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

Adapting to Changing Risk Environments: Operational Resilience

Key Message: Business leaders need to ensure that their organizations can keep critical business processes and services up and running in the face of the unexpected.

Executive Summary

Security, business continuity, disaster recovery, and IT service management can no longer be viewed as separate and distinct disciplines. Business leaders need to build and sustain operational resilience at the enterprise level.

In this podcast, Rich Caralli, who leads CERT's research efforts in operational resilience, shares the critical relationship between security and operational resilience, and why this should be a primary focus for business leaders.

PART 1: WHY OPERATIONAL RESILIENCE?

Operational resilience is the ability of an organization to adapt to changing risk environments, and to manage the hazard risk that is inherent in day-to-day operations.

In business terms, operational resilience represents the organization's ability to protect its critical assets and keep its critical business processes and services up and running, even in the face of a disruption or security event.

Why is this an important topic for business leaders?

- The world is constantly changing in terms of risks and opportunities.
- It is no longer possible to react to all possible situations; leaders must know how their organizations are going to respond well in advance.
- In some market sectors (such as banking and finance), regulations are calling for this.

What is within the scope of operational resilience?

- operational risk
- failed internal processes
- fraud
- inadvertent and deliberate actions of people
- natural disasters (for example, hurricanes and tornadoes)
- terrorism

Most leaders today determine their current state of operational resilience based on what hasn't happened. This is neither sufficient nor particularly useful for predicting future response capability.

The scope of operational resilience as researched by CERT includes security, business continuity, disaster recovery, and IT service management. There is a great deal of commonality across these disciplines.

Important: Operational resilience (not security) is the goal. We do security to make business processes more resilient and to achieve the business mission. The same can be said for business continuity and IT services.

PART 2: DETERMINING HOW MUCH IS ENOUGH

So, how much resilience is enough? Determining the answer to this question is difficult and, in part, determined by the knowing the following:

- what industry we're in
- what we want to accomplish
- what the challenges are
- what our risk appetite is (what we're willing to accept and what we're not willing to accept)
- how we stack up against our peers and competitors

The winter 2007 incident involving JetBlue is a good example. How many planes could be grounded before the company's actions affected its reputation and business?

So, what are some first steps for getting started?

- Know what business you're in.
- Know what your strategic and business drivers are.
- Attach business processes and services to those drivers.
- Identify the assets associated with processes and services.
- Make sure these assets are adequately protected and can be sustained in the face of realized risk.

PART 3: RESILIENCY ENGINEERING: A PREVIEW

Resiliency engineering is the process by which an organization designs, develops, implements, and manages the protection and sustainability of business-critical services, related processes, and associated assets such as people, information, technology, and facilities.

In a nutshell, it's requirements-driven security and business continuity. These need to be considered in an integrated fashion, not as stovepipes, as they affect the same assets.

CERT is developing a framework for resiliency engineering that addresses many of the issues and disciplines discussed here. It addresses such competencies as defining asset requirements and identifying your suppliers and their contributions. It also includes:

- vulnerability management
- incident management
- technology management
- problem management

The goal is to create a repeatable, sustainable process for operational resilience that an organization can follow and that builds upon the Software Engineering Institute's core competency in continuous software process improvement.

The framework will incorporate process definitions that can produce meaningful metrics and measurement.

The framework will be compatible with other leading standards such as ITIL, COBIT, and ISO 27001.

Resources

Focus on Resiliency: A Process-Oriented Approach to Security Management

Basel Accord

BITS

COSO Committee of Sponsoring Organizations of the Treadway Commission

---