Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

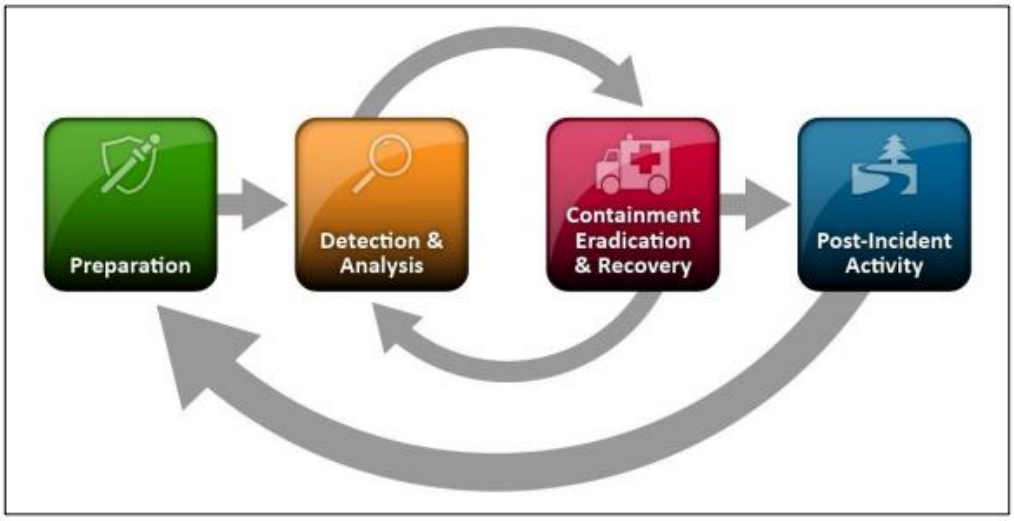
May 2013

Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington State security posture.

The goal of the tabletop exercise is to increase security situational awareness and to facilitate discussion of incident response in as simple a manner possible; targeting a time range of 15 minutes. The exercises provide an opportunity for management to present realistic scenarios to a workgroup for development of response processes.

How to best use the tabletop exercise:

1. Modify the tabletop scenario as needed to conform to your environment.
2. Engage management.
3. Present scenario to the workgroup.
4. Discuss the process to address the scenario.
5. Document the response and findings for future reference



EXERCISE SCENARIO

A pandemic flu starts sickening and killing people in Hong Kong. The medical community fears that the disease will spread to other continents. Anyone who has been in Hong Kong in the past three weeks could be a carrier. As a precautionary measure, employees who have traveled to Hong Kong within the past three weeks have been asked not to return to work until they see a doctor. Additionally, security is screening every visitor to see if they have been to Hong Kong in the past three weeks.

A few people in the region are diagnosed with the disease and absentee rates at local schools rises. Employees start calling in sick, but it's not clear if they are ill or afraid to go out in public. Enough people are absent that the organization struggles to maintain the IT infrastructure (applications, networks, and computers).

Issues for discussion:

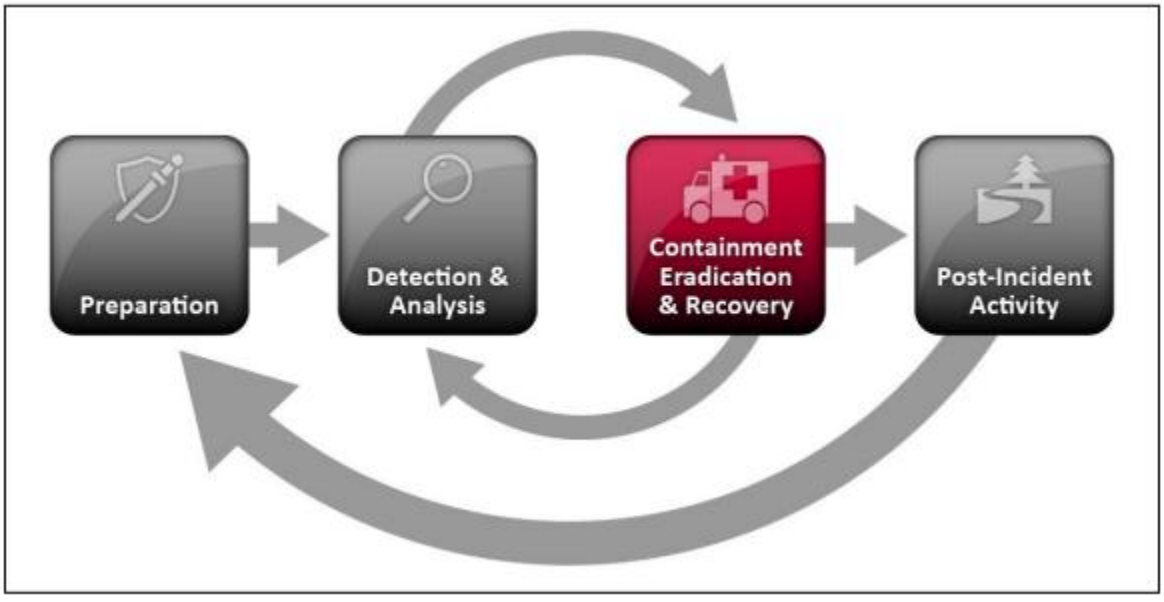
1. What do you do?

