


SECURITY
TECHNOLOGY

SECURITY
SOLUTIONS


SECURITY
TRAINING



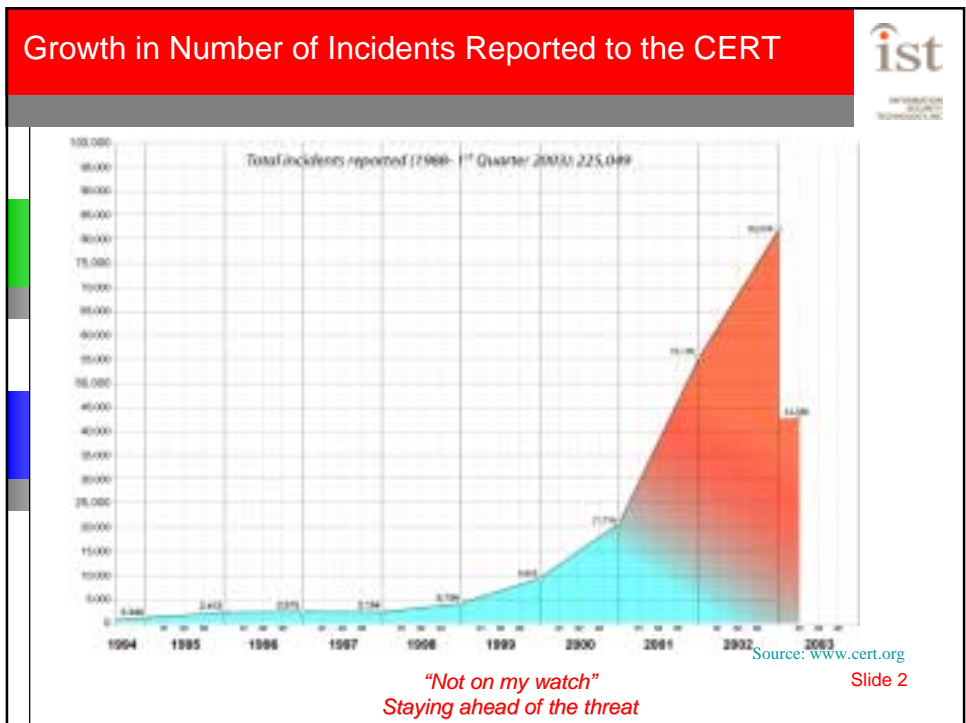
Information Security Technology, Inc.

Staying ahead of the threat: OCTAVE Risk Assessment

Jamie R. Bjerke, CISSP
Director of Technical Services



"Not on my watch"



Attack Impact vs. Intruder Knowledge



Source: www.cert.org

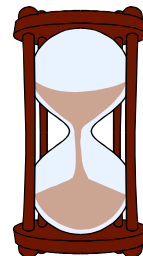
*"Not on my watch"
Staying ahead of the threat*

Slide 3

Cyber Threat Timeline



- **Out-of-the-box Linux PC connected to the Internet, unannounced:**
- **[30 seconds] First service probes/scans detected**
- **[1 hour] First compromise attempts detected**
- **[12 hours] PC fully compromised:**
 - Administrative access obtained
 - Event logging selectively disabled
 - System software modified to suit intruder
 - Attack software installed
 - PC actively probing for new hosts to attack



*"Not on my watch"
Staying ahead of the threat*

Slide 4



Organizational Vulnerabilities

- Resources
- Users
- Inadequate security practices

• Technical Vulnerabilities

- Design
- Implementation
- Configuration

*"Not on my watch"
Staying ahead of the threat*

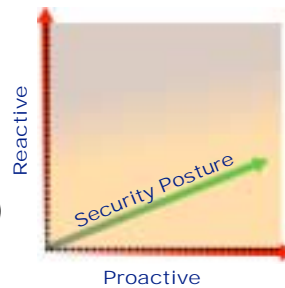
Slide 5

• Vulnerability Management (Reactive)

- Identify and fix vulnerabilities
- Patch/harden systems

• Risk Management (Proactive)

- Identify important assets
- Manage risks



*"Not on my watch"
Staying ahead of the threat*

Slide 6

Welcome to OCTAVE

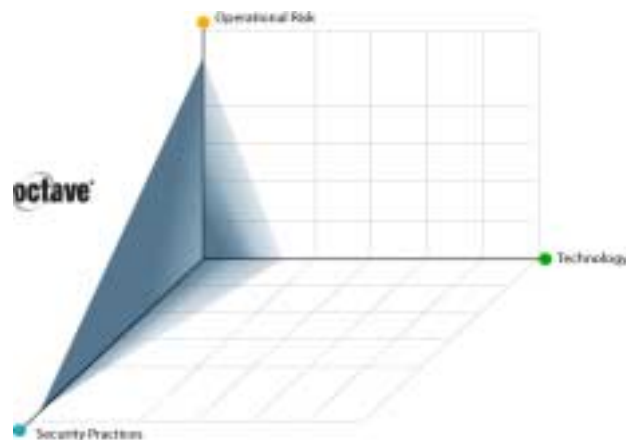


- OCTAVE - Operationally Critical Threat, Asset, and Vulnerability EvaluationSM
- Developed by Carnegie Mellon as a proactive risk assessment approach which is:
 - Workshop driven
 - Self directed
 - Flexible
 - Different from typical technology-focused assessments -> OCTAVE balances operational risk, security practices, and technology.

