Topic 4 Discussion 2

As a security professional, what strategies would you recommend to secure information systems in order to combat daily occurrences of cybersecurity attacks? Be as detailed as possible.

Hello Class,

A robust security strategy requires a multi-layered approach, combining preventative, detective, and responsive measures. Firstly, a strong foundation is built through implementing robust access controls, including multi-factor authentication (MFA) to mitigate credential stuffing and phishing attacks. Regular security awareness training for employees is paramount to address the human element, a common vulnerability in many attacks(CISA, 2025) Secondly, network security is critical. This involves deploying firewalls, intrusion detection/prevention systems (IDS/IPS), and regularly updating security software to patch vulnerabilities. Regular vulnerability scanning and penetration testing are also essential for proactive identification and remediation of weaknesses(National Security Agency, 2018). Thirdly, data protection is paramount. Data loss prevention (DLP) tools should be employed to monitor and control sensitive data movement. Data encryption, both at rest and in transit, is crucial to protect confidentiality. Regular data backups are essential for business continuity and disaster recovery(NIST, 2020). Fourthly, incident response planning is vital. This involves establishing clear procedures for identifying, containing, eradicating, recovering from, and learning from security incidents. Regular simulations and drills are crucial to ensure preparedness(CISA, 2023). Finally, continuous monitoring and logging are essential. Security information and event management (SIEM) systems can help organizations aggregate and analyze security logs from various sources, enabling faster threat detection and response(Sukianto, 2025). The integration of these strategies, coupled with continuous improvement based on threat intelligence and security audits, forms a comprehensive approach to securing information systems and mitigating the risks of daily cybersecurity attacks.

References:

CISA. (2025). *Cybersecurity Best Practices*. Www.cisa.gov. https://www.cisa.gov/topics/cybersecurity-best-practices

CISA. (2023). *Cybersecurity Incident Response | CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response

National Security Agency. (2018). *NSA’S Top Ten Cybersecurity Mitigation Strategies*. https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf

NIST. (2020, January 12). *NIST SP 800-34*. NIST. https://www.nist.gov/privacy-framework/nist-sp-800-34

Sukianto, A. (2025, January 2). *10 Ways to Reduce Cybersecurity Risk for Your Organization*. Upguard. https://www.upguard.com/blog/reduce-cybersecurity-risk