Cyber Security Tabletop Exercise

After-Action Report/Improvement Plan (AAR/IP)

Campus Resilience Program Exercise Starter Kit

October 23, 2018

HANDLING INSTRUCTIONS

The title of this document is the *Cyber Security Tabletop Exercise (TTX) After-Action Report/Improvement Plan (AAR/IP)*. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, is prohibited without prior approval from the exercise planning team. This document has been marked as "FOR DISCUSSION PURPOSES ONLY."

For more information on this exercise, please consult the following point of contact:

Cheryl Dowd
Cyber Fellow
WICHE
WCET
(303)541-0210
cdowd@wiche.edu

TABLE OF CONTENTS

OVERVIEW

Exercise Name	Cyber Breach Tabletop Exercise
Exercise Date	10/23/18; 9:00 AM – 11:00 AM
Scope	This exercise is a discussion-based "abridged" tabletop exercise, planned for two hours at the WCET Annual Meeting Precon. Divided into three Modules, this exercise will examine response and recovery operations related to a cyber breach targeted against institutional data.
Mission Areas	Response and Recovery
Objectives	1. **Operational Coordination:** Assess the ability to establish an effective command structure that integrates all critical stakeholders to ensure campus and community resources are used efficiently to respond to and recover from a cyber incident 2. **Cybersecurity:** Evaluate existing capabilities to protect and restore electronic systems, networks, information, and services from damage, unauthorized use, and exploitation during a cyber incident 3. **Situational Awareness:** Examine the ability to provide timely and relevant information regarding the cyber incident to critical campus and community decision-makers 4. **Public Information and Warning:** Assess the ability to deliver coordinated, actionable, and timely information to critical partners and stakeholders when faced with a cyber incident targeting institutional operations
Scenario	The exercise scenario will include a cyber breach that results in the compromise of personal and institutional data.
Participating Groups/Departments	▪ **WICHE** – **WCET** ▪ **Cooley, LLP**
Sponsoring Organization	WCET
Point of Contact	Cheryl Dowd, Cyber Fellow, WICHE (303)541-0210, cdowd@wiche.edu

ANALYSIS OF CORE CAPABILITIES

Operational Coordination

Assess the ability to establish an effective command structure that integrates all critical stakeholders to ensure campus and community resources are used efficiently to respond to and recover from a cyber incident.

Strengths

The following strengths were observed throughout the exercise related to Operational Coordination:

Strength 1: [Insert relevant observations, findings, and/or conclusions.]

Strength 2:

Strength 3:

Areas for Improvement

The following areas for improvement were identified throughout the exercise related to Operational Coordination:

Area for Improvement 1: [Insert relevant observations, findings, and/or conclusions. This should clearly state the problem or gap and should include a root cause analysis or summary of why this particular component of the core capability was not achieved. References to specific plans, policies, procedures, regulations, or laws are also recommended. Specific recommendations or corrective actions should be documented in the Improvement Plan.]

Area for Improvement 2:

Area for Improvement 3:

Cybersecurity

Evaluate existing capabilities to protect and restore electronic systems, networks, information, and services from damage, unauthorized use, and exploitation during a cyber incident.

Strengths

The following strengths were observed throughout the exercise related to Cybersecurity:

Strength 1: [Insert relevant observations, findings, and/or conclusions.]

Strength 2:

Strength 3:

Areas for Improvement

The following areas for improvement were identified throughout the exercise related to Cybersecurity:

Area for Improvement 1: [Insert relevant observations, findings, and/or conclusions. This should clearly state the problem or gap and should include a root cause analysis or summary of why this particular component of the core capability was not achieved. References to specific plans, policies, procedures, regulations, or laws are also recommended. Specific recommendations or corrective actions should be documented in the Improvement Plan.]

Area for Improvement 2:

Area for Improvement 3:

Situational Awareness

Examine the ability to provide timely and relevant information regarding the cyber incident to critical campus and community decision-makers.

Strengths

The following strengths were observed throughout the exercise related to Situational Awareness:

Strength 1: [Insert relevant observations, findings, and/or conclusions.]

Strength 2:

Strength 3:

Areas for Improvement

The following areas for improvement were identified throughout the exercise related to Situational Awareness:

Area for Improvement 1: [Insert relevant observations, findings, and/or conclusions. This should clearly state the problem or gap and should include a root cause analysis or summary of why this particular component of the core capability was not achieved. References to specific plans, policies, procedures, regulations, or laws are also recommended. Specific recommendations or corrective actions should be documented in the Improvement Plan.]

Area for Improvement 2:

Area for Improvement 3:

Public Information and Warning

Assess the ability to deliver coordinated, actionable, and timely information to critical partners and stakeholders when faced with a cyber incident targeting institutional operations

Strengths

The following strengths were observed throughout the exercise related to Public Information and Warning:

Strength 1: [Insert relevant observations, findings, and/or conclusions.]

Strength 2:

Strength 3:

Areas for Improvement

The following areas for improvement were identified throughout the exercise related to Public Information and Warning:

Area for Improvement 1: [Insert relevant observations, findings, and/or conclusions. This should clearly state the problem or gap and should include a root cause analysis or summary of why this particular component of the core capability was not achieved. References to specific plans, policies, procedures, regulations, or laws are also recommended. Specific recommendations or corrective actions should be documented in the Improvement Plan.]

Area for Improvement 2:

Area for Improvement 3:

APPENDIX A: IMPROVEMENT PLAN

The purpose of this Improvement Plan is to provide a way for institutions to act upon and track identified areas for improvement following an exercise. Members of the planning team should update this table on a continuous basis to ensure that all specific corrective actions are completed in the identified timeline. Additional core capabilities, areas for improvement, and corrective actions should be added as necessary. A sample has been provided in the first row of the table.

This section is in a table format. As you add/delete terms, you will need to do so by adding and/or deleting identified rows. To do this, highlight the identified row, right click, and choose add/delete as appropriate.

This Improvement Plan has been developed specifically for _____as a result of the Cyber Security Tabletop Exercise conducted on October 23, 2018.

Core Capability	Area for Improvement	Corrective Action	Responsible Organization / Individual	POC	Start Date	End Date
Operational Coordination	1. Need for a more structured approach to forming a response team	Ensure all responding personnel have received Incident Command System (ICS) training	Emergency Management Office	Jane Doe	March 15	July 31
Operational Coordination	1. [Insert Area for Improvement]	[Insert Corrective Action]				
Operational Coordination	2.					
Operational Coordination	3.					
Cybersecurity	1.					
Cybersecurity	2.					
Cybersecurity	3.					

Core Capability	Area for Improvement	Corrective Action	Responsible Organization / Individual	POC	Start Date	End Date
Situational Awareness	1.					
Situational Awareness	2.					
Situational Awareness	3.					
Public Information & Warning	1.					
Public Information & Warning	2.					
Public Information & Warning	3.					