Ronald William Sudol III

SNHU CYB200

Project Three

08/13/2023

**Technical Brief**

This technical brief is directed to the security/IT director of our organization as a basis for a proactive adversarial detection plan. We are a contractor handling projects for the U.S. Armed Forces and it has recently come to the attention of this employee that a possible unwitting or malicious threat may be coming from a coworker who shall be referred to as Jan. It is difficult to characterize the motivations of Jan at this time but she is outright disregarding the organization’s “bring your own device”(BYOD) policy. As a whole, personal devices are not allowed and per company policy, “that IT asset and its user still must abide by the organization’s mobility policy, BYOD policy, and ‘acceptable use policy(AUP)’”(Kim & Solomon, 2021). Not only is Jan not allowed to use personal devices within the facility but has also been witnessed utilizing a personal device to transport top secret data off the premises. This is a flagrant violation of multiple policies.

Any traffic accessing the cloud stored images taken by Jan’s tablet should be monitored and logged to potentially generate leads to any potential larger bodies at work that may have influenced or incited Jan’s actions. Jan’s activities should be restricted at this time and any attempts to access their account should be monitored to detect any continued attempt to breach data confidentiality.

The ethical and legal factors here are potentially very long reaching. Top-secret data is defined as “information that the classifying authority finds would cause grave damage to national security if disclosed”( Kim & Solomon, 2021). This wording does not specify whether that disclosure is intentional or not. Jan’s mishandling of top-secret data as an unwitting and consequence-free threat is the best-case scenario. If Jan is found to be acting maliciously in mishandling top-secret data from the U.S Government, the consequence could be far more severe. Jan’s actions could not be ruled out from being treasonous at this time.

Responding to and countering this threat requires swift and decisive action. Auditing to uncover evidence of Jan’s practices accessing data and processes is essential. Real-time surveillance of any further attempts to access classified data as well as any attempts made to access cloud stored data before it was recovered can give insight into the scope of this breach. Jan’s access should be restricted pending investigation and any data that was cloud stored should be scrubbed immediately.

Reasonable tactics to reduce the likelihood of this happening again would be requiring that devices be locked away at the security desk before entering the premises. This layer of physical security reduces the chance of actors disregarding or trying to work around security policy. It also reduces the ability of malicious actors accessing and corrupting or stealing sensitive data.

The potential ramifications of Jan’s actions are yet to be seen. “Sensitivity is the measure of the effect that a breach of integrity or the disclosure of information would have on an organization”(Kim & Solomon, 2021). As we evaluate the sensitivity of the data that was mishandled by Jan, the full scope of this breach will come into view. Given that the data was classified top-secret, it should be assumed until proven otherwise that protection of this data is of the utmost importance and that this breach could potentially be damaging to national security.

**CITATIONS**:

Kim, D., & Solomon, M. G. (2021). *Fundamentals of Information Systems Security*. Jones & Bartlett Learning.

*A Taxonomy of Operational Cyber Security Risks Version 2*. (2014a, May 21). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91013