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

Managing Relationships with Business Partners to Achieve Operational Resiliency

Key Message: A defined, managed process for third party relationships is essential, particularly when business is disrupted.

Executive Summary

Ensuring operational resiliency, particularly during times of stress caused by natural disasters, market changes, service disruptions, and other unanticipated outages, is becoming more important for sustaining mission and business success. While resiliency is challenging to manage when all service providers are members of the organization, it becomes even more so as organizations depend on the services and products of external parties.

In this podcast, David White, Product Manager for CERT's Resiliency Management Model, discusses how to effectively manage relationships with business partners, suppliers, and other parties that are essential for ensuring operational resiliency.

PART 1: WHY ARE EXTERNAL RELATIONSHIPS INCREASINGLY IMPORTANT?

CERT's Resiliency Management Model

Two previous podcasts introduce CERT's RMM and its foundational concepts. They are as follows:

- Adapting to Changing Risk Environments: Operational Resilience
- Resiliency Engineering: Integrating Security, IT Operations, and Business Continuity

The model is structured as a capability maturity model, similar to the Software Engineering Institute's Capability Maturity Model Integration (CMMI).

RMM

- provides guidance to help organizations establish, manage, and sustain their operational resiliency activities
- builds upon operational risk management
- reflects a convergence of business continuity, information security, and IT operations
- is a process improvement model
- is descriptive, not prescriptive (addresses the "what," not the "how" although there many implementation examples are provided)

The Growing Importance of External Relationships

Increasingly, business leaders are contracting for skills, systems, data, equipment, and facilities with outside organizations. These can manifest as outsourcing arrangements, use of global supply chain partners, acquisitions, and other forms of business partnerships.

Given the pervasiveness of information technology, the boundaries between the buyer and provider often become quite blurred.

These "external dependencies" need to be actively managed to ensure the organization's operational resiliency.

PART 2: SET PRIORITIES; MANAGE RISKS

Top Four Goals

The top four goals of the External Dependencies Process Area within RMM are:

- Identify and prioritize external dependencies
- Manage risks due to external dependencies
- Establish formal relationships
- Manage external party performance

Setting Priorities

Some relationships are more important than others. Those with higher priority require greater attention, oversight, more resources, and may require more stringent performance measures.

An organization needs to determine what criteria to use when prioritizing external relationships. Cost may appear to be an obvious one, but it may not be the best.

In one case, cost was used as the primary factor, which resulted in an organization giving its paper products supplier the highest priority.

The Role of High-Value Services

Critical services are those whose disruption would affect the organization’s ability to achieve its mission.

A better way to prioritize may be to understand the extent to which an external party plays a key role in providing or supporting a high-value service.

Organizing external dependencies into tiers and then prioritizing them may make this process more manageable.

Normal Operations vs. Times of Stress

The priority of an external dependency may shift from day to day. It may have one priority during normal, unstressed operations but take on a greater priority during service disruption (such as for the provider of backup services or failover data center support).

Managing Risks

An external party’s financial condition can have an enormous impact on their ability to provide service.

Other risk areas to pay attention to include:

- availability of key personnel
- the external party’s dependence on other third parties
- unmet resiliency requirements (managed as residual risks)

PART 3: BUILD ROBUST CONTRACTS; MANAGE PARTNER PERFORMANCE; USE A PROCESS APPROACH

Establishing Formal Agreements

First and foremost understand your resiliency requirements that apply to all external parties and that are unique to a specific engagement.

Blanket requirements may include compliance requirements and background checks for staff that will have access to certain types of data.

Specific requirements, such as how quickly service is to be restored during an outage, are often captured in service level agreements.

Acquisition and procurement personnel may require some additional training to enhance their ability to elicit and specify a comprehensive set of resiliency requirements.

Contracts also need to address what recourse the organization has to correct external party performance under certain scenarios.

The priority of the external dependency will help inform how much time to invest in developing a robust contract.

Are Service Providers Performing as Expected?

The number one recommendation is to establish a standard procedure and make someone responsible for the relationship and for executing the procedure.

There may be different processes and different review frequencies based on the provider’s priority.

Monitoring performance includes inspecting deliverables (such as software or data) or testing a service under various scenarios in accordance with the service level agreement.

Assessments and Audits

For high priority relationships, regular audits should be part of the performance monitoring process. In addition, an audit or assessment should be part of the due diligence process when selecting an external party and developing a formal agreement.

The Advantages of a Defined Process

Having a process defined and implemented as part of normal, day-to-day business (institutionalized) ensures that all value-producing, mission-focused business processes continue to operate as intended.

The real test is being able to rely on a robust process during times of stress.

Resources

CERT’s Resiliency Management Model

Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook: Outsourcing Technology Services, June 2004.