Topic 8 Discussion 1

Attempting to make framework-compliant policies is a difficult task for cybersecurity experts. However, it is well known that implementing these policies is an even more difficult task, as it takes stakeholder buy-in and understanding in order for policies to be fully realized parts of the infrastructure. With this in mind, research and discuss implementation strategies that you would use to ensure that the security policies that have been set are being followed and that compliance levels remain well within the standards outlined in the framework.

Hello Class,

To ensure cybersecurity policies are followed and compliance levels remain within framework standards, a multi-faceted implementation strategy is crucial, prioritizing stakeholder buy-in. An effective approach involves clear and consistent communication about the purpose and benefits of the policies. This can include regular workshops, training sessions, and informational materials tailored to different stakeholder groups. For instance, a policy mandating multi-factor authentication might be explained to end-users in terms of protecting their personal data and simplifying access, while explaining to IT staff the technical benefits and integration ease. Research highlights the effectiveness of the Theory of Planned Behavior (TPB) in understanding cybersecurity policy implementation and compliance behavior, suggesting that influencing attitudes, subjective norms, and perceived behavioral control among stakeholders is key(Katrakazas & Papastergiou, 2024).

Furthermore, engaging stakeholders in the policy development process can significantly enhance buy-in. A systemic, AI-powered approach to stakeholder needs analysis, as explored in MDPI research, can help identify and address concerns early on, ensuring policies are practical and relevant. This collaborative method ensures that policies are not merely imposed but are co-created, fostering a sense of ownership.

Regular audits and assessments are vital to monitor compliance. The Cybersecurity and Infrastructure Security Agency (CISA) provides guidance on cyber hygiene, which includes practices like mandatory training, lockout policies, and revoking ex-employees' login information, all of which contribute to a secure environment(USDHS, 2020). These practices should be continuously reviewed and updated based on audit findings and evolving threat landscapes.

Finally, leveraging technology for enforcement and monitoring can automate compliance checks and provide real-time feedback. This includes using security information and event management (SIEM) systems and intrusion detection systems. The development of cybersecurity policy framework requirements for interconnected health data spaces, as discussed in a May 2024 paper, emphasizes the need for robust, interoperable solutions to ensure compliance in complex environments(Omoyiola, 2020).

References:

Katrakazas, Panagiotis , and Spyros Papastergiou. “A Stakeholder Needs Analysis in Cybersecurity: A Systemic Approach to Enhancing Digital Infrastructure Resilience.” *Businesses*, vol. 4, no. 2, 17 June 2024, pp. 225–240, https://doi.org/10.3390/businesses4020015.

Omoyiola, Bayo. *Exploring Strategies for Enforcing Cybersecurity Policies Exploring Strategies for Enforcing Cybersecurity Policies*. 2020.

USDHS. “Cybersecurity Framework Implementation Guide.” *CISA*, May 2020, www.cisa.gov/sites/default/files/publications/Emergency\_Services\_Sector\_Cybersecurity\_Framework\_Implementation\_Guidance\_FINAL\_508.pdf.