
Incident Response Planning

The 15 Minute Workgroup Tabletop Exercise

February 2016



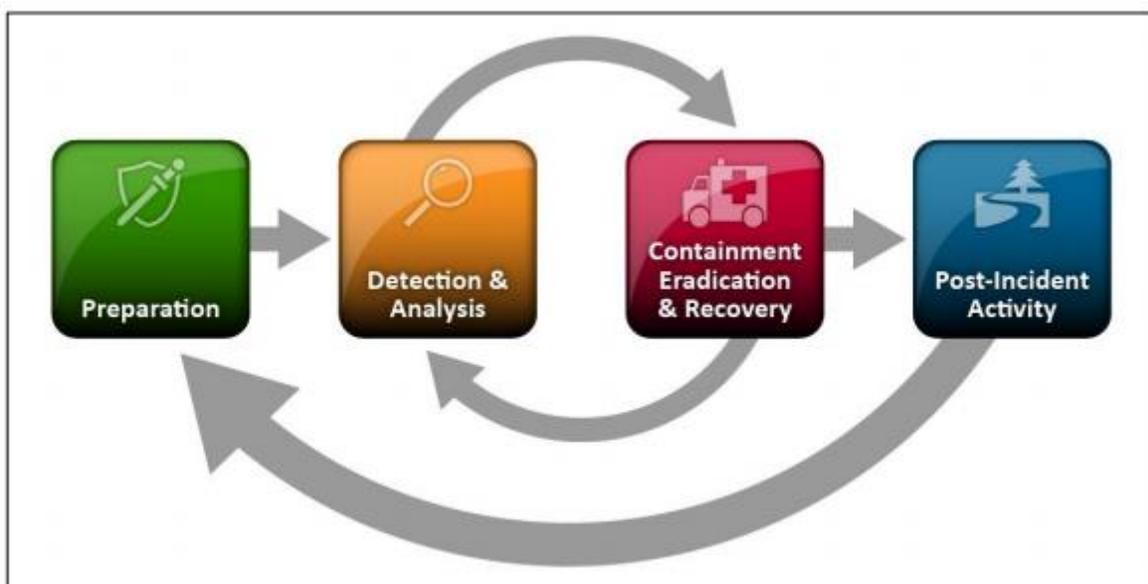
Provided for your use is a 15-minute tabletop exercise template for use in developing education and awareness at your agency. These exercises are brought to you by the State Office of Cyber Security, Security Operations Center (SOC), with a mission of providing centralized information sharing, monitoring,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

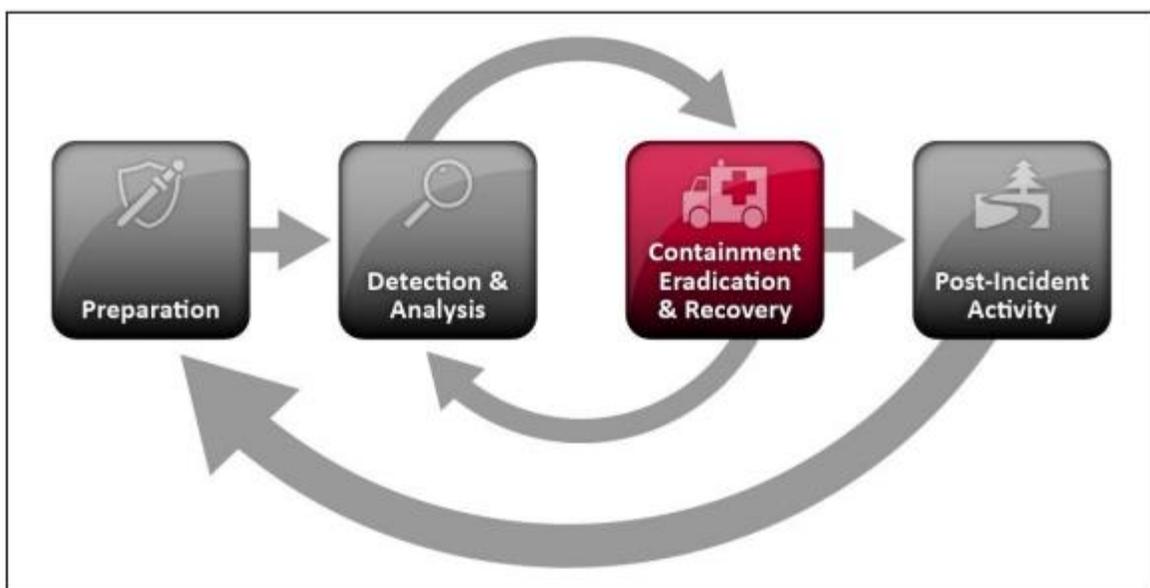
Note: A member of the State Office of Cyber Security, Security Operations Center will be happy to facilitate this exercise with a workgroup from your agency upon request to the WaTech Service Desk at 360-753-2454.