2. How do you prioritize the workload?

The disease spreads and absentee rates shoot up to almost 50%. Critical functions are not getting done.

1. What other options are available?

2. How will you sustain the operations?

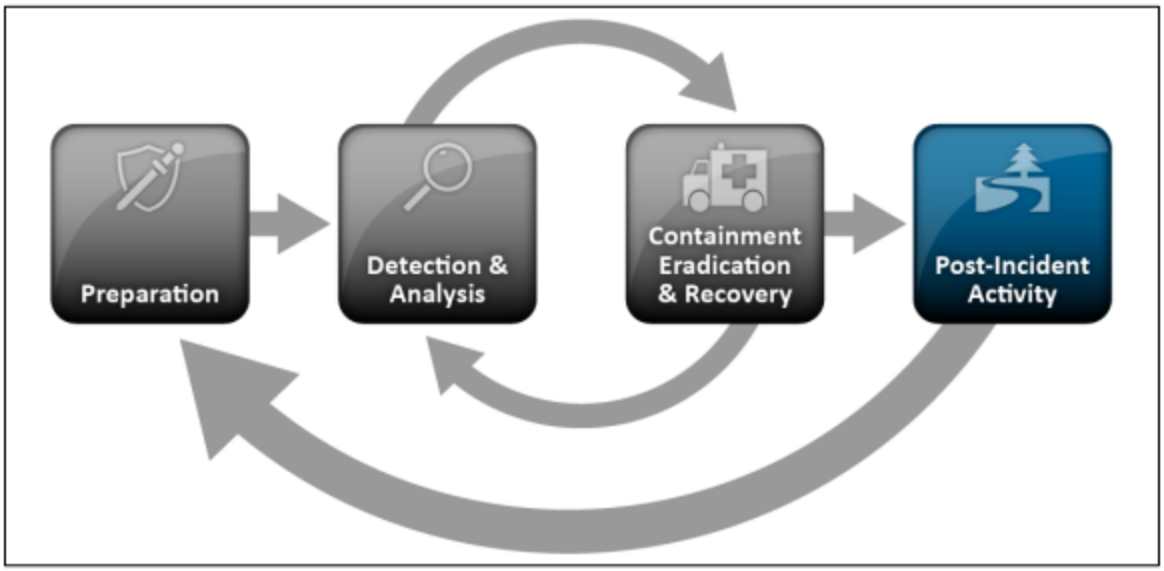


ITEMS TO DISCUSS

- Who would the service desk notify?
- How would you confirm the claim?
- Who would you call to address the scenario?

ITEMS TO REPORT

- Did communications flow as expected? If not, why?
- Were processes and procedures followed?
- Were there any surprises?
- How well did the exercise work for your organization?



CONTACT US

The CTS SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

Contact the CTS Service Desk to report a cyber-incident, or report cyber incidents online at:

http://sharepoint.dis.wa.gov/soc/default.aspx

To speak with a SOC analyst, call **360-407-8800**. For general questions, send us an email at soc@cts.wa.gov.

The CTS Security Operations Center (SOC) is an active member with the Multi-State Information Sharing and Analysis Center (MS-ISAC) which has been designated by the US Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through this relationship, the CTS SOC is able to leverage resources available from MS-ISAC of malware analysis, reverse engineering, log analysis, and forensics analysis in a cyber incident.

The mission of the CTS SOC is to provide centralized information sharing, monitoring, and analysis of Washington State security posture. The promotion of cyber security education and awareness to end users is critical to maintenance of a strong security posture of the Washington State network.