Module 5: Security Personnel

- The placement of the information security function within the organization is a key decision facing the organization. The most popular options involve placing the information security function within the IT function or within the physical security function. Organizations searching for a rational compromise should place the information security function where it can balance its need to enforce organizational policy with its need to deliver service to the entire organization.

- The selection of information security personnel is based on a number of criteria. Some of these factors are within the control of the organization and others are not.

- In most cases, organizations look for a technically qualified information security generalist with a solid understanding of how an organization operates in addition to the following attributes:

    - An attitude that information security is usually a management problem, not an exclusively technical problem
    - Good people skills, communications skills, and writing skills and a tolerance for users
    - An understanding of the role of policy in guiding security efforts
    - An understanding of the role of education and training in making the users part of the solution
    - An understanding of the threats facing an organization and how these threats can become attacks, as well as an understanding of how to protect the organization from information security attacks
    - A working knowledge of many of the most common technologies and a general familiarity with most mainstream IT technologies

- Many information security professionals enter the field through one of two career paths: via law enforcement or military personnel, or from other technical information systems professions. In recent years, college students have been able to take courses that prepare them to enter the information security workforce directly.

- During the hiring process for an information security position, an organization should use standard job descriptions to increase the degree of professionalism among applicants and also to make sure the position's roles and responsibilities are consistent with those of similar information security positions in other organizations. Studies of information security positions have found that they can be classified into one of three areas: those that define, those that build, and those that administer.

- When filling various information security positions, many organizations indicate the level of proficiency required for the job by specifying that the candidate have recognizable certifications. Some of the more popular certifications are:

- (ISC)² International Information Systems Security Certification Consortium is considered one the foremost organizations offering information security certifications today.
    - (ISC)² family of certifications:
        - Certified Information Systems Security Professional (CISSP)
        - Systems Security Certified Practitioner (SSCP)
        - Associate of (ISC)²
        - Certification and Accreditation Professional (CAP)

- (ISACA) Information Systems Audit and Control Association was founded by a group of individuals with similar jobs in computer auditing who sought to provide a centralized source of information and guidance.
    - ISACA family of certifications:
        - Certified Information Systems Auditor (CISA)
        - Certified Information Security Manager (CISM)

- The System Administration, Networking, and Security Organization, better known as SANS developed a series of technical security certifications in 1999 that are known as the Global Information Assurance Certification (GIAC).
    - Global Information Assurance Certification (GIAC) family of certifications
        - Audit
            - GIAC Certified ISO-17799 Specialist (G7799)
            - GIAC Systems and Network Auditor (GSNA)
        - Legal
            - GIAC Legal Issues (GLEG)
        - Management
            - GIAC Information Security Professional (GISP)
            - GIAC Security Leadership Certification (GSLC)
            - GIAC Certified Project Manager Certification (GCPM)
        - Security Administration
            - GIAC Information Security Fundamentals (GISF)
            - GIAC Security Essentials Certification (GSEC)
            - GIAC Web Application Penetration Tester (GWAPT)
            - GIAC Certified Forensic Analyst (GCFA)
            - GIAC Certified Enterprise Defender (GCED)
            - GIAC Certified Firewall Analyst (GCFW)
            - GIAC Certified Intrusion Analyst (GCIA)
            - GIAC Certified Incident Handler (GCIH)
            - GIAC Certified Windows Security Administrator (GCWN)
            - GIAC Certified UNIX Security Administrator (GCUX)
            - GIAC Certified Penetration Tester (GPEN)
            - GIAC Reverse Engineering Malware (GREM)
            - GIAC Assessing Wireless Networks (GAWN)

- Software Security
    - GIAC Secure Software Programmer—.NET (GSSP-NET)
    - GIAC Secure Software Programmer—Java (GSSP-JAVA)

- Security Certified Professional (SCP) is one of the newer certifications in the information security discipline is the Security Certified Program's hands-on IT security certifications.

- CompTIA Security+ has introduced the first truly vendor-neutral technical professional IT certifications - the A series.

- Certified Computer Examiner (CCE) certification is a computer forensics certification provided by the International Society of Forensic Computer Examiners.

▪ The general management community of interest should integrate solid concepts regarding information security into the organization's employment policies and practices. Areas where information security should be a consideration include:

- Background checks, a background check should be conducted before an organization extends an offer to a candidate. A background check is an investigation into the candidate's past that specifically looks for criminal or other types of behavior that could indicate potential for future misconduct.

- Employment contracts, once a candidate has accepted a job offer, the employment contract becomes an important security instrument.

- New hire orientation, when new employees are introduced into the organization's culture and workflow, they should receive as part of their employee orientation an extensive information security briefing. All major policies should be explained, along with the procedures for performing necessary security operations and the new position's other information security requirements.

- Performance evaluation, to heighten information security awareness and minimize workplace behavior that poses risks to information security, organizations should incorporate information security components into employee performance evaluations.

- Termination
    - Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting. Before the employee knows that he or she is leaving, or as soon as the hostile resignation is tendered, the security staff should terminate all logical and keycard access. In the case of involuntary terminations, the employee should be

escorted into the supervisor's office for the bad news. Upon receiving the termination notice or tendering a hostile resignation the employee should be escorted to his or her office, cubicle, or personal area and allowed to collect personal effects. No organizational property should be allowed to be taken from the premises, including diskettes, pens, papers, and books. Regardless of the claim the employee has on organizational property, he or she should not be allowed to take it from the premises.

- Friendly departures include resignation, retirement, promotion, or relocation. In this case, the employee may have tendered notice well in advance of the actual departure date. This scenario actually makes it much more difficult for the security team to maintain positive control over the employee's access and information usage. Employee accounts are usually allowed to continue to exist, though an expiration date can be set for the employee's declared date of departure. Another complication associated with friendly departures is that until their departure date employees can come and go at will, which means they are usually collecting their own belongings and leaving under their own cognizance. As with hostile departures, employees should be asked to drop off all organizational property on their final way out.

- Organizations may need the special services of nonemployees, but the resulting relationships should be carefully managed to prevent information leaks or theft. The categories of nonemployees are:

    - Temporary employees are hired by the organization to serve in a temporary position or to supplement the existing workforce.

    - Contract employees are typically hired to perform specific services for the organization. In such cases, the host company often makes a contract with a parent organization rather than with an individual for a particular task.

    - Consultants sometimes onsite contracted employees are self-employed or are employees of an organization hired for a specific, one-time purpose. These people are typically referred to as consultants, and they have their own security requirements and contractual obligations. Consultants should have all specific requirements for information or facility access integrated into their contracts before these individuals are allowed into the workplace.

    - Business partners, on occasion, businesses find themselves in strategic alliances with other organizations wishing to exchange information, integrate systems, or simply discuss operations for mutual advantage.

- Separation of duties is a control used to reduce the chance of any one individual violating information security and breaching the confidentiality, integrity, or availability of information. The principle behind this control is that any major task that involves sensitive information should require two people to complete.

- Privacy and security of personnel and personal data have government-mandated requirements for special security considerations and must be covered in the organization's information security program.

Reference:

Principles of Information Security by: Michael E. Whitman & Herbert J. Mattord