Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

February 2014

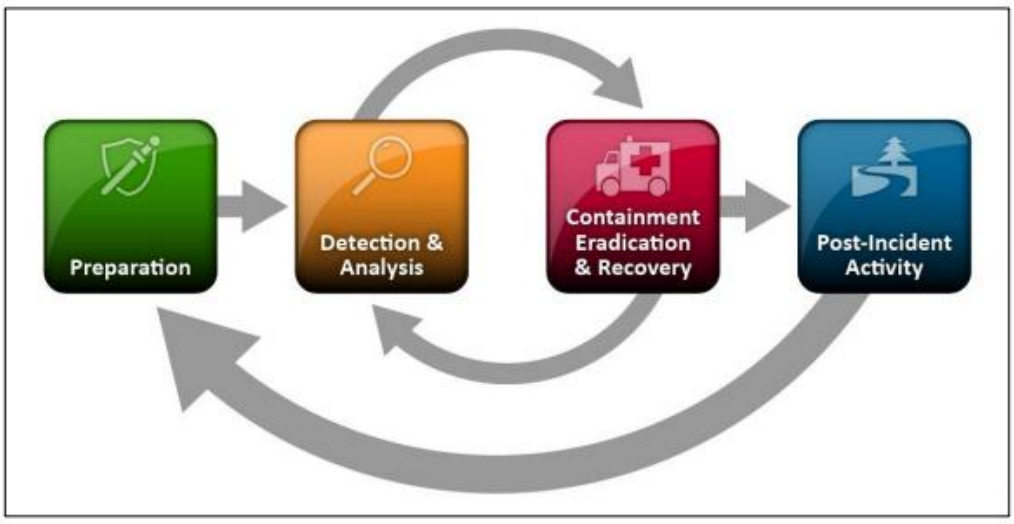
Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the CTS Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring, and analysis of Washington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

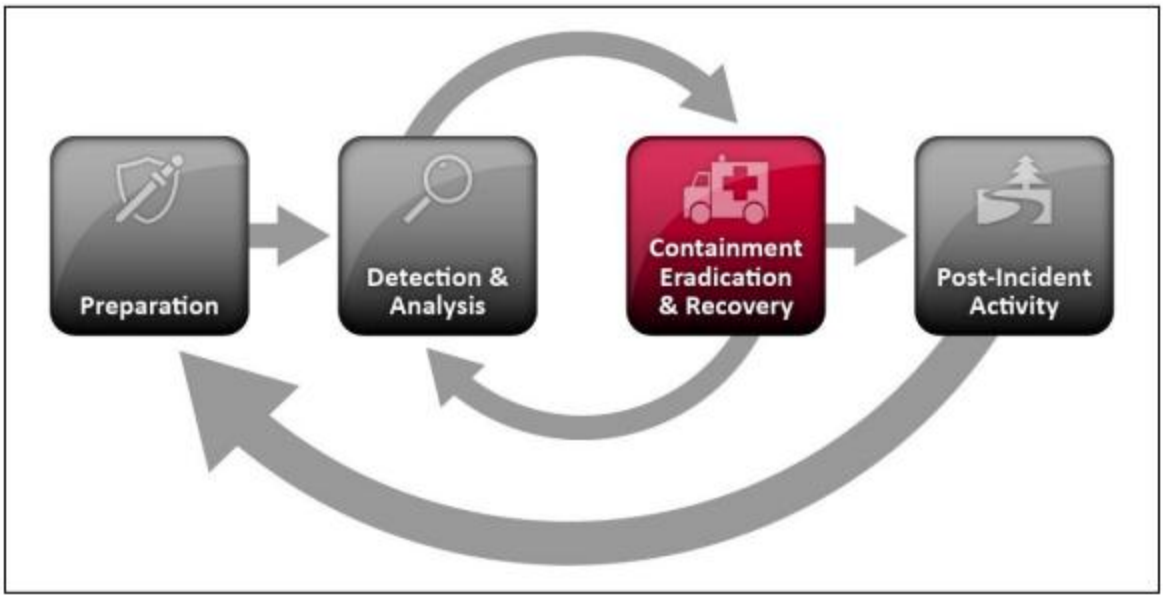
Note: A member of the CTS Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the CTS Service Desk at 360-753-2454.



EXERCISE SCENARIO

- An employee calls to ask for the password for the Wi-Fi network, indicating they would like to use it on their personal cell phone so they can check Facebook on their lunch break. You don't have a Wi-Fi network. A scan of the building indicates there are 4 Wi-Fi networks, clearly originating from within government space and broadcasting a variety of names that suggest people are using them for work purposes. How do you respond?

- Inject: In the course of follow-up to this report it is found that all 4 devices are plugged into your hard wired network. Two have logging enabled and show that they are being used by employees for official work purposes.



ITEMS TO DISCUSS

- How would your organization address the employee's call?
    - What escalation and notification procedures do you have in place?

- How would your organization identify and respond to the identification of rogue access points (wireless networks)?

- Does your organization have procedures in place to identify and respond to the identification of rogue access points (wireless networks)?

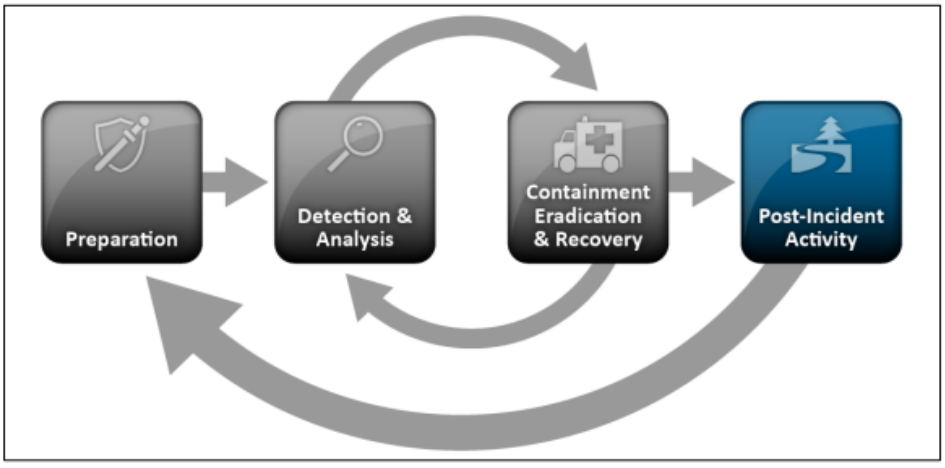
- Who in your organization is responsible for the identification of rogue access points (wireless networks) and response?

- How do employees get notified of policies surrounding the usage of wireless and the risks associated with using rogue, or unauthorized, wireless networks?

- Knowing that two of the networks have been used by employees for official business usage,
    - How would your organization ensure that no confidential/sensitive data was compromised through these channels?
    - How would your organization determine if these networks are protected to your organizational standards?
    - What would your organization do to ensure unauthorized wireless networks are taken down and not visible to employees?
    - How would you coordinate with stakeholders in identifying how these rogue networks were used?

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:

https://sp.cts.wa.gov/ask/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.

SECURITY OPERATIONS