CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Assuring Mission Success in Complex Environments

Key Message: Analysis tools are needed for assessing complex organizational and technological issues (and allocating limited resources) that are well beyond traditional approaches.

Executive Summary

In today's business environment, multiple organizations routinely combine efforts in pursuit of a single objective, resulting in programmatic, process, and technological complexity that can be difficult to manage effectively. Achieving success in such complex settings has proven to be difficult. To determine the chances of succeeding, business leaders managing a program or overseeing a process must have a way to sort through the inherent complexity of multi-organizational objectives.

In this podcast, Christopher Alberts, a senior researcher at Carnegie Mellon's Software Engineering Institute, discusses promising research directions for assessing complex programs and processes, so business leaders can evaluate success against the objectives that define a mission.

PART 1: BACKGROUND AND EVOLUTION FROM OCTAVE

OCTAVE

CERT's security risk assessment method, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), was developed to help organizations better understand their current security posture.

OCTAVE provides a locally optimized approach to dealing with information, system, and organizational security issues.

However, it is not intended to deal with a situation where partners, supplier, vendors, and other collaborators are also part of the equation (the virtual enterprise). This is much more the case in today's business climate.

New Directions

Current CERT research efforts are more closely focused on examining the interrelationships and dependencies that emerge in virtual enterprises, as well as on addressing the question, "What are the primary factors that affect an organization's ability to achieve their business objectives?" in an extended enterprise.

Putting security in a business context is key for a better understanding of how neglecting security can impact the organization.

PART 2: ASSURING MISSION SUCCESS

Developing Confidence in Achieving Business Objectives

This approach targets processes and programs that are distributed across multiple organizations, where a single organization does not have control over the entire process (such as incident management and response).

What does confidence mean?

- "I'll know it when I see it."
- An innate sense of acceptable performance that most experienced managers have.

How can this be determined more systematically?

- Break down objectives into dimensions of success.
- Determine best- and worst-case scenarios, and identify several in-between scenarios.
- Answer the questions "What is good performance?", "What is bad performance?", "What is acceptable and what's not?"
- Map scenarios to these questions.

This analysis approach also looks at risks in the aggregate, not individual risks. It addresses the questions:

- What is the most likely or expected outcome?
- What is the range of likely or expected outcomes based on various conditions?
- Where is the likely outcome in relation to the desired outcome?

The delta between likely outcome and desired outcome identifies the gap that serves as the target for improvement.

What is inherited risk? Why is it important?

- Regardless of how much one organization improves, it is always subject to the practices and performance of partners with whom it is connected.
- Weaknesses in a partner's practice can result in inherited risk — from one organization to another.
- In the case of a supply chain, an organization can inherit risk from its "upstream" providers and pass along risk to its "downstream" providers.
- Risk can be amplified or dampened as it moves through the process or supply chain.
- Often there are no controls in place for risks that are inherited or imposed by others.

PART 3: METHODS AND TOOLS FOR TACKLING RISK IN COMPLEX ENVIRONMENTS

MOSAIC - Mission-Oriented, Structured Analysis and Improvement Criteria

The MOSAIC tool suite creates an integrated view of the mission objectives from process, product and service, and risk perspectives — and the eventual outcomes resulting from these.

It can be used to:

- determine objectives
- define what constitutes success
- forecast the potential for success
- measure health status at any given point in time
- develop strategies to keep from failing

MOSAIC examines the deviation from what's documented versus what people are actually doing, by process and by role.

It then presents a "big picture" view that integrates all of the parts and players and describes, "Here's where you are in relation to where you want to be."

One of the components of MOSAIC is the Mission Diagnostic Protocol (MDP). It is a technique that provides a quick, high-level evaluation of a mission. This evaluation allows a business leader to project the mission's potential for success based on current conditions.

MDP identifies and tailors up to ten indicators that are worth examining for a given process or situation. Examples of indicators for incident management might include:

- Is there a design for the incident management process?
- Are process risks actively managed?
- Are stakeholder pressures affecting the work?
- Is the incident management mission explicitly defined?

Indicators provide a gauge for the general health of the process, so leaders can determine if their current efforts are poor, acceptable/reasonable, or very good.

Indicators also help focus an organization's attention and investment dollars. They help identify gaps at the local level and across the end-to-end process.

End-to-end process indicators sometimes reveal that teams are working at cross-purposes with respect to achieving objectives — and thus may not achieve them.

The MOSAIC tool suite is a life-cycle approach to be used from the beginning and throughout any program. In addition to the Mission Diagnostic, other tools include:

- Workflow diagramming
- MAAP – Mission Assurance Analysis Protocol

MAAP is a comprehensive technique that leaders can use at strategic points in the life cycle to carry out a more comprehensive analysis of a mission. This analysis allows an organization to take an in-depth look at the factors affecting a mission's potential for success.

So who's responsible for end-to-end risk management and thus in the position to make best use of MOSAIC?

- Program managers
- Those who oversee complex missions and contractual relationships
- Senior leaders in roles to sponsor and support improvement programs

Resources

SEI’s Risk and Opportunity Management website
