The Cyber Threat-Response Framework: An Overview

MICROMODULE

Kevin Kuczynski - April 11, 2019

Description

Parts 1 and 2 of this Lesson address identification and initial investigation of a cyber threat. Proper identification and investigation of a cyber threat is essential because significantly different legal structures govern the handling of and response to cyber threats - depending upon the nature of the particular cyber threat.

From the standpoint of the law, determining the nature of the cyber threat will directly impact: what law governs; who should, and who can, respond; and what responses are lawful. This determination is based upon a three-fold inquiry:

(1) Who or what is being injured - government, business, individual, critical infrastructure?

(2) What type of threat is it - domestic crime, terrorism, national security?

(3) Who is the threat actor – state actor or non-state actor?

Outcomes

remember and understand

Students will be able to understand the difference between defensive measures versus countermeasures that may rise to the level of "hacking back".

remember and understand

Students will be able to understand the distinction between domestic cyber threats and crimes, cyber terrorism, and national security cyber threats and be able to identify what laws govern defensive measures against the cyber threat and offensive measures in response.

remember and understand

Students will be able to understand the legal differences that arise in handling and responding to cyber threats based upon the nature of the cyber threat. determining the nature of the cyber threat - and thus what law governs and who should respond – is based upon a three-fold inquiry: (1) who is being injured - government, business, individual; (2) what type of threat is it - is domestic crime, terrorism, national security; and (3) who is the threat actor – state actor or non-state actor.

remember and understand

Students will be able to understand what constitutes a cyber threat and what cyber threat indicators are.