
Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

December 2013

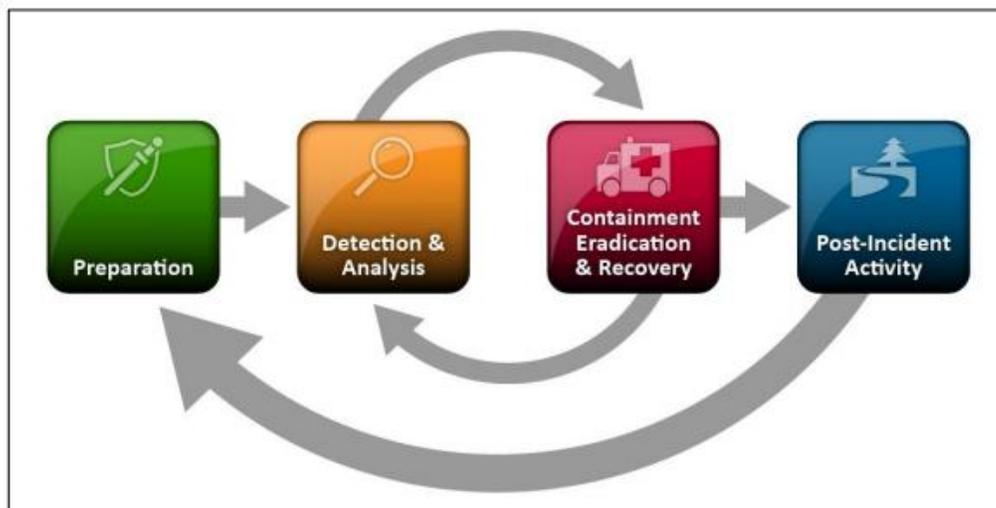


Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington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

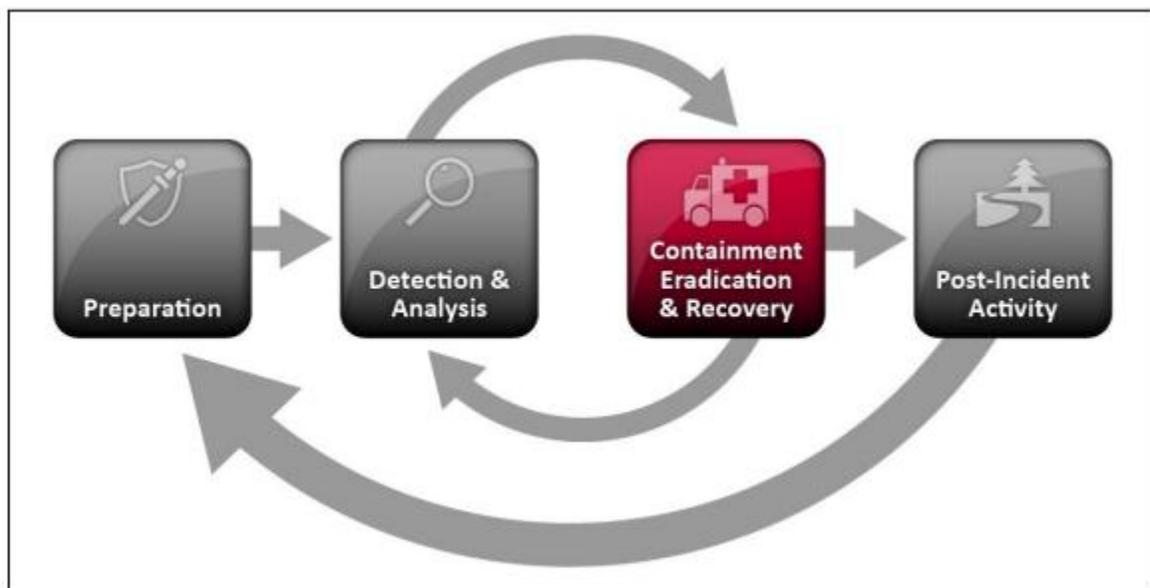
How to best use the tabletop exercise:

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

- *One of your organization's internal departments frequently uses outside cloud storage to store large amounts of data, some of which may be considered sensitive. You have recently learned that the cloud storage provider that is being used has been publically compromised and large amounts of data have been exposed. All user passwords and data in the cloud provider's infrastructure may have been compromised.*

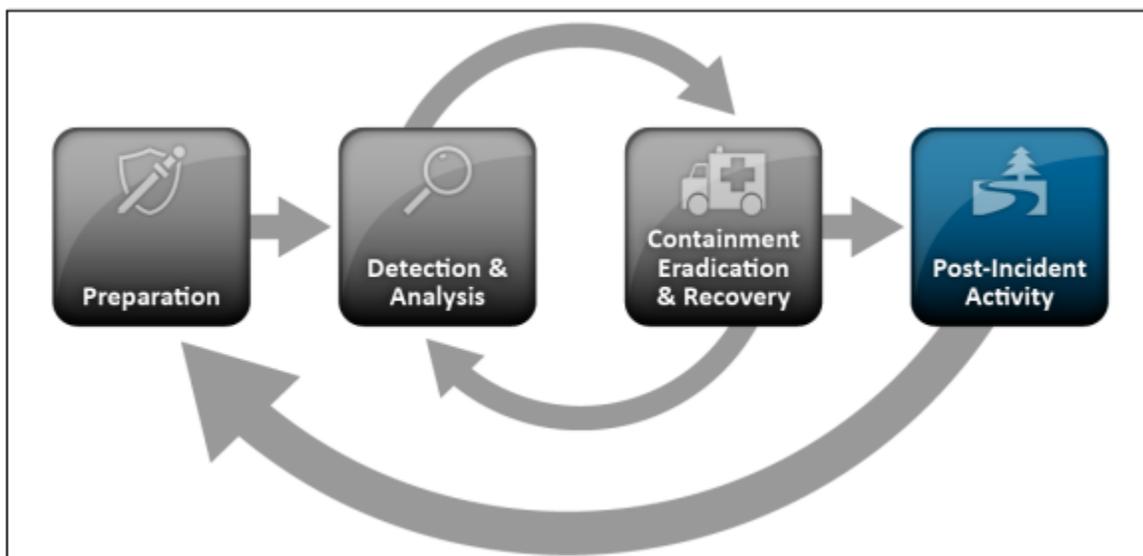


ITEMS TO DISCUSS

- What steps will your organization take?
- Does your organization have current policies that take into account third party cloud storage?
- Should your organization still be held accountable for the data breach?
- What actions and procedures would be different if this was a data breach on your own local area network?
- What should management do? Who else in the organization should be involved?
- What, if anything, do you tell your constituents? How and when would you notify them?

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.

