

---

# Incident Response Planning

---

## The 15 Minute Workgroup Tabletop Exercise

---

*August 2014*

---



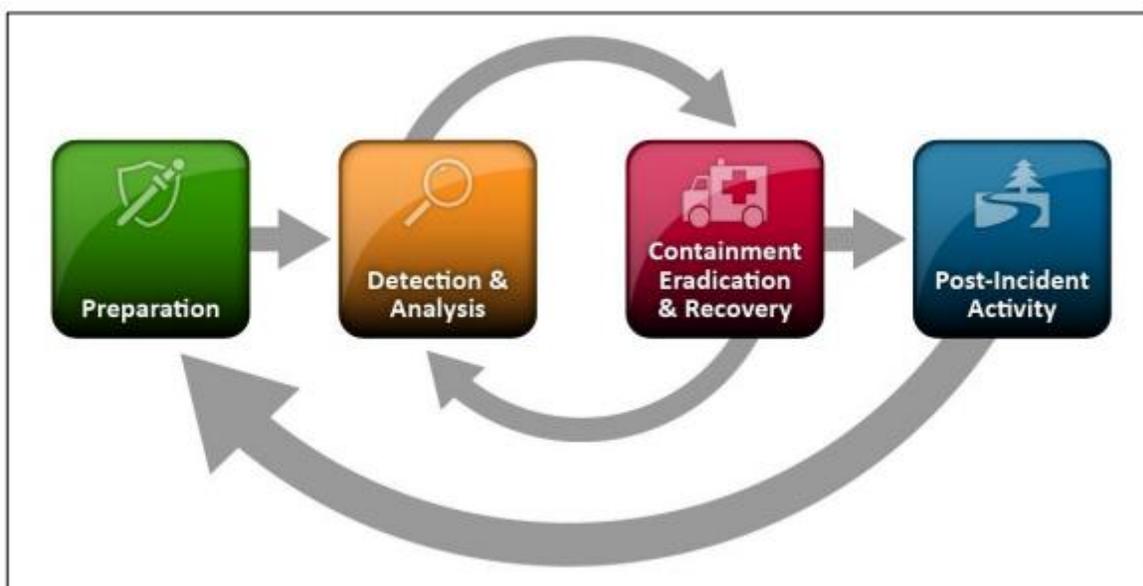
Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington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

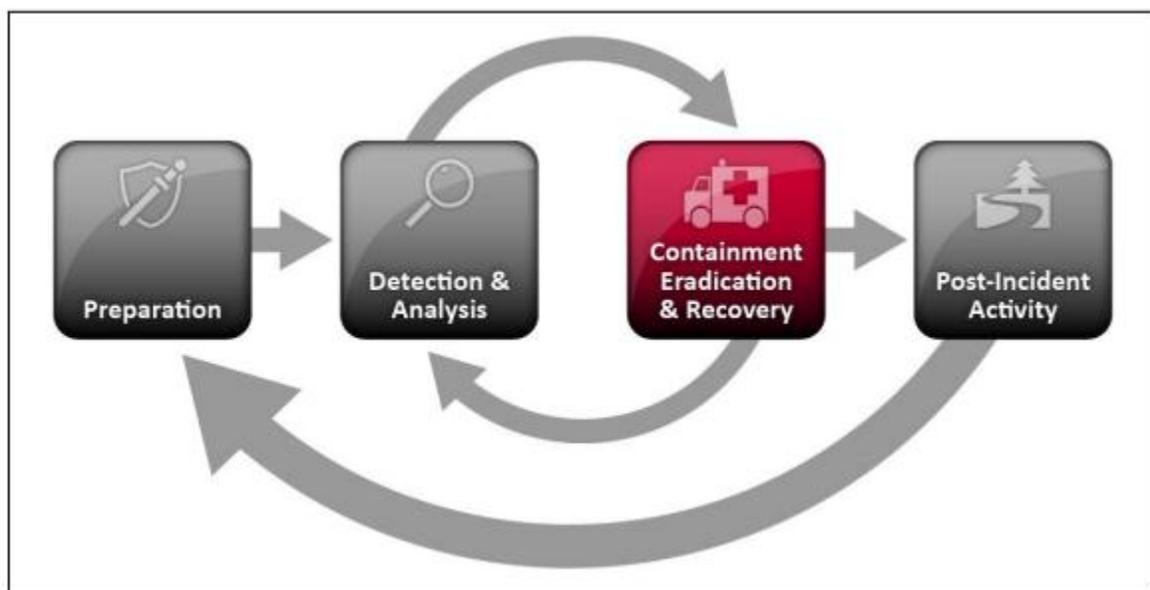
1. Modify the tabletop scenario as needed to conform to your environment.
2. Engage management.
3. Present scenario to the workgroup.
4. Discuss the process to address the scenario.
5. Document the response and findings for future reference

