Amjad Alqahtani

Principles of Cybersecurity

Assignment 2

09/25/2024

First Question:

Summary of what is the question all about:

This improvement is crucial for federal organizations to take action of protections regarding the sensitive information. This will maintain public trust and effectively respond to cyber threats. The question highlights the urgent need for organizational transformations and establishing goals and timelines to enhance cybersecurity across federal agencies.

Important of federal action:

The action will ensure national security, guarantee the consistency across agencies, allocate resources, and increase public confidence in government operations. This will lead to better defense against attacks, minimize risks, and enhance overall resilience.

Recommendation by GAO:

1. Establishing clear roles and responsibilities for all federal agencies across all levels.
2. Enhancing training and awareness for all employees which will lead to less human error.
3. Continuous monitoring systems to assess the effectiveness of cybersecurity measures that have been taken.

Second Question

Summary of what is the question all about:

The question seeks to identify specific actions that can be taken to address weakness in the information security programs of federal agencies. The question really highlights the great need for improvement in protecting sensitive data and systems against any cyber threats. It also ensures compliance with federal regulations like the Federal Information Security Modernization Act.

Important of federal action:

Protecting sensitive data including personal data and national security information from unauthorized access and breaches. Weaknesses in information security can lead to a disruption of agency functions and compromise mission-critical activities that are important for many people. Addressing security weaknesses is vital for compliance with all federal laws.

Recommendation by GAO:

1. The reporting mechanisms regarding information security should be improved by all federal agencies. All federal agencies should also ensure accountability for the timely implementation of recommendations made by GAO and IGs.
2. Agencies should fix identified security issues and prioritizing the actions like:
   a. identify risks
   b. protecting against threats
   c. detect incidents
   d. recovery systems.
3. GAO highly recommends that the Office of Management and Budget improve its guidance to Inspectors General (IGs) for conducting evaluations. The evaluation should come in many forms like establishing a nuanced rating scale that accurately reflects the effectiveness of agency information security programs.

Third Question

Summary of what is the question all about:

The question emphasizes the need for effective strategies and coordination following significant breaches, such as those involving SolarWinds and Microsoft Exchange, which exposed vulnerabilities in federal cybersecurity practices.

Important of federal action:

The strong responses will help safeguard critical government data and systems from cyber threats. Effective incident response is vital for maintaining national security, especially as threats evolve and become more sophisticated. Enhancing agencies' collaboration, private sector partners, and law enforcement can all lead to quicker and effective responses to security incidents.

Recommendation by GAO:

1. Establish standardized ways of exchanging information among federal agencies and private sector partners to improve threat response coordination in a timely and effective manner.
2. Ensure that cybersecurity investments directly address the most critical vulnerabilities and operational priorities of federal agencies.
3. DOD and other agencies should fully implement processes for managing cyber incidents, including complete reporting and documentation of notifications to affected individuals regarding breaches of personal data.