2. **What is OCTAVE?**

3. **Key Characteristics**

4. **OCTAVE Criteria**

5. **The OCTAVE Methods**
   - OCTAVE: For Large Organizations
   - OCTAVE-S: For Small Organizations
   - How to Choose

6. **Minimal Example**

7. **Homework**
Introduction

  - OCTAVE is registered with US Patent and Trademark Office by CMU
- It is a technique for performing risk analysis.
- Considers both technological and organizational issues.
- Looks at the daily usage of organization's computing infrastructure.
- Provides a baseline for improvement.
The Security Working Integrated Project Team (WIPT), Office of the Assistant Secretary of Defense/Health Affairs (OASD/HA), endorses OCTAVE as the preferred information security risk assessment to prepare for complying with the Administrative Simplification subsection of the HIPAA of 1996.

Some users of OCTAVE:

- Telemedicine & Advanced Technology Research Center
- Advanced Technology Institute
- Office of the Comptroller of the Currency
- Secure Communications Solutions, Inc.
- Department of Transportation
- Department of Commerce
- Library of Congress
- US Nuclear Regulatory Commission
- National Center for Manufacturing Sciences
What is OCTAVE?

- It is self directed: *People from the organization do the actual evaluation, they are aware of the organization’s requirements and operations.*
- Targeted: *Focused at organizational risk and strategic, practice-related issues.*
- The team: *A small team of people from operational (or business) units and the Information Technology department.*
- Approach: *Driven by operational risk and security practices, technology is examined only in relation to the security practices.*
The Balance of the Three Aspects


**Activities**

OCTAVE has a distinct beginning and end in the organizations Risk Management Activities. OCTAVE can be performed on an event or periodical basis.
## Differences between OCTAVE and other Methods

<table>
<thead>
<tr>
<th>OCTAVE</th>
<th>Other Evaluations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations evaluation</td>
<td>System evaluation</td>
</tr>
<tr>
<td>Focus on security practices</td>
<td>Focus on technology</td>
</tr>
<tr>
<td>Strategic issues</td>
<td>Tactical issues</td>
</tr>
<tr>
<td>Self direction</td>
<td>Expert led</td>
</tr>
</tbody>
</table>
- An interdisciplinary team, *analysis team*, leads the evaluation.

- Both business and IT perspectives are important when characterizing the global, organizational view of information security risk.

- OCTAVE is an asset-driven evaluation approach.
Functions of the Analysis Team

- Identify information related assets that are important to the organization.
- Focus risk analysis on the most important organizational assets.
- Consider the relationships among critical assets, the threats to those assets and vulnerabilities that can expose assets to threats.
- Evaluate risks in an operational context.
- Create practice-based protection strategy and risk mitigation plans to reduce risk.
**THE PHASES OF OCTAVE RISK EVALUATION**

**Phase 1:** Build Asset-Based thread profiles
- Important Assets Identifies
- What is done to protect the assets
- Security Requirements for each Asset are Identified

**Phase 2:** Identify Infrastructure Vulnerabilities
- Examine Network Access Paths
- Identify Classes of IT Components for Each Asset
- Determine Resistance to Network Attacks
Phase 3: Develop Security Strategy and Plans
- Identify Risks to Critical Assets
- Develop Protection Strategy and Mitigation Plans.
- The Analysis is Based on Previous Phases.
Phases

octave® Process

Phase 1
Organizational View
- Assets
- Threats
- Current Practices
- Organization Vulnerabilities
- Security Requirements

Phase 2
Technological View
- Key Components
- Technical Vulnerabilities

Phase 3
Strategy and Plan Development
- Risks
- Protection Strategy
- Mitigation Plans

Progressive Series of Workshops
OCTAVE Criteria

- A Set of:
  
  **Principles**  Fundamental concepts driving the nature of evaluation. It shapes the approach and provides basis for evaluation.

  **Attributes**  Distinctive qualities or characteristics of evaluation, defines what makes the evaluation successful. Attributes are derived from principles.

