Udipto Chowdhury

FCM 761

Prof. Kennedy

05/13/2023

Week 12 Assignment

Task: Please reflect on what elements of the NIST framework constitute "left of the boom" elements, and which constitute "right of the boom" elements. You can generalize the types of elements that fit each. No need to be overly specific. Please provide feedback on the incident response portion of the class. What did you learn? Did it change anything about the way you approach cybersecurity? How?

Based on IBM's Beyond the Boom, the presentation introduces the fact about high-profile data breaches to the point that the IT Department of a conglomerate or a high-profile company is not focusing on all problems equally. Since they are focusing on detection and prevention and don't pay enough attention to response and remediation, it can then be deduced that these IT people need to have better training when it comes to mitigating and eliminating any conflicts regarding NIST's Cybersecurity Framework. IBM then supports this claim by stating that "a study from the Ponemon Institute found that 75 percent of organizations don't have an incident response plan applied consistently across the organization..". This creates an effect that breach notification laws

and regulations are becoming stricter around the world, with decreasing times allowed for reporting to government parties and the public. IBM then defined the "boom" concept by listing the four critical events: when does a breach occur, when was the data taken or destroyed, when is the breach discovered (either by external or internal parties), and when was the breach made public? Under the NIST's concept, the whole "boom" concept applies to all five concepts of NIST's Cybersecurity Framework. Because the term "left of the boom" describes the concept with examples in which cyber thieves are taking credentials, gaining deeper access, stealing data to be monetized, targeting key intellectual property, or preparing a destructive cyber/physical attack. This implies the concept of detecting - which defines the concept of finding the cause(s) that contribute to the situation, responding - coming up with a solution and executing the actions that resolve the solutions, and identifying - knowing the cause and effect under NIST's cyber framework. On the other hand, the concept of the "right of the boom" deals with responding as well. All in all, I think that IBM did a great job when it comes to informing anyone when it comes to self-awareness regarding cybersecurity infrastructure.

Jumping to the story of a Patient who Dies After a Ransomware Attack Hits a Hospital, people are not generally expecting the unexpected when "Westphalia state justice minister said that the attack encrypted about 30 hospital servers and left a message instructing the Heinrich Heine University, to which the Düsseldorf hospital is affiliated, to contact the attackers." Fortunately, the attackers reportedly withdrew the extortion demand and provided a decryption key to unlock the servers. When Düsseldorf police eventually communicated with the attackers and told them that the attack had hit a hospital treating emergency patients, not the university. In spite of the fact that Citrix didn’t immediately respond to an email asking if the vulnerability was the initial entryway into the Düsseldorf hospital, federal prosecutors believed it was one of several

vulnerabilities allegedly used by hackers backed by the Chinese government to breach the game, and software makers. In a nutshell, I believe this article is a 'wake-up call' when it comes to facing an unexpected event.