Surviving a Mock Disaster Building an effective Tabletop Exercise

May 2019 – Secure360 Conference

Ken M. Shaurette
CISSP, CISA, CISM, CRISC, NSA IAM
Director InfoSec and Audit

2019 Special Olympics Polar Plunge - Wisconsin

2017 This Is What Happens In An **Internet Minute**

- facebook — 900,000 Logins
- Google — 3.5 Million Search Queries
- NETFLIX — 70,017 Hours Watched
- $751,522 Spent Online
- 1.8 Million Snaps Created
- 15,000 GIFs Sent via Messenger
- 120 New Accounts Created — Linked in
- 50 Voice-First Devices Shipped — amazon echo
- 40,000 Hours Listened — Spotify
- 156 Million Emails Sent
- 990,000 Swipes — tinder
- 452,000 Tweets Sent
- 46,200 Posts Uploaded — Instagram
- 342,000 Apps Downloaded — Google play / App Store
- 4.1 Million Videos Viewed — YouTube
- 16 Million Text Messages

Created By:
@LoriLewis
@OfficiallyChadd

2018 This Is What Happens In An **Internet Minute**

- facebook — 973,000 Logins
- Google — 3.7 Million Search Queries
- NETFLIX — 266,000 Hours Watched
- $862,823 Spent Online
- 2.4 Million Snaps Created
- 25,000 GIFs Sent via Messenger
- 38 Million Messages
- 67 Voice-First Devices Shipped — amazon echo
- 936,073 Views — twitch
- 187 Million Emails Sent
- 1.1 Million Swipes — tinder
- 481,000 Tweets Sent
- 174,000 Scrolling Instagram
- 375,000 Apps Downloaded — Google play / App Store
- 4.3 Million Videos Viewed — YouTube
- 18 Million Text Messages

Created By:
@LoriLewis
@OfficiallyChadd

Objectives

- Identify the major components for BCP/DR.

- Understand the types of Testing.

- What is a Script versus a Scenario?

- Why is a timeline script important?

- Ties to Incident Response.

