**Summary Post**

**Knowledge and Understanding**

Cybersecurity is a global concern due to our reliance on digital infrastructure and the risks of cyber-attacks. Companies like Amazon must invest in cybersecurity to protect economic interests, comply with regulations, and maintain their reputation. My initial post highlighted Amazon’s cybersecurity measures, emphasising protecting customer data and ensuring business continuity. The economic benefits of investing in cybersecurity include avoiding high costs associated with data breaches and maintaining customer trust, crucial for competitiveness (Brookshear, 2020; Anderson, 2008).

Peers expanded on this by highlighting the importance of cybersecurity frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001, which help organisations manage and reduce risks. Continuous monitoring and updating security protocols to address evolving threats were also emphasised (Williams, 2019).

Engaging with peers provided a deeper understanding of cybersecurity’s multifaceted nature. One peer noted the economic implications of cybersecurity investments, pointing out that while initial costs might be high, the long-term benefits far outweigh these expenses. Another peer highlighted the legal implications, explaining how non-compliance with data protection regulations like GDPR can result in hefty fines and loss of customer trust (Troncoso, 2019).

**Criticality evaluating the feedback**

I agree that adopting comprehensive cybersecurity frameworks is crucial. Integrating cybersecurity into the company culture, as suggested by a peer, ensures all employees are aware of their role in maintaining security, creating a more resilient defence system. However, it is important to note that while frameworks provide guidelines, the dynamic nature of cyber threats requires continuous adaptation and real-time response capabilities (Anderson, 2008).

**Conclusion**

The peer feedback significantly enhanced my understanding of cybersecurity. By considering economic, legal, and cultural perspectives, I have gained a more comprehensive view of why cybersecurity is vital for organisations globally. This discussion has highlighted the importance of a multi-faceted approach to cybersecurity, integrating technical measures with strategic and organisational practices.

**References**

* Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*. 3rd ed. Indiana: Wiley & Sons.
* Brookshear, J. G. (2020). *Computer Science: an overview*. 13th ed. New York: Addison Wesley Longman Inc.
* Department of Computer Science. (2019). Cybersecurity Roles and Job Titles. School of Engineering & Applied Sciences, The George Washington University.
* Troncoso, C. (2019). Privacy & Online Rights Knowledge Area Issue 1. *The Cyber Security Body of Knowledge*.
* VanSyckel, L. (2018). Introducing Cybersecurity. Sealevel Systems, Inc.
* Williams, L. (2019). Secure Software Life Cycle. *Knowledge Area Issue 1. The Cyber Security Body of Knowledge*.