EAS 596 – CYBERSECURITY ANALYTICS

CRITICAL RESPONSE 1

As a newly appointed **Chief Information Security Officer (CISO)** in a small organization with about 100 employees, my first priority would be to gain a thorough understanding of the **organization's structure**, **operations**, and **existing security posture**. Establishing a strong foundation of knowledge about the organization is essential to effectively address its security needs and align them with its business objectives.

Understanding the Organizational Structure: The first step I would take is to familiarize myself with the organizational structure, including the **various departments**, their **roles**, and the **key personnel** managing them. This would involve meeting with department heads and understanding their functions, goals, and how their operations align with the organization's overall mission. Establishing these relationships early on is crucial for fostering collaboration and ensuring that security initiatives are well supported.

Assessing the Organization's Infrastructure: Next, I will conduct a thorough assessment of the **organization's IT infrastructure**. This includes understanding the **hardware**, **software**, and **services** in use. A complete asset inventory is a foundational component of any security program, as the saying goes: ***"You can't protect what you don't know about."*** This inventory would also help identify critical assets that require prioritized protection.

Reviewing Inventory and Vulnerability Management Processes: The next action would be to evaluate how the organization is currently managing its inventory and conducting **vulnerability assessments**. This includes understanding the processes for **tracking assets**, **patch management**, and **identifying security gaps**. If these processes are insufficient, I would prioritize implementing a robust system for continuous monitoring and vulnerability management to minimize the risk of exploitation.

Identifying and Securing Personally Identifiable Information (PII): A key focus area would be understanding the types of PII that the organization collects, stores, or processes. Protecting sensitive data is critical, not only for the organization's reputation but also for regulatory compliance. I would review existing policies and procedures related to PII management to ensure they align with best practices and relevant legal requirements or industry-specific standards.

Reviewing Policies and Regulatory Compliance: I would then examine **the organization's active policies and regulations**. This would involve reviewing acceptable use policies, incident response plans, and data protection policies to ensure they are up to date and effective. If gaps are identified, I would work to strengthen these policies to align with industry standards and legal obligations.

Assessing Third-Party Relationships: If the organization has partnerships or dependencies on third-party vendors, I will review these relationships and their associated contract terms. Third-party risks can often be a weak link in the security chain, so it's essential to ensure that vendors adhere to appropriate security standards.

Looking into Past Security Incidents: To understand the organization's current risk landscape, I would inquire about any recent **security incidents**, **breaches**, or **near misses**. This would help me identify vulnerabilities or systemic issues that need to be addressed immediately. Analyzing past incidents also provides valuable lessons for improving incident response processes and preventing recurrence.

Evaluating the Playbook and Business Continuity Plans: Finally, I would review the organization's **incident response playbook** and **Business Continuity Plans**. These documents are critical for ensuring the organization is prepared to respond to and recover from security incidents. If these plans are outdated or inadequate, I would prioritize developing and testing them. A well-crafted BCP ensures the organization can maintain operations and minimize downtime during disruptive events.

In summary, my initial focus as a CISO would be on understanding the organization's structure, assets, policies, and risk landscape. This foundational work would enable me to identify and address vulnerabilities, align security efforts with business objectives, and build a resilient security program. By taking these steps, I will be able to lay the groundwork for a robust and effective cybersecurity strategy.