Assignment 1: Pre-Incident

Name : Andrei Cirlig

SRN:20049583

**PART1**

**Similarities:**

There are several similarities between the two subjects.Both texts place significant emphasis on the implementation of a systematic approach to incident response, underscoring the criticality of adequately preparing for potential incidents, promptly detecting them, effectively responding to them, and conducting thorough post-incident activities.Both plans place significant emphasis on the necessity of adequate preparedness for incidents. This include the establishment of a structured incident response capability, the formulation of policies, and the formulation of tailored processes for various categories of incidents.The importance of post-incident activities, particularly the concept of "lessons learned," is emphasised in both texts. This process include conducting a comprehensive analysis of the events, assessing the efficacy of the implemented measures, and implementing appropriate modifications to mitigate the occurrence of similar accidents in the future.Both plans emphasise the importance of documenting incidents, encompassing the process of their discovery as well as the subsequent actions undertaken in response.

**Differences:**

There exist disparities between the two entities.The "Computer Security Incident Handling Guide" provides a comprehensive analysis from a strategic and organisational standpoint, with a specific emphasis on the development of policies, strategies, and procedures. On the other hand, the "Sample Intrusion Detection Incident Response Plan" exhibits a more tactical approach by providing a comprehensive outline of the actions to be executed in response to an occurrence.The event categorization plan utilises a system that classifies incidents according to their level of threat, hence facilitating the prioritisation and customization of response strategies. The guide does not include an in-depth analysis of such categorization.The sample plan focuses a significant emphasis on forensic procedures, including the thorough examination of logs and the systematic interrogation of witnesses. Although the guide does cover these aspects, it lacks a comprehensive procedure.The sample plan expressly emphasises the importance of informing other agencies for prospective prosecution, while the guidance places greater emphasis on the sharing of information with external parties for the purpose of joint defence.

**Critical Analysis:**

The comparison between depth and breadth is a central focus of this analysis. The guide offers a comprehensive perspective, highlighting the significance of a methodical approach. In contrast, the sample plan delves further into the particulars, providing a more detailed examination. The appropriateness of each option may vary depending on the maturity level of the organisation.

The comparative analysis between flexibility and rigidity reveals that the inclusion of precise procedures in the sample plan can yield advantageous outcomes in terms of enhancing clarity in high-pressure scenarios. Nevertheless, it is plausible that this could also result in inflexibility. The guide's overarching methodology affords greater adaptability, while potentially necessitating increased cognitive deliberation in the event of an issue.

**Recommendations:**

The adoption of a hybrid strategy is recommended for organisations, where they combine the strategic insights derived from the guide with the tactical steps outlined in the sample plan. This approach guarantees the simultaneous achievement of flexibility and clarity in the context of occurrences.

Frequent Updates: Due to the ever-changing nature of security threats, it is imperative to consistently revise the incident response plan, integrating insights gained from previous occurrences and adaptations in the threat environment.

Training and drills are essential components in ensuring the efficacy of an incident response plan. It is imperative to conduct frequent training sessions and simulated event drills to enhance preparedness and response capabilities. This practise guarantees that all individuals involved in a particular endeavour has a comprehensive understanding of their respective duties and obligations.

External Collaboration: It is advisable for organisations to engage in collaborative efforts with external entities, such as industry groups or governmental agencies, in order to remain abreast of current dangers and optimal methodologies.The establishment of a feedback loop is crucial following any significant incident, as it allows all parties involved to provide their perspectives on both successful aspects and areas for improvement. This practise guarantees the ongoing enhancement of the incident response procedure.

**Conclusion:**

In conclusion, while both documents provide valuable insights into incident response, a combination of their strengths, tailored to the specific needs and context of the organization, would yield the most effective incident response plan.

**PART2**

**Identifying and Classifying a Security Breach**

**1. Identification:**

* **Monitoring and Logging**: Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for suspicious activities. Regularly review system and application logs.
* **User Reports**: Sometimes, end-users might notice and report unusual activities, such as unexpected password reset emails or unfamiliar devices accessing their accounts.
* **Anomalies in Traffic Patterns**: A sudden spike in traffic or unusual times of activity can indicate a breach.
* **Unusual System Behavior**: Systems crashing, running slowly, or displaying unexpected messages can be indicators.

**2. Classification:**

Once identified, classify the breach based on:

* **Source**: Internal (e.g., disgruntled employee) vs. External (e.g., hackers).
* **Type of Attack**: E.g., DDoS attack, malware, phishing, SQL injection, etc.
* **Severity**: Based on the potential impact on the organization's operations, reputation, and finances.
* **Data Compromised**: Personal data, financial data, intellectual property, etc.

**Impact Assessment:**

* **Data Loss**: Determine the type and amount of data compromised. Personal data breaches can lead to regulatory fines and loss of trust.
* **Operational Impact**: Assess how the breach affects daily operations. For instance, a ransomware attack can halt operations entirely.
* **Financial Impact**: This includes immediate costs like ransom payments, and long-term costs like regulatory fines, lawsuits, and loss of business.
* **Reputational Impact**: A significant breach can erode trust, leading to loss of customers and partners.

**Recommendations:**

* **Regular Audits**: Conduct regular security audits to identify vulnerabilities and rectify them.
* **Employee Training**: Regularly train employees on security best practices and how to recognize phishing attempts and other threats.
* **Multi-Factor Authentication (MFA)**: Implement MFA for accessing sensitive systems and data.
* **Backup**: Regularly back up data and ensure it can be restored quickly in case of ransomware or other data-loss incidents.
* **Patch Management**: Regularly update and patch software to protect against known vulnerabilities.
* **Incident Response Plan**: Have a clear plan detailing steps to take in case of a breach. This should include communication plans, both internally and with affected customers or partners.

**Prioritization:**

* **Severity of Impact**: Incidents that can cause significant operational, financial, or reputational damage should be prioritized.
* **Breadth of Impact**: Incidents affecting a larger number of users or systems should be given priority.
* **Regulatory Implications**: Incidents that might lead to regulatory fines or legal actions should be prioritized.

**Justification:**

Regular audits, employee training, MFA, backups, patch management, and having an incident response plan are foundational security practices recommended by cybersecurity experts globally. These measures not only help in preventing incidents but also in mitigating their impact. Prioritizing based on severity, breadth, and regulatory implications ensures that resources are allocated where they can have the most significant effect in reducing harm.

**Conclusion:**

Identifying and classifying security breaches promptly and accurately is crucial for effective response and mitigation. By understanding potential threats, assessing their impact, and implementing recommended measures, organizations can significantly reduce their risk profile and ensure resilience against cyber threats.