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

Key Message: Business leaders need new approaches to address multi-enterprise, systems of systems risks across the life cycle and supply chain.

Executive Summary

Traditional approaches to risk management rely on historical data, focus on cause and effect, and address risk in silos such as life cycle phase, organizational unit, or type of risk. These approaches fall short when you need to identify and manage unprecedented risks across the life cycle, across the global supply chain, and across systems that need to inter-operate.

In this podcast, Chris Alberts, a senior researcher in risk management at Carnegie Mellon's Software Engineering Institute, discusses effective ways to manage risk in complex, distributed, systems-of-systems programs. Chris will also describe some of the implications for security.

PART 1: WHY TRADITIONAL APPROACHES FALL SHORT

Three Characteristics of Traditional Approaches to Risk Management

When it comes to developing and operating software-intensive systems and systems of systems, traditional risk management approaches:

- rely solely on historical data such as taxonomies of historical sources of risk, and probabilities and frequencies based on statistical data or past occurrences
- employ a tactical analysis of risk where risk is typically defined as a cause (an event) and an effect (a consequence). One example is how a staffing shortfall may affect the quality of response for an incident management help desk.
- appear as point solutions where risk is managed in silos, based on life cycle phase or type of risk (for example, security risk, operational risk, architecture risk, program risk)

Why These Approaches Are Insufficient

These approaches fall short in today's environments for the following reasons:

- Events and market drivers are rapidly changing which means that the past is not a good predictor of the future.
    - Security is one excellent example due to frequent discovery of new vulnerabilities and new exploits that introduce new risks. These will not be reflected in the historical data.
- Tactical approaches tend to generate lists of hundreds of risks which are rank ordered based on probability of occurrence and impact (risk exposure).
    - Managers tend to focus on the top 10-20 percent but are often caught off guard by a risk in the remaining 80 percent.
    - Often a set of small, relatively benign risks combine to cause a greater failure.
    - This approach can build false confidence that you've identified the key risks.
- Risks are often interrelated, so managing them by type tends to overlook the extent to which they can affect one another. For example, security risks affect business processes and programs such as in the case where a competitor gains unauthorized access to proprietary information.

Addressing the Shortfalls

Historical data must be augmented with more model-based structured analysis of system characteristics ("system" includes a process, a program, or an IT system).

Tactical approaches can be greatly strengthened by aggregating risks into groups, called drivers, and focusing management action and continuous review at the driver level.

Risk silos can be broken down by taking a more holistic, integrated view of risk.

PART 2: MANAGING RISKS ACROSS THE LIFE CYCLE; USING THE MOSAIC TOOLKIT

Taking a Life Cycle View of Risk

Processes, programs, and systems are almost always interconnected and interrelated. Systems are developed, deployed, operated, and maintained. Decisions made early in the life cycle can impose risk later in the life cycle. In other words, later life cycle phases “inherit” risk from earlier phases.

Supply Chain Risk

This same principle applies to supply chains, where each downstream partner is dependent upon the products and services delivered by upstream providers. Upstream decisions affect product quality and timeliness, and thus introduce inherited or imposed risk downstream.

What This Means

Effectively dealing with inherited and imposed risk calls for more holistic solutions that link to business mission and objectives, rather than specific programs, processes, or systems.

When you’re examining only one link in the chain, this is local optimization – perhaps necessary but not sufficient.

Mosaic: A More Integrated, Holistic View

The need for Mosaic derived from organizations needing something more than traditional approaches could offer when dealing with multi-enterprise, multi-system management environments.

Mosaic is a suite of methods that can be applied across the life cycle and across the supply chain. Some methods can be self-applied; advanced methods require more expertise.

An Analogy

It is useful to think of Mosaic in the same fashion as the range of treatments available for diagnosing and treating health-related conditions such as:

- utilizing self-diagnosis and over-the-counter remedies
- visiting a general practitioner for simple testing or more specialized testing such as an MRI
- visiting a specialist for more in-depth testing and diagnosis

Mosaic Tool Suite

Mosaic comprises:

- self-applied assessments (basic health checks)
- diagnostics applied by risk management experts
- advanced analyses that provide an in-depth view of processes, programs, and systems including determining root causes of risk
- specialized assessments such as a security risk assessments. Some specialized assessment are outside the scope

of Mosaic.

Applying Mosaic

Mosaic can be applied in a general, broader fashion to help identify top-level risks or to a specific domain or context such as security.

Structured analysis using Mosaic includes:

- identifying key objectives for the program, process, or system, incident management being a case in point:
  - Objectives likely include the quality of the response to the event, timeliness of the response, and customer satisfaction.
- identifying a small set of drivers that derive from the objectives. A driver is a factor that has a strong influence on whether or not the objectives will be met.
  - For incident management, ten drivers were identified including determining if task execution is effective and efficient.
  - Drivers are framed as yes/no questions with five possible responses.
  - For incident management, drivers helped elicit:
    - experience and expertise of people performing the task
    - experience and actions of management
    - staffing levels and resources
    - tool availability
    - training effectiveness
    - impact of events such as losing key staff, key tools, and key systems

Mosaic can be used to drill down to the desired level of detail.

PART 3: DEALING WITH PREVENTABLE FAILURESM

Causes of Preventable Failures

Causes include:

- uneven or inconsistent application of current risk practices
- selected methods that are not well suited to the organization’s environment
- risk management poorly integrated with other management practices
- risk management viewed as time consuming and bureaucratic, with little perceived value in executing day-to-day activities

Business leaders need to ask and answer the following questions:

- Are our risk management practices effective?
- Are they providing the information we need when we need it?
- Can we improve our current methods? Do we need better methods?
- Where are our most pressing gaps?

Following a Process versus Being Effective

When addressing risk management, business leaders need to be concerned with both adherence to a defined process AND the effectiveness of the process in generating useful outcomes and results.

Adherence to a defined process includes:

- doing the right things

- developing a risk management plan
- identifying and expressing risks
- confirming that all of the pieces are in place

Effectiveness includes asking and answering the following questions:

- If I have a risk management plan, is it a good plan?
- If I am identifying risks, are the risk statements well constructed?
- Am I keeping within your established risk tolerances?
- Is my risk management process informing my day-to-day business decisions?
- Is the process helping inform decisions at critical juncture points such as a merger and acquisition or a major new system, product, or service development?

Effective risk management is about making better decisions based on the risks you are confronting. When using a standard or guideline, don't lose sight of this objective.

What's Next for Mosaic?

- The development team has recently released a new set of courses and evaluation services.
- The risk management framework is due for release in fall 2009 along with supporting evaluations.
- A new book on systemic risk management is in the planning stages for late 2010, early 2011.
- Work is continuing to codify advanced methods, possibly including risk simulation models using system dynamics to evaluate risk in mission critical systems.

Resources

SEI's Risk and Opportunity Management web site

SEI report – A Framework for Categorizing Key Drivers of Risk, April 2009

SEI course – Practice Risk Management: Framework and Methods

SEI webinar – A Practical Approach for Managing Risk (under June 18, 2009)