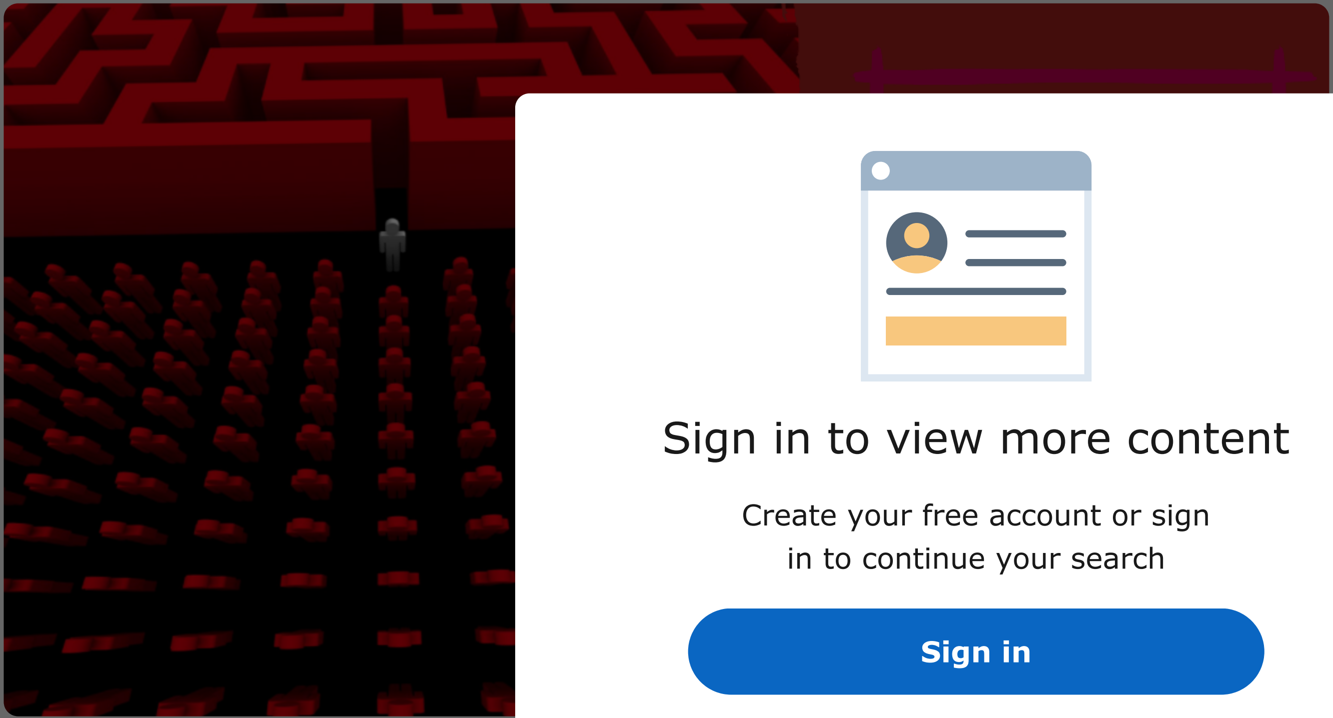

Clearing th among IRP DRP

Hashan Wickramasingha Wadanambi (H.W.W)

IT Infrastructure Specialist | IT Infrastructure Services Management | IT Project Management | Cybersecurity | ISO/IEC 27001 Information Security Internal Auditor | Scrum Master | Strategy Implementation Professional

+ Follow

Like Comment Share 8

nsights from the ommunity

IT Service Management

What are the common ITSCM gaps and how do you address them?

Business Continuity

How do you align your RPO with your recovery time objective (RTO) and service level agreement (SLA)?

From my observations, I've seen IT teams often getting stressed because of the confusion in distinguishing between the Incident Response Plan (IRP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). While it might appear that these plans overlap, they actually have distinct definitions and are three separate plans.

First, the Incident Response plan responds to abnormal operating conditions to keep the business operating. An incident is "An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.". In here the event is defined as "Any observable occurrence in a network or system" (Source: **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**).

The four major components of IRP are.

1. Preparation
2. Detection and Analysis
3. Containment
4. Eradication and Recovery
5. Post-Incident Activity

Incident response life cycle

Business Operations

What are the best ways to improve incident response capabilities with business continuity metrics?

Business Continuity Planning

How do you incorporate lessons learned from previous crises into your business continuity plan?

Business Continuity Planning

How do you incorporate RPO, RTO, and MTO into your risk management and contingency planning?

Contingency Planning

How do you integrate contingency planning testing with other business continuity and resilience activities?

Show more

Others also viewed

(source: **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**)

Below are the major tasks which are included in each phase of Incident response life cycle.

