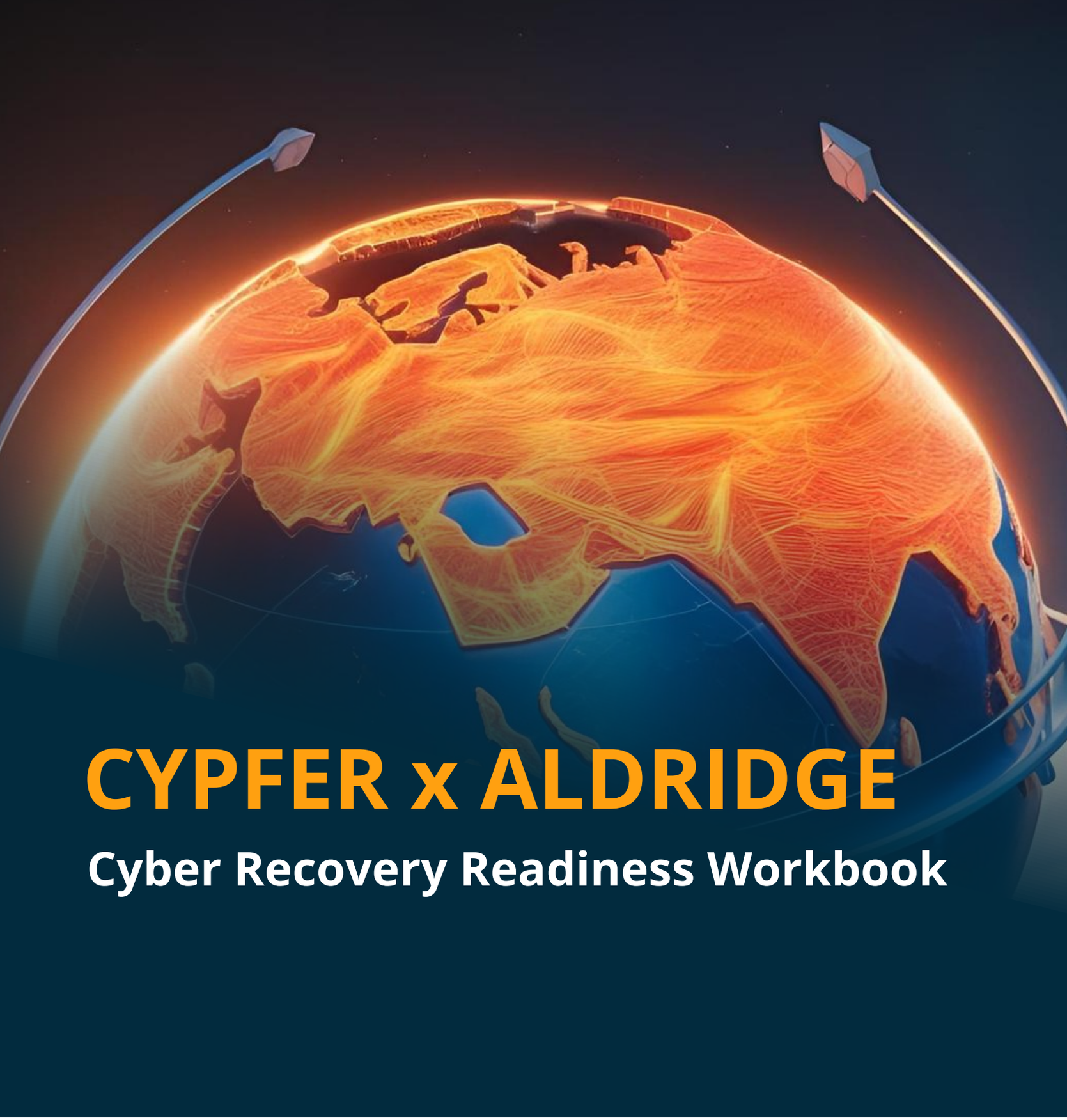

CYPFER x ALDRIDGE

Cyber Recovery Readiness Workbook

GLOBAL EMERGENCY CYPFER RESPONSE

ALDRIDGE

INTRODUCTION

This hands-on guide is designed to help assess your organization's cyber recovery readiness, identify critical gaps, and shape a structured approach to resilience.

It's not a step-by-step action plan but a starting point, a tool to initiate the critical conversations necessary for effective recovery. Use it to document your current state, outline recovery processes, and refine your strategy.

Cyber resilience is an ongoing journey, and this workbook is here to help you take the first steps toward strengthening your organization's ability to recover and adapt in the face of cyber threats.

