What Happens If

Tabletop Methodology and Live Exercise

IT NATION™ SECURE

Matt Topper

Senior Evangelism Director, ConnectWise

- 12+ MSP Years
- Infrastructure, Architecture, Projects, Security
- 2 Software Companies
- Created /r/msp
- CISSP, CISM, CCSP
- Contact
  - matt.topper@connectwise.com
  - linkedin.com/in/matthew-topper

A Time Capsule

Choices

image: Freepik.com

Activity Types

- Walkthrough
- Tabletop
- Functional
- Live Fire

A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

TRANSLATION:

Ask and Answer: *What Happens If?*

Basic Process

Travel Nightmare

You are the service manager.
What happens if... A tech notifies you that their laptop was stolen from their hotel room.

We respond by:

- Notify hotel security
- Verify that it was encrypted
- See whether it's communicating
- Issue a wipe command
- Following the IR Plan

Common Pitfalls

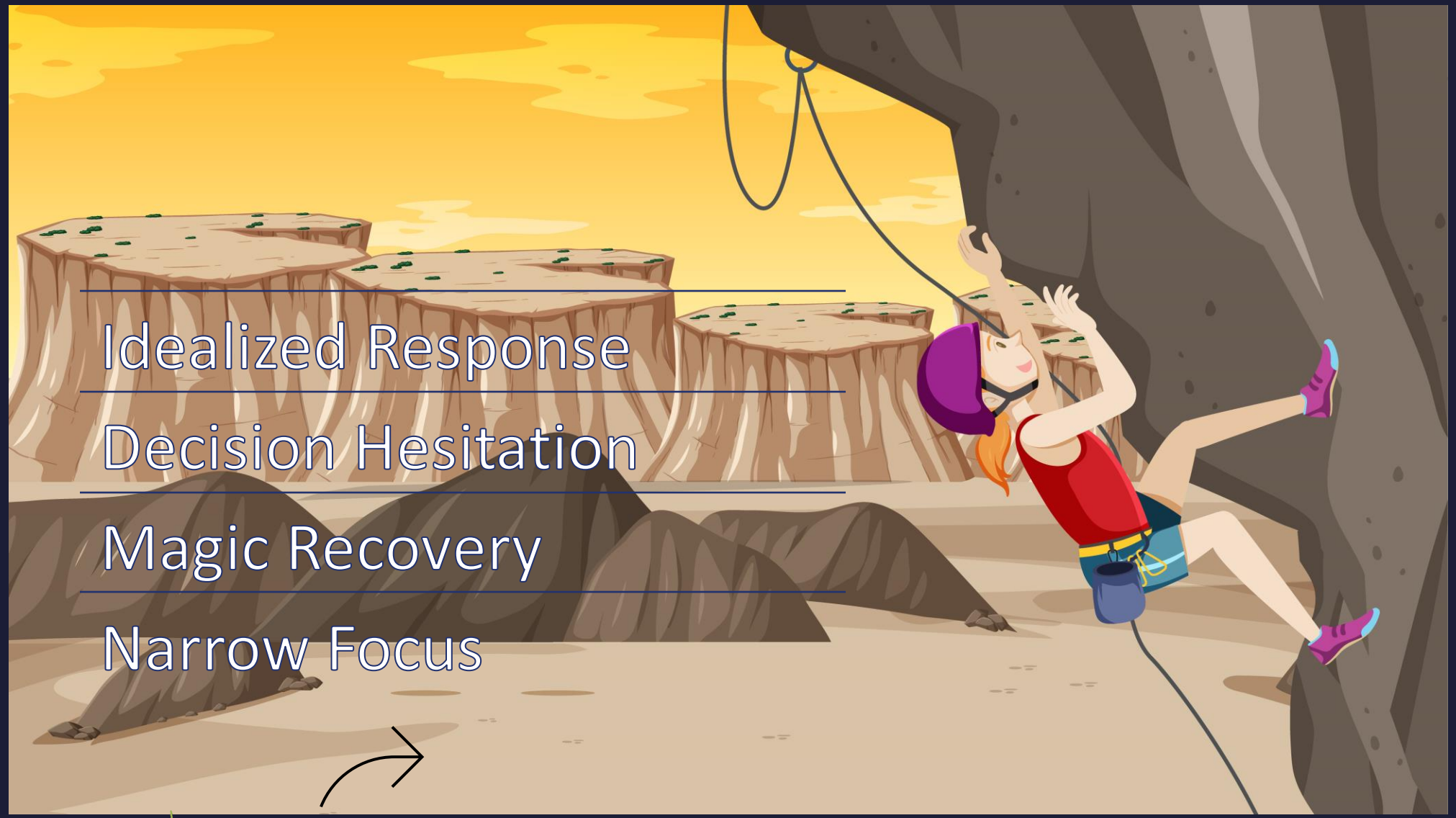

image: Freepik.com

Formal Methodology

Design	Development	Conduct	Evaluation
Planning and Preparation Steps	Coordinate Logistics	Execute the Exercise	Realize Value by Improving
Identify Scope	Create Documents:	Brief participants	Debrief
Select Participants	Briefing	Introduce Scenario	Write Report
Nominate Facilitator	Facilitator Guide	Initiate Discussion	Lessons Learned
Choose Scenarios	Participant Guide	Ask Questions	Present Findings
Schedule	Report Template	Collect Data	Update Plans

Business Email Compromise

You are the service manager.
What happens if... You receive an internal email with a malicious link.

We respond by:

- Messaging the security guy in Teams
- Resetting the user's password
- Deleting the email and moving on because we only accept support via tickets
- Ending all sessions, investigating other activity on the account, and resetting credentials
- Following the IR Plan

Response Dependency Chain

Endpoint Excitement

You are the service manager.

What happens if... A tech at your own company has a ransomware note pop up on his screen?

We Respond By:

- Isolate the system
  - How? Is evidence preserved?
- Revoke access
  - Who does this? Are you sure *that* account is secure?
- Investigate other systems for activity
  - Do you need a forensics firm? Do you have in-house expertise?
- Compensating actions.
  - Reset passwords? Notify clients?
- Following the IR Plan

Communication Breakdown

Password Manager Compromise

You use a web-based hosted password manager.
What happens if... The provider suffers a security incident that exposes credentials.

We respond by:

- Resetting all passwords
  - Who? How? Where are they recorded? Who decides to do that?
- Notifying clients
  - How? Who does it? Are you exposing yourself to liability?
- Reviewing all systems
  - Are your logs *that* good? Do you have forensic skills on staff?
- Engaging a third-party incident response service
  - Do they have capacity? Is insurance involved?

Service Providers

- Surges
- Access
- Alternatives

Bonus Round

You are the security director

What happens if... A threat actor gains access to an admin-level account in your RMM.

We respond by:

- Panicking
- Shutting down access
  - How? Has this been tested?
- Reviewing activity logs for the account
  - Are you sure there's a trail?
- Engaging a third-party incident response firm
  - Do they have capacity?
- Following the IR plan

Don't forget to fill out your

SESSION SURVEY