Lab: Cyber Resilience Playbook Mapping

Module: Data & Cyber Resilience
Duration: 1.5 Hours

Overview

In this lab, you will take on the role of a **cyber resilience task force** responsible for building a **Cyber Resilience Playbook** that connects cybersecurity, incident response, and business continuity practices.
Your goal is to map out a structured framework showing how cyber events are managed — from detection to recovery — ensuring the organization remains operational during disruptions.

This exercise directly supports your preparation for **DRI International certifications (ABCP, CBCP, ACRP, CCRP)** by bridging cybersecurity operations and resilience planning into a unified strategic framework.

Scenario

You are part of the **Cyber Resilience Division** at **NovaTech Systems**, a global logistics technology provider.
The company recently faced a ransomware incident that temporarily disrupted supply chain operations.
While the cybersecurity team contained the threat, leadership realized there was **no integrated playbook** connecting cybersecurity, continuity, and recovery actions.

You have been assigned to create a **Cyber Resilience Playbook Map** that illustrates how NovaTech can align technical response actions with organizational resilience strategies.

You have **1.5 hours** to research, design, and present your playbook map.
You may use **Google** or other online sources to gather best-practice models and examples.

Your Task

Work in **teams of 3–4** to design and document a **Cyber Resilience Playbook Map**.
This playbook will serve as a visual and strategic guide for coordinating cybersecurity and business continuity functions.

Your deliverable is a **Google Slides presentation** that explains:

1. The structure of your playbook (sections, roles, and workflows).
2. How cybersecurity and continuity teams coordinate during incidents.
3. Key actions from detection to recovery.
4. Metrics and governance for maintaining resilience maturity.

Step 1: Define the Purpose of the Playbook

Begin by answering these questions:

- What is the purpose of the Cyber Resilience Playbook?
- Which teams and functions are involved?
- How does it align with organizational continuity and governance goals?

State your objectives clearly in the introduction of your slides.

Step 2: Map Cyber Resilience Phases

Structure your playbook using **five key phases**:

1. **Preparation:** Roles, contacts, tools, and readiness activities.
2. **Detection:** Monitoring, alerts, and identification of threats.
3. **Response:** Containment, communication, and mitigation.
4. **Recovery:** Restoration of systems, data, and operations.
5. **Post-Incident Review:** Lessons learned and improvement cycles.

Include visual flowcharts or diagrams that show how teams transition between each phase.

Step 3: Integrate Continuity and Recovery Actions

Show how your playbook connects to the organization’s **business continuity plan (BCP)** and **disaster recovery plan (DRP):**

- Align IT recovery steps with resilience objectives.
- Include RTO/RPO targets.
- Identify decision-making authority during incidents.
- Define escalation and communication procedures.

Step 4: Define Roles and Responsibilities

Assign responsibilities for each phase, such as:

- **CISO / Cyber Lead:** Approves escalation and external communication.
- **IT Operations:** Executes containment and recovery tasks.
- **Continuity Manager:** Ensures business processes remain active.
- **Communications Lead:** Coordinates internal and external messaging.

Summarize roles in a clear RACI-style chart or responsibility matrix.

Step 5: Add Metrics and Governance Elements

Include measures to evaluate the playbook’s effectiveness:

- **MTTD (Mean Time to Detect)**
- **MTTR (Mean Time to Recover)**
- **Number of successful incident drills**
- **Compliance audit success rate**

Also, define governance cadence:

- Frequency of reviews
- Ownership of updates
- Required training or simulations

Step 6: Present Your Cyber Resilience Playbook Map

Deliver a **10-minute presentation** that includes:

- Your visual playbook map (phases, workflows, and roles)
- Explanation of how it integrates with resilience and continuity frameworks
- Key metrics and improvement actions

Each team member should explain part of the playbook or decision process.

Evaluation Criteria

Category	Description	Points
Structure & Clarity	Logical flow and organization of playbook phases	25
Integration with Resilience	Links between cybersecurity, continuity, and governance	25
Governance & Metrics	Clear measures, accountability, and improvement cycle	25
Presentation & Teamwork	Clear visuals, collaboration, and communication	25

Total: 100 points

Expected Outcome

By the end of this lab, your team will have:

- Developed a **Cyber Resilience Playbook Map** showing coordination between cybersecurity and resilience.
- Identified clear **roles, responsibilities, and workflows**.
- Integrated **continuity and recovery actions** into cyber response planning.
- Strengthened your understanding of **cyber resilience governance and metrics.**

Key Takeaways

- Cyber resilience bridges security, continuity, and recovery.
- A structured playbook provides clarity during high-stress events.
- Metrics enable organizations to measure readiness and improvement.
- Governance ensures accountability, alignment, and sustainability.