1. QUICK READINESS ASSESSMENT

Current State of Preparedness

On a scale of 1-10, how prepared is your organization for a cyber incident?

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

Do you have an up-to-date incident response plan?

❑ YES ❑ NO

Note: make sure that you have a printed copy of it in case your systems become unavailable.

Does your IR plan identify all parties that might need to be involved (e.g. executive leadership, internal/external IT staff, IR/Recovery company, cyber insurance carrier, inside/outside counsel and etc) along with their point of contacts?

❑ YES ❑ NO

Note: the IR plan should also define an alternative communication methods in case your corporate email, messaging and/or VOIP phone solutions would get compromised.

When was your last tabletop exercise conducted?

Date: DD/MM/YYYY

QUICK READINESS ASSESSMENT

Current State of Preparedness

Do you have defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)?

→ RTO: _____

→ RPO: _____

Note: RTO (Recovery Time Objective) is the maximum downtime your business can tolerate, while RPO (Recovery Point Objective) is the maximum data loss acceptable before impacting operations.

Do you have a Cyber insurance policy?

❑ YES ❑ NO

Note: ideally your cyber insurance policy documents shouldn't be stored electronically – typically it's the first document that cyber criminals are searching for.

Who has the authority to initiate recovery procedures?

Name / Title

Note: Keep in mind that recovery efforts should not compromise digital forensics evidence until it's properly collected to avoid unnecessary legal, data mining and/or notification expenses.

2. INCIDENT RESPONSE & RECOVERY TIMELINE

Exercise

Review the following **real-world breach scenario** and complete the questions below.

Scenario

*An employee receives what appears to be a legitimate Microsoft Teams call from the CEO requesting urgent action on a confidential business matter. The voice, video, and context are highly convincing; however, the executive is an **AI-generated deepfake** designed to steal funds, credentials, or proprietary data. The employee shares sensitive information and approves an action that results in initial unauthorized access to internal systems, giving attackers a foothold in the environment.*

Response Planning Questions

1. **What verification processes, approval controls, and employee training would your organization rely on when voice, video, and written communications can no longer be trusted as proof of identity?**

   Step 1: _____
   Step 2: _____
   Step 3: _____

2. **What internal and external teams need to be notified immediately?**

   - Internal Teams:
   - External Teams:

3. **How will you ensure continuous communication during the incident?**

   Response:

3. Data Recovery Workbook

Data Protection & Restoration

What data is most critical to recover first? (Rank top 5)

1: _____
2: _____
3: _____
4: _____
5: _____

Do you have immutable backups?

❑ YES ❑ NO

Where are backups stored?

On-prem | Cloud | Air-Gapped | Offline

Other:

When was the last test recovery performed?

Date: (DD/MM/YYYY)

Outcome:

Who is responsible for backup validation?

Name / Title

4. Business Continuity & Ransomware Decision-Making

Exercise
Fill in your organization's approach.

Do you engage with law enforcement?

❑ YES ❑ NO

WHY:

Do you have a pre-approved ransomware payment policy?

❑ YES ❑ NO

Who decides whether to pay a ransom?

Name / Title

What is your crisis communication plan for internal and external stakeholders?

Response:

If systems remain locked for 48 hours, how will operations continue?

Response:

5. RECOVERY TEAMS & ROLES

Defining Responsibilities

Exercise

Fill in your organization's approach.

Who leads recovery efforts?

Name / Title

Who is responsible for communications?

Internal:

External:

What vendors are pre-approved for recovery assistance?

Response:

Does your cyber insurance policy include recovery costs?

❑ YES ❑ NO

6. ATTACK SURFACE & LESSONS LEARNED

Self-Assessment

What was the root cause of your last security incident?

Response:

What tools are missing from your current recovery toolkit?

Response:

What are the biggest barriers to fast recovery?

Response:

What are the top 3 improvements you will make post-session?

1: _____
2: _____
3: _____

7. ACTION PLAN & TAKEAWAYS

Your 30-Day Recovery Action Plan

Action Item	Owner Deadline Status
Improve backup testing frequency	
Conduct a ransomware tabletop exercise	
Update incident response contacts	
Review cyber insurance coverage	
Document third-party recovery support	

This workbook is designed to be a living document — continuously updated to reflect your organization's evolving cyber recovery strategy. Use this as a foundation to strengthen your cyber resilience and ensure rapid recovery from incidents.

GLOBAL EMERGENCY CYPFER RESPONSE

WWW.CYPFER.COM

ALDRIDGE

WWW.ALDRIDGE.COM