- **Preparation:**

o Develop a policy approved by management.

o Identify critical data and systems, single points of failure.

o Train staff on incident response.

o Implement an incident response team.

o Practice Incident Identification.

o Identify Roles and Responsibilities.

o Plan the coordination of communication between stakeholders with primary and secondary contacts.

- **Detection and Analysis:**

o Monitor all possible attack vectors.

o Analyze incidents using known data and threat intelligence.

The Proper Way of Assessing BCP/DR Readiness When Your Company is Performing an IT Security Risk Assessment on a New 3rd Party Vendor
Rocio Baeza · 3y

Business Continuity Planning in Today’s Everchanging World
Charlene Aldridge · 2y

Do you have a Business Continuity Plan (BCP)?
Ravindra Perera · 7y

Show must Go On ... So Should The BCP
Gautam Sarnaik · 7y

How to Determine Continuity needs using Recovery Point Objective (RPO) and Recovery Time Objective (RTO)
Eric Morano · 9y

By failing to prepare, you're preparing to fail.
Philippe Cornette · 2y

Show more

o Prioritize incident response.

o Standardize incident documentation.

- **Containment, Eradication and Recovery:**

o Gather evidence.

o Choose an appropriate containment strategy.

o Identify the attacker.

o Isolate the attack.

- **Post-incident Activity:**

o Identify evidence that may need to be retained.

o Document lessons learned.

The Business Continuity plan is designed to keep the organization operating through the crisis. When there is an event which has created a disturbance to the operation and if you need to find a way to maintain the business then the Business Continuity Plan (BCP) guides you.

The BCP mainly consists of the following components.

o List of the BCP team members, contact methods and secondary contacts when primary is not available.

Explore topics

Sales

Marketing

Business Administration

HR Management

Content Management

Engineering

Soft Skills

See All

o Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.).

o Notification systems and call trees for alerting personnel that the BCP is being enacted.

o Guidance for management, including designation of authority for specific managers.

o How/when to enact the plan.

o Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

At last, if both the Incident Response and Business Continuity plans fail, the Disaster Recovery plan is activated to return operations to normal as quickly as possible.

The general objective of the **DRP** is bringing the operation back to normal stage as quickly as possible. The DRP generally includes the components below.

o Executive summary providing a high-level overview of the plan.

o Department/Sector specific plans.

o Technical guides for IT personnel responsible for implementing and maintaining critical backup systems.

o Full copies of the plan for critical disaster recovery team members.

o Checklists on individual contributions and responsibilities.

I once performed a gap analysis on the infrastructure operations to develop an Infrastructure roadmap for an organization. Even if the plans like IRP, BCP, and DRP are written down, sometimes they're not really part of how things happen. So, even though they're written, it's a big problem when there's a real issue.

There was a time when ERP System in the organization was running slowly. The security and infrastructure teams were worried and trying hard to fix it. Everyone was making calls, and it was a stressful time for all the teams. As things got worse, four questions came up from both non-tech business users and senior leaders in infrastructure and security.

1. Why can’t we activate the disaster recovery plan?

2. Why can’t we stop applications from primary Data Center and spin out Apps from Disaster Recovery Data Center?

3. There is huge pressure from business, what can we do?

4. What else can we do as an alternative plan to run the operation?

After the teams resolved the issue, I scheduled a meeting to discuss this matter.

I asked the senior technical experts that I heard some of you were telling “Why can’t we activate DR plan? “. Then I received an answer saying, “no one took the responsibility for taking that decision”.

Next, I asked when we should activate the DR plan, then there was only silence.

Then I further asked where the DR plan is and then it was identified that most of the technical persons were not aware of the DR plan. But in the DR plan it is properly documented when to activate and how to proceed and the roles who are responsible for taking decisions.

Then after that as a team we started awareness sessions and initiated a journey of looking at these important factors.

In short, regularly checking the prepared plans like IRP, BCP, and DRP is crucial. It doesn't matter how well-written the documents are; what matters is putting them into practice. It should be a routine, normal practice in real situations, avoiding confusion and pressure.

This article aims to share industry experiences to help others learn from mistakes and improve their IRP, BCP, and DRP if they haven't been well-prepared. It underscores the importance of being aware of and effectively implementing these plans.

I would like to thank **https://www.isc2.org/** for the knowledge that was produced and listening to a podcast between **Chad Kliewer** and Daniel Hernandez on Incident Response Priorities motivated me to write this article.

Further I believe a vision of sharing knowledge and experiences with others makes a world a better productive place as I have learnt a lot from others. Therefore I value sharing knowledge with others and learn from others.

To view or add a comment, **sign in**

More articles by this author

Have we identified what digital…
Feb 3, 2024

The Future Of IT Departments
Jan 19, 2024

The Untold Story of Kangoo Jumps Quee…
Dec 31, 2023

See all