Topic 7 Discussion 1

Internet use within any business has become commonplace. Given the recent work from home movement, evaluate the implication of internet use within a small or medium-sized business from the perspective of intellectual property and data protection. How do growing trends in technology hinder or help the growth in home-based workers?

Hello Class,

The recent shift towards remote work has significantly impacted small and medium-sized businesses (SMBs) regarding internet use, particularly concerning intellectual property (IP) and data protection(Alashwali et al., 2025). As employees increasingly access company resources from home, the risk of data breaches and IP theft has escalated. Remote work environments often rely on personal devices and unsecured networks, which can expose sensitive information to cyber threats. To mitigate these risks, SMBs must implement robust cybersecurity measures, including strong passwords, multi-factor authentication, and comprehensive employee training on safe internet practices(Fortinet, 2024). Additionally, clear policies regarding IP ownership and data handling are essential to protect proprietary information.

The growing trends in technology present both challenges and opportunities for home-based workers. On the one hand, advancements in cloud computing and collaborative tools enhance productivity and facilitate seamless communication among remote teams. These technologies allow for centralized data storage and improved accessibility, which can drive efficiency. However, they also introduce vulnerabilities if not properly secured. For instance, the rise of Bring Your Own Device (BYOD) policies can complicate data protection efforts, as personal devices may not meet the same security standards as company-issued equipment(ACISITSolutions, 2024).

In addition the rapid pace of technological change necessitates continuous investment in cybersecurity infrastructure and employee training. SMBs must stay informed about emerging threats and adapt their security protocols accordingly. This ongoing commitment to security can be resource-intensive, particularly for smaller organizations with limited budgets. Ultimately, the success of remote work models hinges on balancing the benefits of technological advancements with the need for stringent data protection measures(Mills & Mills, 2024). By fostering a culture of security awareness and implementing effective policies, SMBs can navigate the complexities of internet use in a remote work environment while safeguarding their intellectual property.

References:

ACISITSolutions. (2024, August 5). *The Impact of Remote Work on IT Infrastructure for Small Businesses - ACIS IT Solutions | Managed Service Provider Springfield, MO*. Acisitsolutions.com. https://acisitsolutions.com/it-infrastructure-for-small-business-remote-work-impact/

Alashwali, E., Peca, J., Lanyon, M., & Cranor, L. F. (2025). Work from home and privacy challenges: what do workers face and what are they doing about it? *Journal of Cybersecurity*, *11*(1). https://doi.org/10.1093/cybsec/tyaf010

Fortinet. (2024). *Work From Home: Evolving Cybersecurity Risks*. Fortinet. https://www.fortinet.com/resources/cyberglossary/work-from-home-cybersecurity-risks

Mills, D., & Mills, T. (2024, February 8). *Security Implications of a Remote Work Environment | Carr, Riggs & Ingram*. Carr, Riggs & Ingram. https://www.criadv.com/insight/security-implications-of-a-remote-work-environment/