**Note:** A member of the CTS Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the CTS Service Desk at 360-753-2454.



## EXERCISE SCENARIO

You have been notified that your organization may be targeted through spear phishing emails and social engineering phone calls.

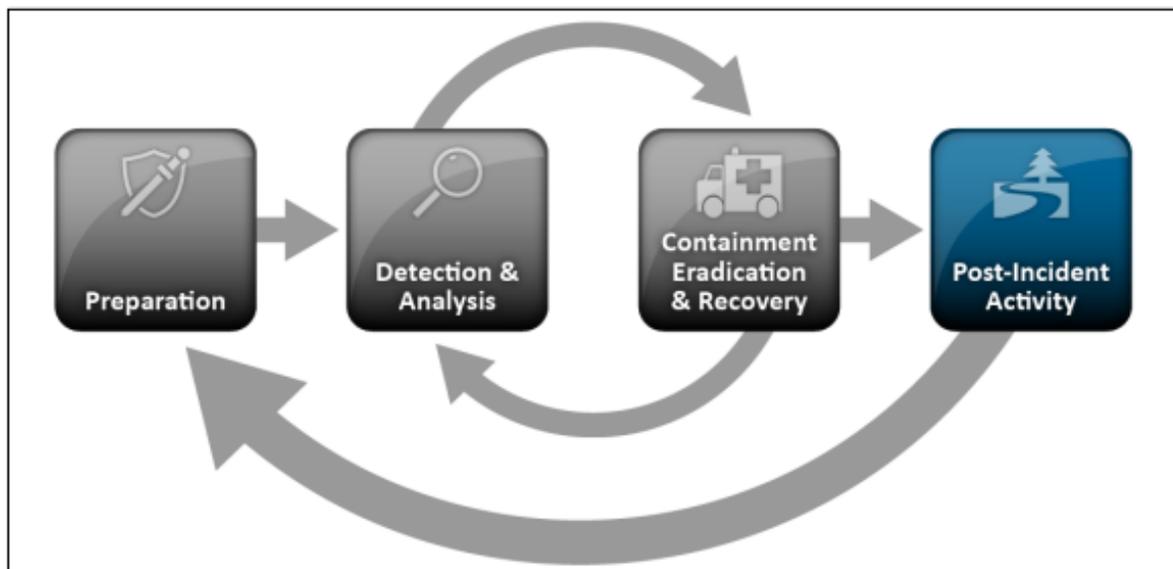


## ITEMS TO DISCUSS

- Do your end users know what to do with a suspicious email or phone call?
- What does your policy say about reporting suspicious emails?
- How do you notify end users?
- How do you notify IT staff?
- At what point do you communicate the event to upper management?
- What do you do if individuals within your organization click on the malicious links found in the email?
- How do you educate users on identifying phishing emails and social engineering attempts?
- How will you incorporate any lessons learned from this exercise?

## 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.

To report a cyber-incident, contact the CTS Service Desk at (360) 753-2454 / 1-888-241-7597.

For general questions, send us an email at [soc@cts.wa.gov](mailto:soc@cts.wa.gov).

For more information, visit our site at: <http://soc.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.



SECURITY OPERATIONS