  **Outputs**  The required result of each phase. Unique activities are not set because more than one activity can be done to achieve the outputs of OCTAVE.
Criteria

OCTAVE Methods

OCTAVE Method
(as defined in OCTAVE Method Implementation Guide v2.0)

OCTAVE Criteria

OCTAVE-S
(An OCTAVE-Consistent Method for Small Organizations)

Other Methods Consistent with the OCTAVE Criteria

Developed by others

Developed by the SEI

Under development by the SEI

Used by the SEI

Large

Small

Choosing

Minimal

Example

Homework
# Mapping of Principles to Attributes

<table>
<thead>
<tr>
<th>Principle</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Direction</td>
<td>RA.1 Analysis Team</td>
</tr>
<tr>
<td></td>
<td>RA.2 Augmenting Analysis Team Skills</td>
</tr>
<tr>
<td>Adaptable Measures</td>
<td>RA.3 Catalog of Practices</td>
</tr>
<tr>
<td></td>
<td>RA.4 Generic Threat Profile</td>
</tr>
<tr>
<td></td>
<td>RA.5 Catalog of Vulnerabilities</td>
</tr>
<tr>
<td>Defined Process</td>
<td>RA.6 Defined Evaluation Activities</td>
</tr>
<tr>
<td></td>
<td>RA.7 Documented Evaluation Results</td>
</tr>
<tr>
<td></td>
<td>RA.8 Evaluation Scope</td>
</tr>
<tr>
<td>Foundation for a Continuous Process</td>
<td>RA.9 Next Steps</td>
</tr>
<tr>
<td></td>
<td>RA.3 Catalog of Practices</td>
</tr>
</tbody>
</table>
## Mapping of Principles to Attributes (Continuation)

<table>
<thead>
<tr>
<th>Forward-Looking View</th>
<th>RA.10 Focus on Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus on the Critical Few</td>
<td>RA.8 Evaluation Scope</td>
</tr>
<tr>
<td></td>
<td>RA.11 Focused Activities</td>
</tr>
<tr>
<td>Integrated Management</td>
<td>RA.12 Organizational and Technological Issues</td>
</tr>
<tr>
<td></td>
<td>RA.13 Business and Information Technology Participation</td>
</tr>
<tr>
<td></td>
<td>RA.14 Senior Management Participation</td>
</tr>
<tr>
<td>Open Communication</td>
<td>RA.15 Collaborative Approach</td>
</tr>
<tr>
<td>Global Perspective</td>
<td>RA.12 Organizational and Technological Issues</td>
</tr>
<tr>
<td></td>
<td>RA.13 Business and Information Technology Participation</td>
</tr>
</tbody>
</table>
### Mapping of Principles to Attributes

(Continuation)

| Teamwork | RA.1 Analysis Team  
|          | RA.2 Augment Analysis Team Skills  
|          | RA.13 Business and Information Technology Participation  
|          | RA.15 Collaborative Approach |
Further information about each attribute can be found in the OCTAVE Criteria Technical Report.
The OCTAVE Methods

- OCTAVE has two methods.
- OCTAVE is for large organizations with 300 or more employees.
- OCTAVE-S is for organizations with 20 to 80 employees.
OCTAVE: Phase 1 - Build Asset-Based Thread Profiles

Gathering of information from across the organization and defining threat profiles for critical assets

**Process 1:** Identify Senior Management Knowledge - *important assets, security requirements, threats, and organizational strength and vulnerabilities from senior managers.*

**Process 2:** Identify Operational Area Knowledge - *important assets, security requirements, threats, and organizational strength and vulnerabilities from selected operational areas.*

**Process 3:** Identity Staff Knowledge - *important assets, security requirements, threats, and organizational strength and vulnerabilities from general staff and IT staff.*

**Process 4:** Create Threat Profile - *select 3 to 5 critical information-related assets and defines the threat profiles for those assets.*
The analysis team evaluates key components of systems supporting the critical assets for technological vulnerabilities.

**Process 5:** Identify Key Components - *set of key components from the systems that support or process the critical information-related assets are identified, and an approach for evaluating them is defined.*

**Process 6:** Evaluate Selected Components - *The components are evaluated using various tools, and the results are analyzed to update the threat profiles for the critical assets.*
OCTAVE: Phase 3 - Develop Security Strategy and Plans

Evaluate risks to critical assets and develop an organizational protection strategy and risk mitigation plans

**Process 7**: Conduct Risk Analysis - *impact value is determined using the High, Medium, Low scale.*

**Process 8**: Develop Protection Strategy - *organization-wide security increase plan is developed.*

Complete set of instructions are found on http://www.cert.org/octave in *OCTAVE Method Implementation Guide.*
Organizational information is identified and used to define threat profiles for three to five critical information related assets.

