6-2 Journal: Policy

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

5 August 2024

An Acceptable Use Policy (AUP) is crucial for establishing the rules of engagement for all users of an organization's IT systems and resources. It delineates acceptable and unacceptable behaviors to safeguard the organization from potential internal and external threats that could compromise its digital assets. The AUP educates users about their responsibilities and the consequences of non-compliance, which includes potential legal actions or termination. For instance, in 2018, a primary healthcare provider faced significant fines after an employee breached their AUP by improperly accessing and sharing protected health information, highlighting the necessity of strict enforcement. This policy is about controlling and protecting the integrity of the organization's technical resources. By setting clear usage boundaries, the AUP helps prevent activities that could lead to security breaches, data loss, or legal liabilities. Reflecting on insights from Nagar (2023), a well-defined AUP aligns with the strategic goals of an organization's cybersecurity governance by ensuring that all users are aware of and comply with security protocols, thereby reducing the organization's risk exposure. This policy supports the governance framework by establishing accountability and reinforcing the organization's security culture.

The Incident Response Policy is a cornerstone of an organization's cybersecurity strategy. It outlines how the organization responds to detected cybersecurity incidents, emphasizing the importance of swift and effective handling. This approach minimizes the impact on operations and reduces recovery time and costs. The policy provides a structured approach for the security team to follow in the case of various types of cybersecurity incidents, ensuring that every potential threat is addressed systematically and efficiently. For example, during the 2017 global ransomware attack that affected thousands of organizations, those with effective incident response policies were able to quickly isolate affected systems, apply patches, and restore data

from backups, significantly minimizing downtime and financial impact. The policy includes clear procedures for incident identification, classification, response, recovery, and post-incident analysis to improve future response efforts. It serves as a blueprint that guides the security team through the chaos often accompanying a security breach. According to Nagar (2023), having a robust incident response plan enhances stakeholders' trust in the organization's ability to manage and mitigate cyber risks. It aligns with the best practices in cybersecurity by not only addressing the technical response but also incorporating the management of communications with internal and external stakeholders during and after an incident.

The Password Management Policy is a critical component of an organization's cybersecurity strategy, particularly in the digital transformation era. It ensures that strong and effective passwords are used to secure access to all organizational systems. The policy outlines standards for password complexity, such as using alphanumeric and special characters, the frequency of password changes, and the prohibition of password reuse. Effective password management reduces vulnerabilities that attackers can exploit and is a first defense against unauthorized access. For instance, a significant university recently suffered a security breach when hackers accessed administrative accounts with weak passwords, leading to the theft of personal data from thousands of students—a preventable mishap with stricter password policies. The policy is essential in the digital transformation era, where the security perimeter has expanded to include remote access points and cloud services. It should also address the storage and transmission of passwords to avoid exposure during data breaches. As part of a comprehensive cybersecurity governance framework, the Password Management Policy ensures that security measures keep pace with the evolving threat landscape, safeguarding sensitive information and maintaining the integrity and availability of systems (Nagar, 2023).

References

Nagar, R. (2023, July 9). *(25) The Significance of Cybersecurity Governance in the era of Digital Transformation | LinkedIn*. https://www.linkedin.com/pulse/significance-cybersecurity-governance-era-digital-ronak-nagar/