*"Not on my watch"
Staying ahead of the threat*

Slide 7

OCTAVE: A Practice-Based Approach



*"Not on my watch"
Staying ahead of the threat*

Slide 8

OCTAVE vs. Other Assessment Methods

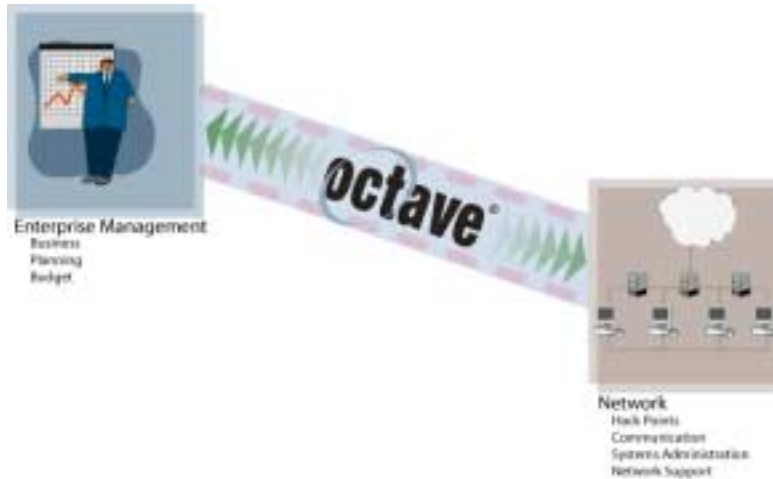


OCTAVE	Other Assessments
Organization evaluation	System evaluation
Focus on security practices	Focus on technology
Strategic issues	Tactical issues
Self directed	Outside expert led

*"Not on my watch"
Staying ahead of the threat*

Slide 9

OCTAVE Bridges the Gap



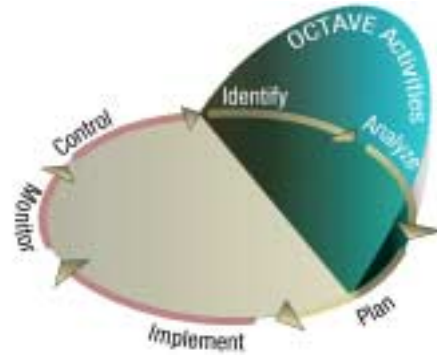
*"Not on my watch"
Staying ahead of the threat*

Slide 10

OCTAVE and Risk Management



- OCTAVE is at the center of a risk management approach to information security.



*"Not on my watch"
Staying ahead of the threat*

Slide 11

OCTAVE Risk Assessment Methodology



Founding Principles

- You cannot mitigate all information security risks
- Your budget is limited, so are other resources
- You cannot prevent all determined, skilled incursions
- You need to determine the best use of your limited resources to ensure the survivability of your enterprise
 - Enterprise view
 - Focus on critical few

*"Not on my watch"
Staying ahead of the threat*

Slide 12

Objectives of the OCTAVE Risk Assessment



Objectives of the Initiative

- Direct and manage future risk assessments independently
- Make the best decisions based on your unique risks
- Focus on protecting key information assets
- Effectively communicate key security information

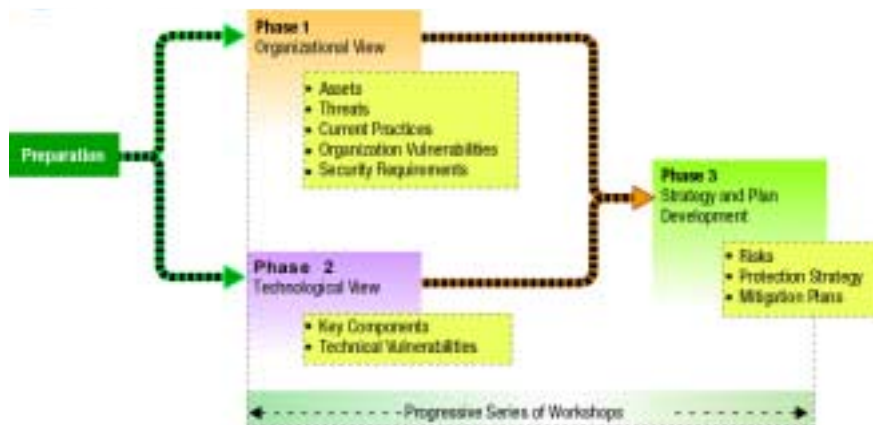
*"Not on my watch"
Staying ahead of the threat*