**Process S1:** Identify Organizational Information - *identification of important information related assets, defines a set of impact evaluation criteria, and the current state of security practices.*

**Process S2:** Create Threat Profiles - *select 3 to 5 critical information-related assets and defines the threat profiles for those assets.*
The analysis team takes a high-level review of their infrastructure and technology-related practices to refine the threat profiles.

**Process S3:** Examine the Computing Infrastructure in Relation to Critical Assets - *analysis of network access paths that relate to assets and how they are protected by technology.*
The risks to critical assets are evaluated and an organizational protection strategy and risk mitigation plans are defined.

**Process S4:** Identify and Analyze Risks - evaluates all active risks for impact and, optionally, probability.

**Process S5:** Develop Protection Strategy and Mitigation Plans - an organization-wide protection strategy and risk mitigation plans based on security practices is developed.

Complete set of instructions are found on http://www.cert.org/octave in *OCTAVE-S Implementation Guide*.
# How to Choose the Method

<table>
<thead>
<tr>
<th>Question</th>
<th>OCTAVE</th>
<th>OCTAVE-S</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Size and complexity of the organization</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your organization small? Does your organization have a flat or simple hierarchical structure?</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Are you a large company (300 or more employees)? Do you have a complex structure or geographically-dispersed divisions?</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td><strong>Structured or Open-Ended Method</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you prefer a more structured method using fill-in-the-blanks, checklists, and redlines, but not as easy to tailor?</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Do you prefer a more open-ended methodology that is easy to tailor and adapt to your own preferences?</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
### Analysis team composition

<table>
<thead>
<tr>
<th>Can you find a group of three to five people for the analysis team who have a broad and deep understanding of the company and also possess most of the following skills? problem-solving ability, analytical ability, ability to work in a team, at least one member with leadership skills, ability to spend a few days working on this method</th>
<th>✗</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can you find a group of 3-5 people for the analysis team who have some understanding of at least part of the company and also possess most of the following skills? problem-solving ability, analytical ability, ability to work in a team, at least one member with leadership skills, at least one member who understands the computing infrastructure and how to run and interpret vulnerability tools, ability to spend a few weeks working on this method</td>
<td>✗</td>
</tr>
</tbody>
</table>
## How to Choose the Method

**IT resources**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you outsource all or most of your information technology functions?</td>
<td>×</td>
</tr>
<tr>
<td>Do you have a relatively simple information technology infrastructure that is well understood by at least one individual in your organization?</td>
<td>×</td>
</tr>
<tr>
<td>Do you manage your own computing infrastructure and are familiar with running vulnerability evaluation tools?</td>
<td>×</td>
</tr>
<tr>
<td>Do you have a complex computing infrastructure that is well understood by one or more individuals in your organization?</td>
<td>×</td>
</tr>
<tr>
<td>Are you able to run, comprehend, and interpret the results of vulnerability evaluation tools within the context of information-related assets (i.e., can you tell if a particular vulnerability means a particular asset is exposed to unwanted modification or destruction)? Are you able to use the expertise of a current service provider to interpret results?</td>
<td>×</td>
</tr>
</tbody>
</table>
How to Choose the Method

Using a Beta-version method

Are you willing to use a beta-version of a method (that is, use a method that may not have all the guidance you might need)?

×
POSA Example

- A group consisting of IT personnel, Customer Service representatives, management and others involved.
- The areas of operation: cashers, business management, IS support.
- Key components: the register, POSA, The database.
- Protection Strategy: only authorize personnel has access to the database, cashers are not allowed to operate the POSA credit card reader.
Homework: NO GTS!

- Determine which organization category (OCTAVE or OCTAVE-S) Polytechnic University fits into by answering the “selection” (on slides 27-30) questions.

- Would it be enough to perform OCTAVE on just the Online Purchasing System at Amazon.com? Why or Why not?

- You are a Systems Administrator of the ISIS laboratory and somebody within the University is performing OCTAVE. Pick 2 assets and complete the Security Requirements Worksheet. HINT: It is located on page 41 in Volume 5A of the OCTAVE Implementation Guide, it can be downloaded from http://www.cert.org/octave/ in the Methods section.