****

**Incident response tabletop exercise**

This document outlines an incident response tabletop exercise which is intended for use in a classroom setting. It assumes that students are familiar with the principles and concepts outlined in the CyBOK knowledge area “Security Operations and Incident Management” and presents a scenario that is explored in a role-playing fashion.

Th document describes the setup, scenario, and general outline of the game. It is up the too teacher to modify and extend the scenario as needed.

Contact the developer, Joakim Kävrestad at Jönköping School of engineering for questions.

Joakim.kavrestad@ju.se

© Crown Copyright, The National Cyber Security Centre 2024. This information is licensed under the Open Government Licence v3.0. To view this licence, visit <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>.

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK incident response tabletop exercise © Crown Copyright, The National Cyber Security Centre 2024, licensed under the Open Government Licence: <https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>.

**Introduction**

In this exercise, students are to be split into groups of 4-5 people. Each group will act as a crisis group for the company Economistas during an IT-incident and the participants will assume different roles in this group. The groups will be presented with events and will be given some time to respond to those events. Depending on their response, the game leader will provide additional events.

The game rules can be used to play any cyber incident response scenario. This document will outline a scenario which intends to mimic a ransomware/extortion attack.

**Setup***The PowerPoint Tabletop exercise.pptx contains slides to aid the setup and presentation of the game.*

The game design is simple, students are divided into groups and all group members will assume a different role. They are the presented with a starting event which they are to respond to. The response is to be written on a response card and include:

* The groups general assessment of the event
* The technical response to the event, i.e. what actions to take to investigate, isolate, mitigate etc.
* Actions taken for legal purposes if any
* Internal communication
* External communication

The group members should assume the following roles:

* CEO
* IT-manager
* Legal advisor
* Communications manager (divided into internal and external communication manager for groups of five).

The group members are responsible for their respective areas. The CEO, while not responsible for any specific area has the final say in all matters. The CEO is also responsible for submitting the response cards to the game leader.

The students are to be instructed that they can:

* Make reasonable assumptions about the company’s infrastructure. For instance, if the players claim that the company has immutable backups, they are allowed to use those in their incident handling. The assumptions should be reasonable at the game leader’s discretion.
* Ask the game leader for company information that is important for their decisions. They could, for instance, ask if the company is about to deliver on a big order or likewise. Again, how to answer is up to the game leader.

Finally, the game leader should in advance prepare and provide the groups with response card and follow-up events. Templates and sample events are available at https://github.com/kavrestad/CybSec\_Courseware.

**Game outline**

The game begins with an event, which is the same for all groups. The event description is as follows: The IT-manager receives and e-mail from an employee at Economistas. The employee states that they saw a social media post from a Russian hacking group with the following message. *We now compromised the servers of Economistas. Actions will be taken shortly. To encrypt, or exfiltrate….that is the questions. Maybe both, is the answer.*

The students will work in their groups and decide on what actions to take and note those on the response cards. Once they feel done, they hand the response card to the game leader. The game leader is responsible for providing a reasonable follow-up event which should be dependent on the group’s response actions. While there are some sample follow-up events supplied, the game leader is encouraged to lead the game in a good direction by coming up with realistic events.

The follow-up events can be versatile. Assume that a group decides to do nothing at all. A follow up event could then be that a ransomware attack is launched at Economistas and all of their servers are encrypted. Another group may choose to isolate the entire network and launch an investigation. A follow-up could be that IT is overwhelmed by user tickets since the users are unable to work.

It is up to the game leader to decide when the game ends and tinker with the follow-up events to make the game time fit for the time at your disposal. It is advised to allow time for a reflection session with the entire class.