SECURE360
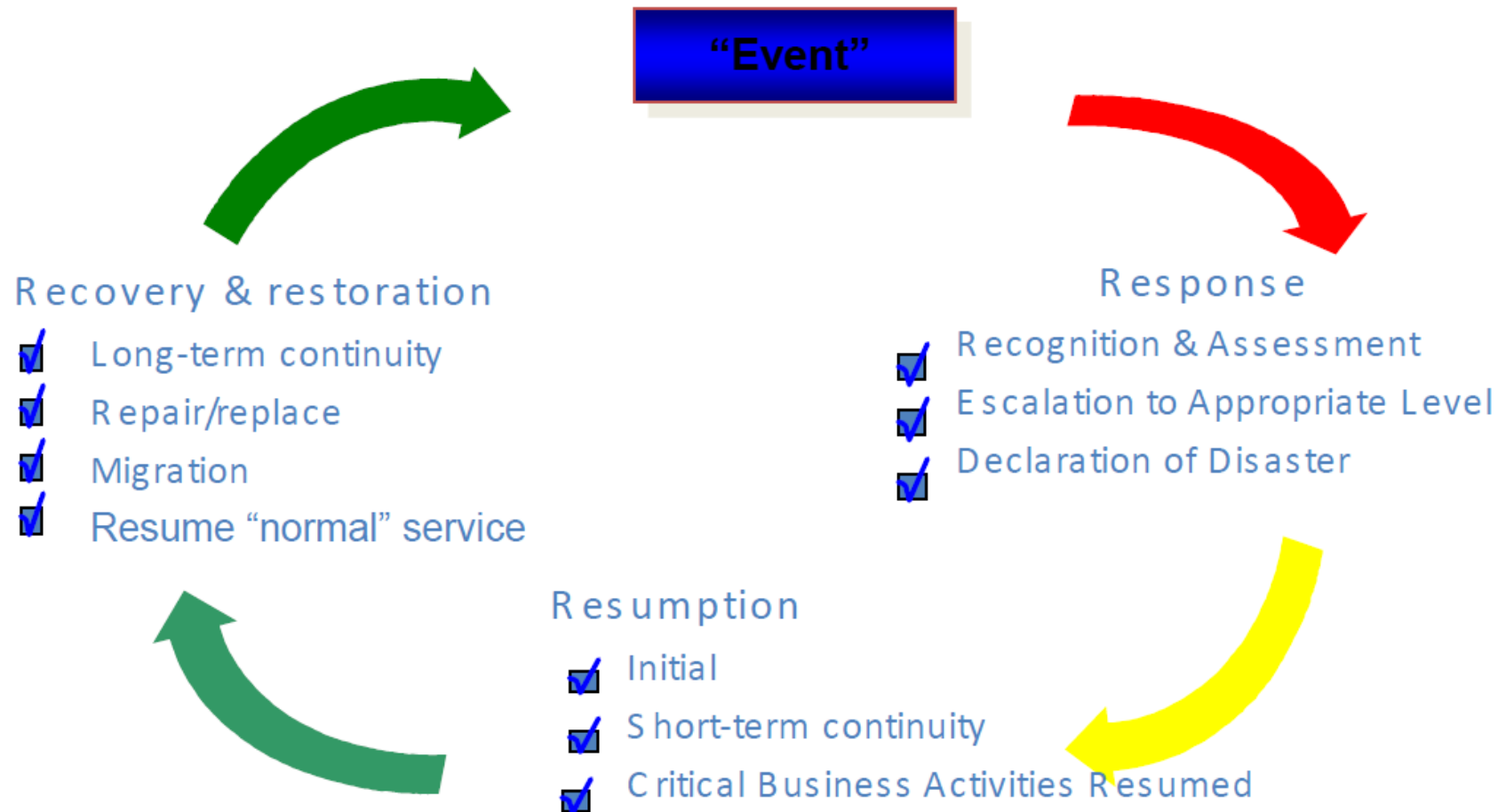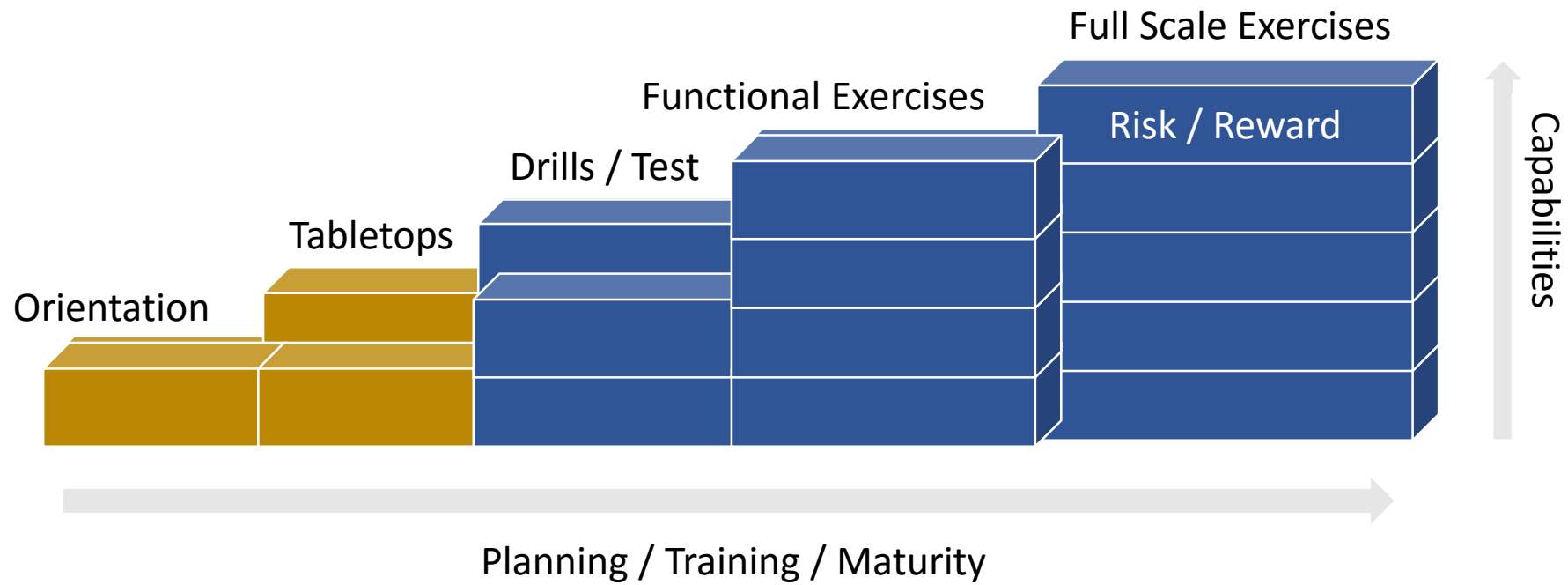Twin Cities

