Cuyahoga County
Together We Thrive

OCITA CYBER THREAT LIVE

Resources & Table Top Exercise Example

March 9, 2017

Jeremy Mio
Information Security Officer – Security & Research

What is the MS-ISAC

CIS Center for Internet Security®

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments. The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.
  - **FREE**
  - **Sign up https://msisac.cisecurity.org/members/register/**
  - **Contact 24x7** 1.866.787.4722 or emailing soc@msisac.org
- MS-ISAC Workgroups:
  - **Business Continuity, Recovery, and Cyber Exercise**
  - Cyber Security Metrics
  - Education and Awareness
  - Intelligence and Analysis
  - Legislative and Compliance
  - Mentoring Program

Instructions

1. Break the scenario into meaningful learning points.
2. Read the scenario aloud to the group and ensure their understanding.
3. Proceed to the discussion page to facilitate a conversation about how your organization would handle the scenario, focusing on the key learning points as you discuss.

These are intended to be brief exercises that take approximately 15 minutes on average.
Take note of the questions being asked and the scope of the exercise.
Use the After Action Report along with these exercises to identify any potential gaps in your Business Continuity Plan or your Security Policies.

DO:

- Designate a single individual to facilitate.
- Be sure to include applicable members of other business units.
- Follow the discussion guide on the final slide.

DON'T:

- Stray from the scope of the exercise. (You may want a designee to keep the group on track.)
- Forget to follow up on any gaps identified during the exercise. An After Action Report Template is available on HSIN.

February 2017 Scenario

Your organization is located within a flood zone. Winter weather with warming has caused flooding throughout your area. Your 911/EOC has declared a state of emergency. In the midst of managing the disaster, a ransomware attack occurs on your EOC/911 Center making the computer systems inoperable.

What is your response?

Discussion

NIST Functions Addressed: ID.AM-3: Organizational communication and data flows are mapped; ID.BE-5: Resilience requirements to support delivery of critical services are established; PR.PT-4: Communications and control networks are protected

- Do you have a COOP or a DRP that you can use in this case of flood?
  - If you do, do you carry out a tabletop or simulation annually?
- Do you have an IRP that specifically details ransomware steps?
  - What steps will you take if restoring from backup is not an option?
  - Does your IRP only take into account the financial implications, or does it consider the severity of the situation as well?
  - Do you have a plan in place for how to acquire bitcoin?
  - Have you considered that a targeted ransomware attack may require more bitcoin than is easily accessible on the market?
- Do you have a backup for completing EOC processes without a computer system?
  - Are there alternate or neighboring entities that emergency communications/processes can be routed through?
- Who do you need to notify, and how will you do so? Consider that increased phone traffic may be congesting the lines.

Business Continuity, Recovery, **and Cyber Exercise**

[Insert Organization Logo]

After Action Report Number _____	Exercise Name: _____ Date: _____		
Exercise Summary: _____			
Participants			
Facilitators	Players		Observers
Objectives: 1. – X _____			
Notes for Objective 1 _____ _____	Notes for Objective 2 _____ _____	Notes for Objective 3 _____ _____	
Major Strengths 1.	Areas for Improvement 1.		
Short Term Recommendations			
Recommendation	Lead	Priority	Due Date
1.			
Long Term Recommendations			
Recommendation	Lead	Priority	Due Date
1.			
Reviewed By _____ Signature			_____ Date

AFTER ACTION REPORT

- Keep Track of who was involved
- Observers are sometimes the best: Think HR, Business Units, Insurance, Auditors, etc.
- **Always Document MAJOR Strengths** it can be depression if you do not!
- The **MOST IMPORTANT** is both Short Term and Long Term recommendations! Then keep track of them.
- Always have a sign off or even a few to sign off, more so for the approval/backing of Recommendations


why
when
who
where
what
why
QUESTIONS
who
how
where
who
what
how
how