Topic 7 Discussion 2

Implementing a successful cybersecurity program does not only depend on having the latest security and software applications. It requires an effective security policy that includes administrative policy, physical security controls, and technology. The organization's security depends on all these different security controls to secure an asset using compliance-driven directives. Research and discuss different ways for an organization to implement an administrative policy for the onboarding and offboarding of employees to ensure the security of the organization's intellectual property.

Hello Class,

During the onboarding process, a key administrative control is the clear definition and communication of IP policies to new hires. This includes outlining what constitutes company intellectual property, the acceptable use of company data and systems, and the consequences of policy violations(Notchup Team, 2023). Access to sensitive information and systems should be granted on a need-to-know basis, with thorough background checks and NDAs (Non-Disclosure Agreements) being standard practice. Training on cybersecurity best practices, including password management and recognizing phishing attempts, should also be a mandatory part of onboarding(Scrut, 2023).

The offboarding process is equally critical, as inadequate procedures can lead to data breaches and IP theft. Organizations must implement a structured offboarding checklist that ensures the timely and complete revocation of all access privileges, including physical access to facilities and logical access to company networks, applications, and data(Rao, 2025). This process should involve the secure retrieval of all company assets, such as laptops, mobile devices, and access cards. Furthermore, a final review of the departing employee's access logs can help identify any suspicious activity prior to their departure. A robust offboarding policy directly mitigates the risk of data exfiltration and system sabotage by disgruntled former employees.

By implementing robust security measures during offboarding, organizations can mitigate the risk of data breaches, protect intellectual property, and ensure compliance. Conversely, a well-orchestrated offboarding process reduces the risk of data breaches and unauthorized access following an employee's departure(Kapolas, 2025). Senior-level employees, who often have access to financial, legal, and intellectual property rights data, require particularly swift access termination upon departure. Inadequate offboarding can lead to data breaches, intellectual property theft, compliance violations, and even wrongful termination claims. Therefore, establishing clear, actionable administrative policies for both onboarding and offboarding is a fundamental step in protecting an organization's most valuable assets.

References:

Kapolas, Caitlin. “Employee Offboarding Excellence: The 5-Step Strategic Framework.” *Lifthcm.com*, Lift HCM, 21 Apr. 2025, lifthcm.com/article/employee-offboarding-strategies. Accessed 16 Aug. 2025.

Notchup Team. “Best Practices for Securely Onboarding and Offboarding Employees.” *Www.notchup.com*, 26 June 2023, www.notchup.com/insights/securely-onboarding-and-offboarding-employees.

Rao, Rohit. “Employee Offboarding: 5 Security Guidelines for a Remote Workplace | Zluri.” *Zluri.com*, 2025, www.zluri.com/blog/offboarding-employees-security-guidelines. Accessed 16 Aug. 2025.

Scrut. “Onboarding and Offboarding Employees for Risk Prevention.” *Scrut Automation*, 20 Apr. 2023, www.scrut.io/post/a-guide-to-onboarding-and-offboarding-employees-for-risk-prevention.