Slide 13

OCTAVE Risk Assessment Process



OCTAVE is organized into three phases



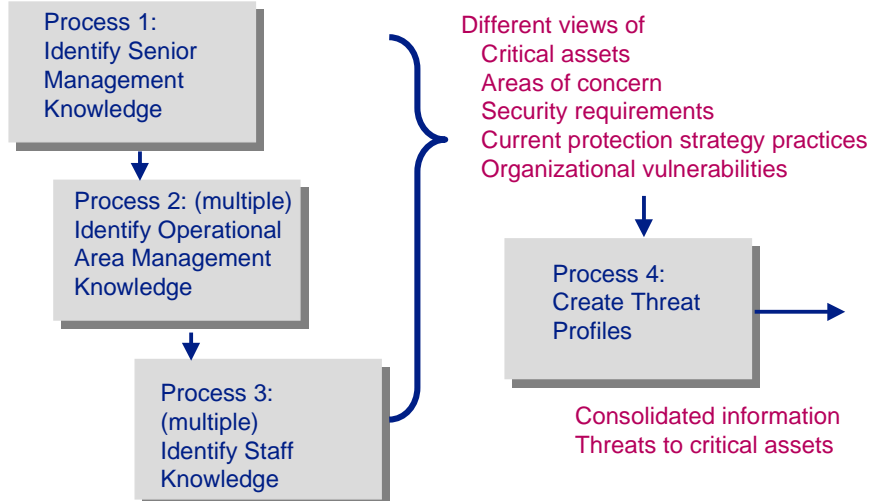
*"Not on my watch"
Staying ahead of the threat*

Slide 14

Assessment Execution



Phase One Organizational View



*"Not on my watch"
Staying ahead of the threat*

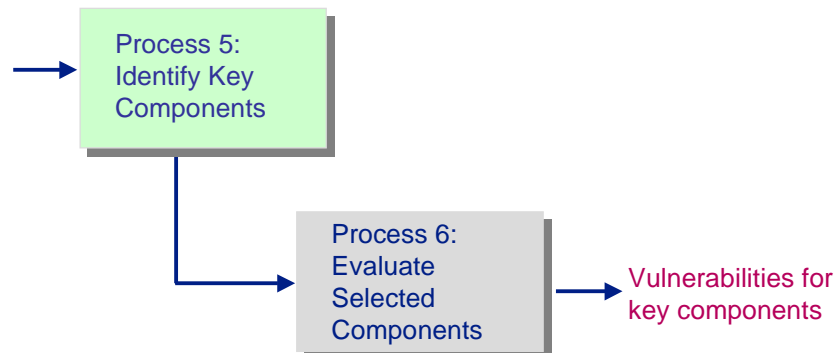
Slide 15

Assessment Execution



Phase Two Technological View

Process 5 requires the identification of system and application components that comprise the critical assets identified during Phase 1



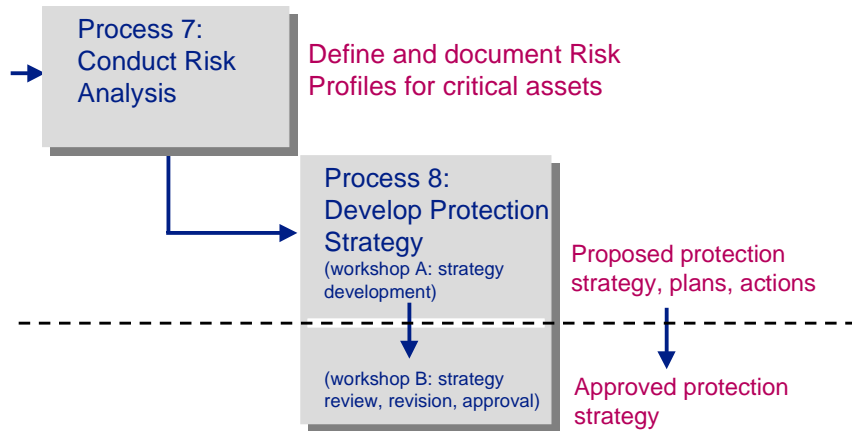
*"Not on my watch"
Staying ahead of the threat*

Slide 16

Assessment Execution



Phase Three Strategic View



*"Not on my watch"
Staying ahead of the threat*

Slide 17

Outputs of OCTAVE



*"Not on my watch"
Staying ahead of the threat*

Slide 18

Conclusion: OCTAVE Risk Assessment



Advantages

- Flexible and self-directed
- Encompasses technical and organizational threats and vulnerabilities to derive risk specific to the organization
- Leverages people's knowledge of their specific organization's security practices and processes to capture the current state of security within the organization
- Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization
- Provides a repeatable framework for enterprise-wide risk assessment

*"Not on my watch"
Staying ahead of the threat*

Slide 19

IST Your OCTAVE Partner



- Training
 - Classroom
 - Onsite
- Implementation support
 - OCTAVE Assessment mentorship
 - Workshop facilitation
 - Methodology adoption

*"Not on my watch"
Staying ahead of the threat*

Slide 20

SECURITY TECHNOLOGY	
SECURITY SOLUTIONS	
SECURITY TRAINING	
 <small>INFORMATION SECURITY TECHNOLOGY</small>	

Thank You!



Jamie R. Bjerke
Director of Technical Services
jrb@istsecure.com

"Not on my watch"