

# IT 4823

## Information Security Administration

### Human Resources Security



Notice: This session is  
being recorded.

Some lecture slides prepared by Dr Lawrie Brown for “*Computer Security: Principles and Practice*”, 1/e, by William Stallings and Lawrie Brown,.



Copyright © 2016 by Bob Brown



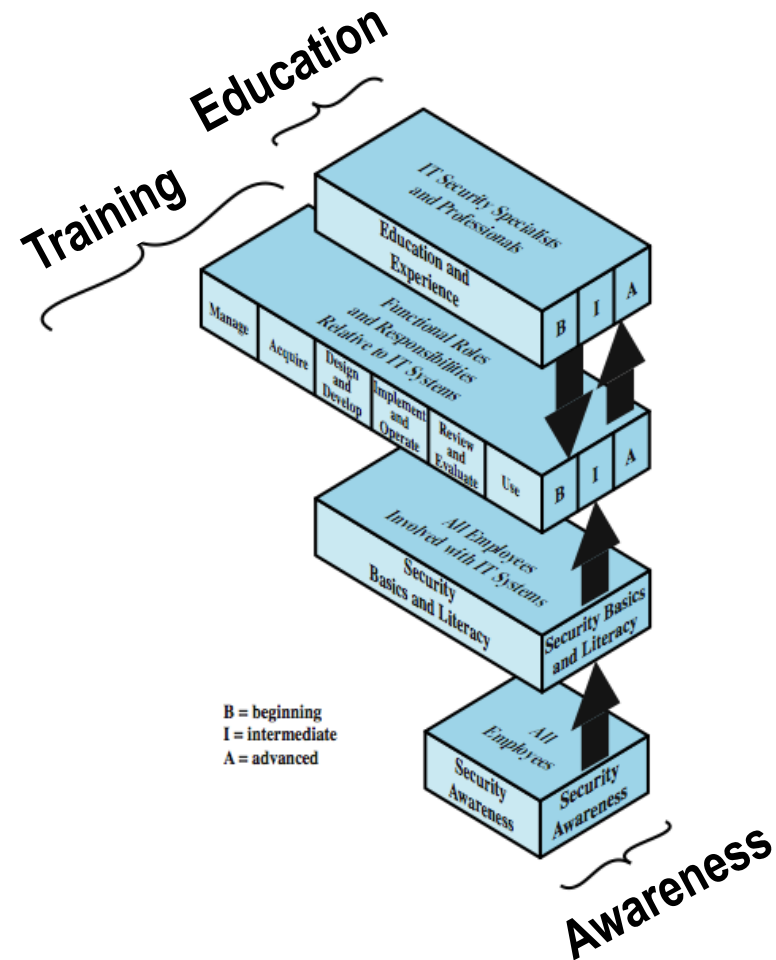
# Human Factors

- An important, broad area
- With a few key topics:
  - Security awareness, training, and education
  - Organizational security policy
  - Personnel security
  - E-mail and World Wide Web use policies
  - The jobs of security professionals
- Two areas to consider
  - Human factors and the organization
  - Staffing the information security function

# Security Awareness, Training, and Education

- A prominent topic in various standards
- Can provide benefits in:
  - improving employee behavior
  - increasing employee accountability
  - mitigating liability for employee behavior
  - complying with regulations and contractual obligations

# Learning Continuum



# Awareness

- Seeks to inform and focus an employee's attention on security issues
  - threats, vulnerabilities, impacts, responsibility
- Must be tailored to organization's needs...
- ...using a variety of means: events, promo materials, briefings, policy documents
- Every organization should have an employee security policy document

# Training

- Teaches what people should do and how they do it to perform IT tasks securely
- Encompasses a spectrum covering:
  - general users
    - good computer security practices
  - programmers, developers, maintainers
    - security mindset, secure code development
  - managers
    - tradeoffs involving security risks, costs, benefits
  - executives
    - risk management goals, measurement, leadership

# Education

- Most in depth
- Targeted at security professionals whose jobs require expertise in security
- More about employee career development
- More focused on underlying principles than specific tasks
- Often provided by outside sources
  - college courses
  - specialized educational programs

# Education and Training

The purpose of higher education is not to produce job ready graduates, it's to produce life ready citizens.