Strategy

Who Facilitates

Publish Updates

Develop Test Training & Exercise Plan → Develop Exercise Plan → Develop Materials

Conduct Exercise → Evaluate Exercise → Update BCM Plan

Revised BCM Plan

Business Continuity Cycle

"Event"

Recovery & restoration
- ☑ Long-term continuity
- ☑ Repair/replace
- ☑ Migration
- ☑ Resume "normal" service

Response
- ☑ Recognition & Assessment
- ☑ Escalation to Appropriate Level
- ☑ Declaration of Disaster

Resumption
- ☑ Initial
- ☑ Short-term continuity
- ☑ Critical Business Activities Resumed

Ongoing Multi-Year Testing

Full Scale Exercises

Functional Exercises

Drills / Test

Tabletops

Orientation

Risk / Reward

Capabilities

Planning / Training / Maturity

Discussion Based

Operations Based

Secure360.org

#SEC360

Types of Tests

Exercise Type	Description
Orientation	A seminar and/or briefing activity used to familiarize participants with BCM responsibilities
Test or Functional Drill	Coordinated, supervised activity normally used to test, develop, or maintain skills in a single operation or function in a single office or organization
Tabletop Exercise	Simulates emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing BCM plan and individual state of training and preparedness
Functional Exercise	Used to validate the capability of an organization to respond to a simulated emergency, in order to test one or more functions of the plan
Full Scale Exercise	Simulates an actual emergency; intended to evaluate operational BCM procedures and capabilities under simulated stressful conditions

Combination Test

ALL OUT TEST

Defining Roles and responsibilities

Position	Roles and Responsibilities
DR/BCP Coordinator / Information Security Officer	• Coordinate schedule / Exercise facilitator
Management Team	• Provide guidance and approval of Exercise Plan
IT – Manager / Network Admin	• Coordinate IT Recovery Plans • Plan and conduct IT Tests • Support BCP Coordinator in Development and exercising
Participants (all employees, DR/BCP Team, Business Area Managers/SME)	• Member of recovery team • Familiar with Plan • Know assignments • Perform specific business duties

Functional and Full Scale Tests

- IT Recovery - test restore of technology, (i.e. data, network)

- Going offsite to a backup location tests recovery site preparedness, communications and utilities

- Trained and informed personnel are typically performing recovery steps

- Transaction testing verifies restore, connectivity and access using a person that knows the business process

- Community resources may be involved

What verifies the completeness of the Plan?

Why Tabletop Exercises?

Provide a forum for the following:

- Team Building
- Validate the Plan Documentation
- Information Collection and Sharing
- Obtain consensus from team
- Evaluation of Differing Perspectives
- Practice makes Easier

Why Tabletop Exercises?

Provide a forum for the following:

- Check that functional testing occurs

- Problem solving of complex issues

- Test considerations for new situations, ideas, processes and/or procedures

- Training/Awareness for management and staff

Exercise Development Steps

Goals and Objectives –

What will success look like?

(SMART)

- <u>S</u>imple (concise)
- <u>M</u>easurable (how to document)
- <u>A</u>chievable (can this be done)
- <u>R</u>ealistic (and challenging) (can it happen)
- <u>T</u>ask Oriented (fits to business functions)

Exercise Development Steps

Scope:

- Exercise Activities
- Departments Involved
- Hazard - Type of Threat Source
- Geographic or outage Impact Area
- Staff Impacted
- Facilities Impacted

Exercise Development Steps

Building a Script from a Scenario

Threat Risk Asmt

- Choosing a Threat to Test
    - Vulnerability – Threat Assessment
- Start with simple basic scenarios – basic Fire minimal damage

Note: For example tornado incidents in the Midwest increased awareness of their threat risk.

The state may provide ongoing tasks of planning, preparing, and training for Tornado preparedness.