EXERCISE SCENARIO

You just received a rather panicked call from one of your system administrators detailing that your organization has been hit by ransomware. This ransomware seems to have infected and then encrypted all the data, including backups, of two of your servers. According to the ransom you received, you must pay the ransom in a week or the encryption key will be deleted and the data lost forever.

The work week is bustling and people are starting to ask why the servers are down. How do you respond?

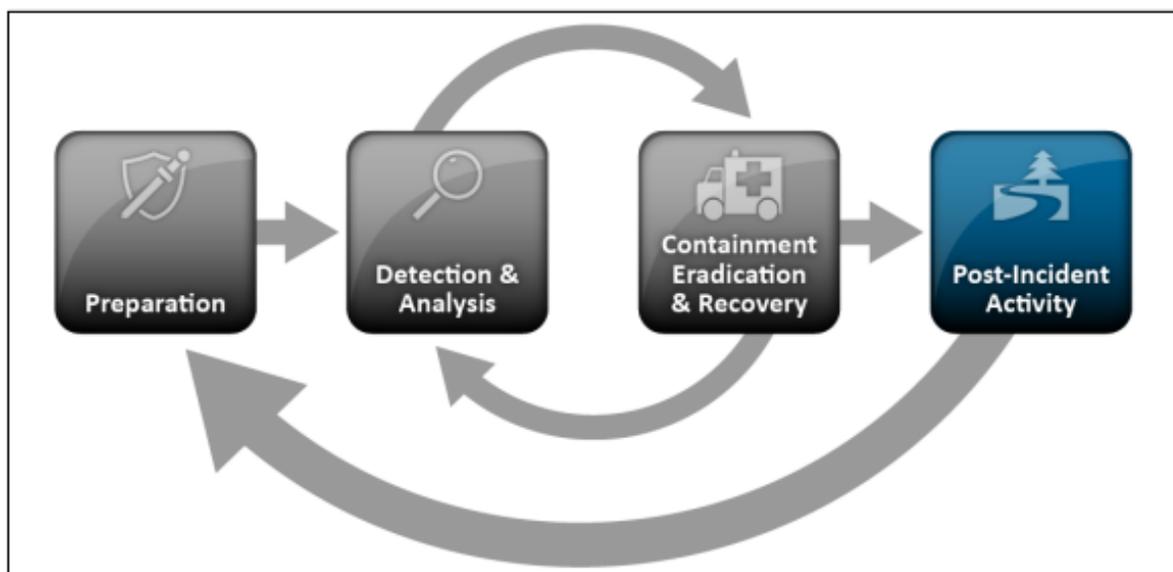


ITEMS TO DISCUSS

- How can you determine which business unit and processes rely on the servers?
 - Do you know those business units' Recover Point Objective?
 - Do you know those business units' Recovery Time Objective?
 - What options are available if you can't reach those two objectives?
- Who do you report the incident to?
 - How do you communicate to the business units?
 - What's the messaging you provide to business units? How about the executives?
 - What would be the messaging for the public if the impact was to a key public facing business process?
- Do you activate your COOP, DR or BCP?
- How do you make sure to prevent future infections?
- How can you determine the infection vector?
- What forms of backups do you have available?
 - Do you have off-site hardcopies of your data?
 - How quickly can you get access to them?
 - What's the most recent version available?
- How do you prioritize which server to recover first?

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 State Office of Cyber Security SOC forms a focal point for the efficient reporting, containment, and recovery of security incidents.

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

For general questions, send us an email at soc@watech.wa.gov.

For more information, visit our site at: <http://www.soc.wa.gov>.

The State Office of Cyber Security, 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 (DHS) 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 State Office of Cyber Security 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 State Office of Cyber Security SOC is to provide centralized information sharing, monitoring, and analysis of Washington State's 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