
Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

March 2013

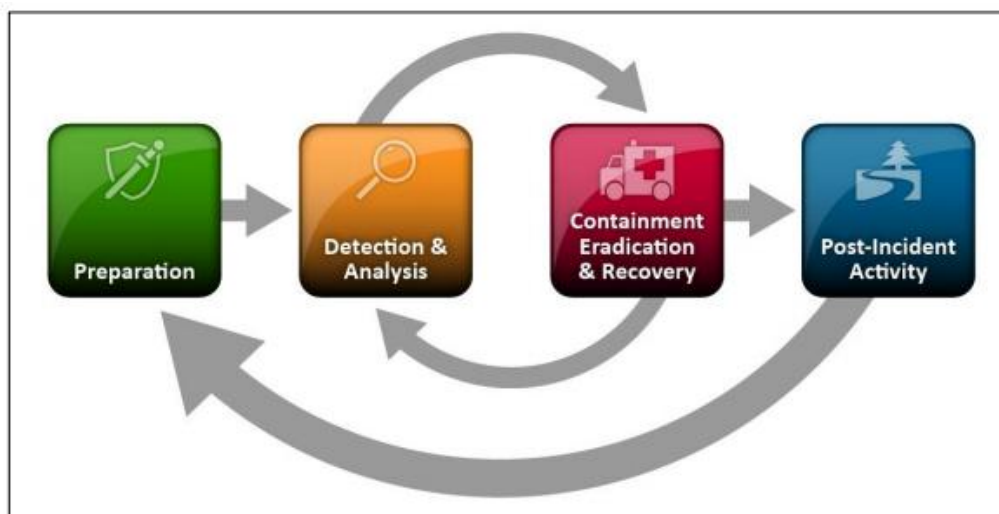


Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington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

This month's exercise is unique.

The news is reporting that a major chemical plant, located 2 miles away, has had a significant toxic chemical leak. There is a chemical "cloud" and your office building is in the path of the plume.

Additionally, the news has reported that a number of people at the factory have died. Authorities have directed everyone to remain where they are and not go outside.

Issues for discussion:

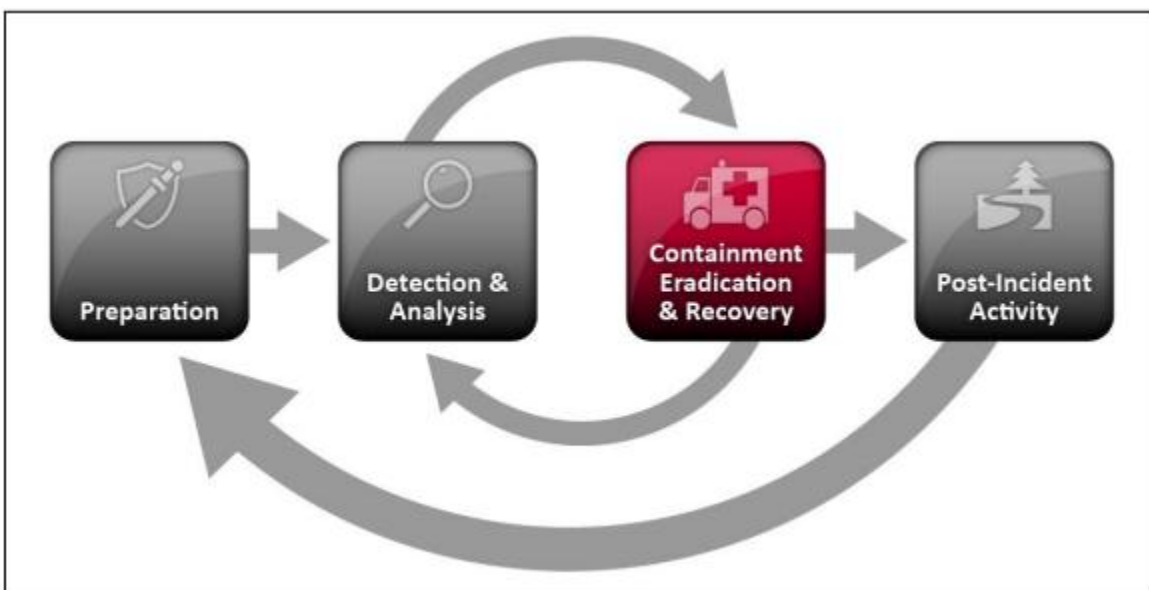
1. Can you shut down the HVAC or air intake system?
2. Who is responsible for shutting the system down?
3. How many people would leave the building in spite of the direction to stay in place?
4. How will your operation continue with so many people leaving?

You are now into the next business day and the authorities have signaled the all clear. The chemical accident was not caused by terrorists.

- Those who sheltered in place are now leaving to go home to get some sleep, food and shower

How will you sustain your operations with so many people out of the office?

1.

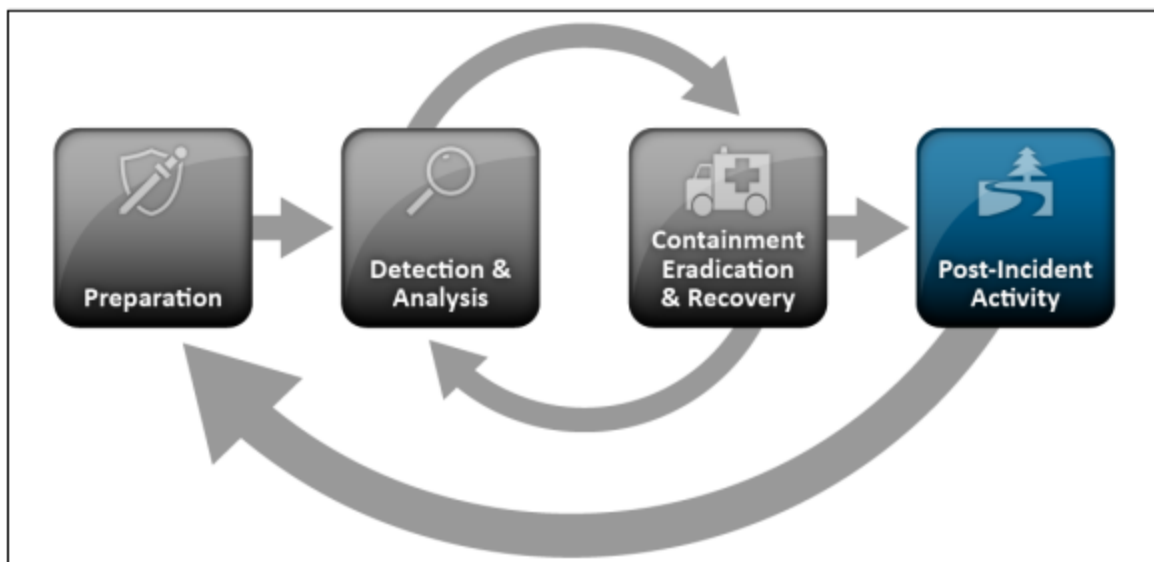


ITEMS TO DISCUSS

- 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.