Secure3

360
ies

Threat Risk Assessment

Threat·Description¤	High¤ Medium¤ Low·¤ °¤	High¤ Medium¤ Low·¤ °¤	High¤ Medium¤ Low·¤ °¤	Risk↵ Rating¤
Accidental·explosion—·off-site¤	°¤	°¤	°¤	°¤
Accidental·explosion—·on-site¤	°¤	°¤	°¤	°¤
Aircraft·crash¤	°¤	°¤	°¤	°¤
Ancillary·equipment·failure¤	°¤	°¤	°¤	°¤
Arson¤	°¤	°¤	°¤	°¤
Bomb·threat¤	°¤	°¤	°¤	°¤
Bombing¤	°¤	°¤	°¤	°¤
Central·computer·equipment· failure¤	°¤	°¤	°¤	°¤
Computer·Intruder¤	°¤	°¤	°¤	°¤

Exercise Development Steps

Using a Scenario and Building a Script

- As your DR/BC matures - make scripts more complex – increase maturity, add advanced "INJECTS"

- Consider the unexpected – not could it happen, but what if it did.

- Don't share the scenario before the exercise

- Does the DR/BCP Team always know when a tabletop will occur?

Exercise Development Steps

Building on a Scenario

- How quickly can you pull together key Business Team Members?

- How quickly can all key individuals be contacted and mobilized to the alternate location?

- Do you test the involvement of any outside parties? (i.e. law enforcement, safety, utilities, telephone, ISP

Exercise Development Steps

Objectives of Exercise

Tabletop Exercise Program Objectives

- To improve operational readiness by demonstrating knowledge of the DR/BCP Plan overall

- To improve Company-wide coordination and response capabilities for effective disaster response

- To identify communication pathways and problem areas between IT, outside entities (utilities, media) business areas, regional and state emergency operations centers

- To establish timely response for safety, recovery and restore to normal operation.

Tips for an Effective Tabletop

- **Decide how much gloom and doom you want.**
  - Do you want this to be a physical event with assets damaged and destroyed,
  - Do you just want things inaccessible?
  - Do you want death and injuries, or just to test the ability to get work up and going someplace else?
  - Do you test unavailable key people?
  - How long will your downtime duration be?

Conducting the Exercise

- Set the Ground Rules
  - Silence Cell Phones
  - Establish timelines – Maximum 4 Hours - breaks, lunch etc..
  - Has Internal Audit been invited?
  - Who leads the exercise?
    - Can they facilitate and participate.
  - Consider issues that need to be tabled for later discussion

Conducting the Exercise

- Set the Ground Rules (cont...)
  - Accept the Scenario as Real
  - Stay in the Scenario - stay in the mindset that the disaster is really occurring
  - Who will take notes – record issues / follow-up
  - Consider taping the exercise on an audio recorder

Exercise – Evaluate - Update

- Planned Test scheduled in advance
  - Attendance by all BCP Team required
  - Team is aware of test scenario
- Document Team Member Attendance
- Confirm that all Team Members have their own up-to-date copy of the plan
- The BC/DR coordinator confirms updates are in the plan.

Exercise – Evaluate - Update

- Review policies and procedures

- Discuss business area changes since last updates – detail continuity procedures

- Confirm accuracy of phone numbers

- Verify Secure and accessible storage of plan (at home)

- Executive summary of the test and discussion results

TIP

Experience has shown that well planned and interesting exercises yield a high level of preparedness with personnel who are able to better cope with the stressful environment of an actual emergency.

Resources

- NIST SP800-84 - Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (google it)

- Homeland Security Exercise and Evaluation Program (HSEEP) hseep.dhs.gov, FEMA: www.ready.gov/

- National Incident Management System (NIMS: https://www.fema.gov/national-incident-management-system

- Emergency Management for Your State emergencymanagement.wi.gov/

- CSOonline Business Continuity, https://www.csoonline.com/resources/

- FIPCO, www.fipco.com/itservices

If Time Allows,
if not:

https://www.fipco.com/solutions/it-audit-security/cyber-security-resources-links

Sample Tabletop Exercise Testing

FIRE

CLICK HERE

STORM

CLICK HERE

Cyber Incident

CLICK HERE

Secure360.org

SECURE360
Twin Cities