CSIT988 Security, Ethics and Professionalism

Workshop 10 for Week 11

1. List and describe the criteria for selecting InfoSec personnel.

Personnel should be technically qualified InfoSec generalists, with a solid understanding of how organizations operate without being overly specialized.

2. What are the critical actions that management must consider taking when dismissing an employee? Do these issues change based on whether the departure is friendly or hostile?

When dismissing an employee, the organization must take measures to ensure business continuity and protect all information to which the individual had access. Standard procedures for dismissal include disabling the employees access, requiring the employee to return all media, changing locks and access cards. The organization should also conduct an exit interview to remind the employee of contractual obligations and non-disclosure agreements. If the departure is hostile, all exit actions should take place immediately and the employee should be escorted from the facility. If the separation is friendly, the organization should consider removing access immediately if it appears maintaining control over information may be a problem.

3. How do the security considerations for temporary or contract workers differ from those for regular employees?

Temporary employees or contract workers often have access to the sensitive information. Therefore, an organization must have an agreement with the individual's employer that they will censure the individual if policies are violated. For contract employees, it is important to have strong service agreements. If needed, contractors should be escorted through facilities.

4. What is separation of duties? How can this method be used to improve an organization's InfoSec practices?

Separation of duties, two-person control, job and task rotation, mandatory vacations, and least privilege are among the practices and methods recommended to minimize employees' opportunities to misuse information.