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

Ensuring Continuity of Operations When Business Is Disrupted

Key Message: Providing critical services during times of stress depends on documented, tested business continuity plans.

Executive Summary

Historically, business continuity planning focused primarily on data processing. Today, it encompasses the technology, information, people, and facilities that are required to keep an organization up and running during times of stress and disruption. Critical services can be interrupted or curtailed by power outages, severe weather, fires, chemical spills, civil disturbances, and attacks by external intruders and malicious insiders. Involving all key stakeholders in enterprise-wide and business unit continuity planning and testing are essential for mission success.

In this podcast, Gary Daniels, Vice President and Director of Corporate Business Continuity Planning for Marshall and Ilsley, discusses the critical role of business continuity planning in support of operational resiliency. Gary provides a four step process for developing and testing a business continuity plan.

PART 1: THE INCREASING SCOPE AND IMPORTANCE OF BUSINESS CONTINUITY PLANNING

The Evolution of Business Continuity

Prior to 9/11, business continuity, disaster recovery, and services continuity generally referred to the recovery and restoration of data processing services – computer rooms, computers, and networks.

For the financial services sector, this limited focus was due, in part, to outsourcing technology to service bureaus where continuity of service was a service provider responsibility.

Today, business continuity has expanded to include not only technology but information, facilities, and people. If you focus on technology, you may find that there are no facilities and no people available to provide service. Similarly, if you neglect the recovery of information, people don’t have what they need to provide services.

Business Continuity and Information Security

Business continuity staff need to work closely with information security staff when developing recovery plans to ensure that:

- information is adequately protected as well as the facilities, hardware, and infrastructure which store the information
- firewalls and encryption at an alternate location operate identically to those at your primary location
- physical and information security controls at an alternate location (for example, access controls) replicate those at your primary location

---

PART 2: DETERMINING WHAT TO PROTECT; IDENTIFYING KEY PLAYERS

Prioritizing Processes, Services, and Assets

Historically, companies approached continuity planning by listing and attempting to address every type of outage such

as mechanical, weather-related by geographical location, and civil disturbances by country.

A key aspect of business continuity planning is planning for a total outage and then being in the position to implement only the part of the plan that applies to a specific type of outage.

Focusing on Scenarios versus Assets

When preparing people who have responsibilities for emergency response, a scenario-based approach tends to work best, for example, severe weather, fire, a power outage, or a chemical spill.

Alternatively, an asset-based approach works best when focusing on the recovery of a high priority business unit. You just need to get the business unit up and running, regardless of the cause of the disruption.

Gaining Buy-in from Key Players

You need to make sure you have the full support and endorsement from your board of directors and top executives. Without this support, business unit owners will not buy in because business continuity is an overhead expense which doesn't bring in revenue.

A business continuity steering committee can help prioritize which business units are most important.

Crisis management teams help determine when to declare a disaster and when to relocate people. They know how an outage can affect each business unit.

Representatives for each line of business are critical for ensuring that plans reflect their needs.

Today, most senior business leaders understand the impact of service disruption; they actively support continuity planning and exercises.

Enact Strong Governance

Governance includes defining the continuity program, setting policy, and assigning clear roles and responsibilities.

Involve Your Vendors

Once you have your plan defined and you identify critical suppliers, make sure suppliers participate in continuity exercises. This includes their participation in your exercises as well as your participation in theirs.

You need to ensure that suppliers can continue to provide service at your alternate location.

PART 3: DEVELOPING & EXERCISING BUSINESS CONTINUITY PLANS

Steps for Developing a Business Continuity Plan

1. Conduct a business impact analysis to determine which business units are most critical based on, for example, revenue production and service delivery.
2. The steering committee prioritizes business units based on the business impact analysis results.
3. Develop templates for recovery plans and have business unit representatives fill them out. Templates should include:
    a. procedures for call notification
    b. procedures for damage assessment
    c. procedures for moving to an alternate site including assets such as required systems and workstations
    d. vendor requirements

Exercise and Test Your Plan

Once you have a fully documented and approved plan, the next step is to conduct exercises to test the plan. These can include table top exercises, simulation, and full scale tests.

For a mission critical business unit, testing should occur two to four times per year. Less essential units and services can be tested once per year or every two years.

Testing ensures that an alternate site is equipped and fully able to support the business unit, for example, online access, workstations, systems, applications, help desk services, and phone service rerouting.

Testing includes performing daily functions at the alternate site to ensure they work as expected.

Increased Vulnerability

Once it becomes public knowledge that you've had a disaster, you may be viewed as being in a weakened position. Fraudsters may more easily learn how to access your backup systems. So you need to pay special attention to security controls at your alternate location.

Communications during an Event

You may want to consider forming a communication team to work with the media and press, and to keep customers informed.

Resources

Disaster Recovery Journal

Disaster Recovery Institute

Contingency Planning & Management

Continuity Insights

CERT Resiliency Management Model, specifically the Service Continuity process area.