*– James Wagner, President, Emory University  
April 3, 2013*



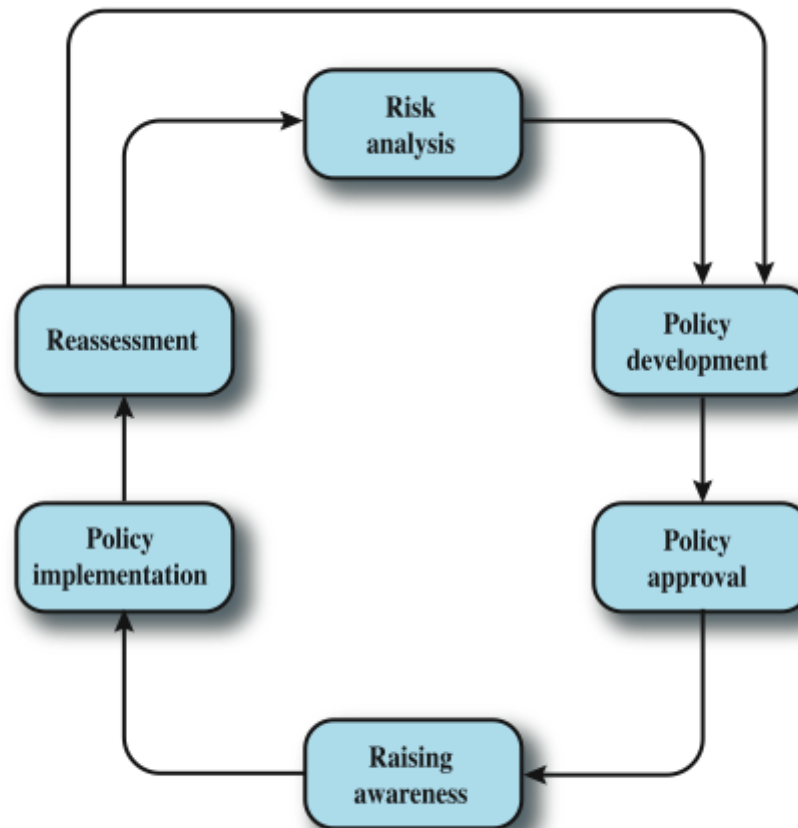
# Personnel Security Policy

- “A formal statement of rules by which people given access to organization’s technology and information assets must abide”
- Policy defines “security.”
- The word “policy” can also be used in other contexts.

# Personnel Security Policy

- Every organization needs a written security policy document for employees...
- ...to define acceptable behavior, expected practices, and responsibilities
  - makes clear what is protected and why
  - articulates security procedures / controls
  - states responsibility for protection
  - provides basis to resolve conflicts
- Must reflect executive security decisions to:
  - protect information
  - comply with law
  - meet organizational goals

# Security Policy Lifecycle



# Policy Document Responsibility

- Security policy needs broad support
- Especially from top management
- Should be developed by a team including:
  - site security administrator,
  - IT technical staff,
  - representatives of user constituencies (*e.g.* business divisions)
  - security incident response team
  - responsible management
  - legal counsel

# Document Content

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- Which laws / regulations is it based on?
- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?
- What information assets must be protected?
- What are users actually required to do?
- How should security breaches be reported?
- What is the effective date / expiration date of it?

# Security Policy Topics

- Principles
- Organizational reporting structure
- Physical security
- Hiring, management, and firing
- Data protection
- Communications security
- Hardware
- Software
- Operating systems

# Security Policy Topics

- Technical support
- Privacy
- Access
- Accountability
- Authentication
- Availability
- Maintenance
- Violation reporting
- Business continuity
- Supporting information

# Resources

- ISO 27002 (Renumbered from ISO 17799 and British Standard 7799)
  - Widely-used international standard
  - With a comprehensive set of controls
  - Provides a convenient framework for policy authors
- COBIT
  - Business-oriented set of standards
  - Includes IT security and control practices
- Standard of Good Practice for Information Security
- Other organizations, *e.g.* CERT-CC, CIO.gov



# Personnel Security Considerations

- Employment practices
- Job descriptions
- Background checks
- Employment contracts
- Orientation and training
- Performance evaluation
- Termination

# Employment Policies and Practices

- Management should integrate information security concepts into the organization's employment policies and practices
- The organization should make information security a documented part of every employee's job description

# Employment Policies and Practices

- From an information security perspective, hiring of employees is a responsibility laden with potential security pitfalls. (Don't hire a crook.)
- CISO and information security manager should provide human resources with information security input to personnel hiring guidelines

# Job Descriptions

- Integrating information security perspectives into hiring process begins with reviewing and updating all job descriptions
- Organization should avoid revealing access privileges to prospective employees when advertising open positions

# Background Checks

- Investigation into a candidate's past
- Should be conducted before organization extends offer to candidate
- Background checks differ in level of detail and depth with which candidate is examined
- May include identity check, education and credential check, previous employment verification, references check, drug history, credit history, and more
- *Always* check references.
- Do not hire a “bad mouth!”

# Employment Contracts

- Once a candidate has accepted the job offer, employment contract becomes important security instrument
- Many security policies require an employee to agree in writing
- You can specify “employment contingent upon agreement,” whereby employee is not offered the position unless binding organizational policies are agreed to

# New Hire Orientation

- New employees should receive extensive information security briefing on policies, procedures and requirements for information security
- Levels of authorized access are outlined; training provided on secure use of information systems
- By the time employees start, they should be thoroughly briefed and ready to perform duties securely

# On-the-Job Security Training

- Organization should conduct periodic security awareness training
- Keeping security at the forefront of employees' minds and minimizing employee mistakes is important part of information security awareness mission
- External and internal seminars also increase level of security awareness for all employees, particularly security employees



# Performance Evaluation

- Organizations should incorporate information security components into employee performance evaluations
- Employees pay close attention to job performance evaluations; if evaluations include information security tasks, employees are more motivated to perform these tasks at a satisfactory level

# Termination

- When employee leaves organization, there are a number of security-related issues
- Key idea is protection of all information to which employee had access:
  - Keys, keycards, badges, etc.
  - Access codes
  - Removable media
- Many organizations use the exit interview to remind former employee of contractual obligations and to obtain feedback

# Hostile Termination

- Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting
- Before employee is aware, all logical and keycard access is terminated
- Employee collects all belongings and surrenders all keys, keycards, and other company property
- Employee is then escorted out of the building

# Friendly Termination

- Friendly departures include resignation, retirement, promotion, or relocation
- Employee may be notified well in advance of departure date
- More difficult to maintain positive control over employee's access and information usage
- Employee access usually continues with new expiration date
- Employees come and go at will, collect their own belongings, and leave on their own

# Activities Upon Termination

- Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores
- It is possible that employees foresee departure well in advance and begin collecting organizational information for their future employment
- Only by scrutinizing systems logs after employee has departed can organization determine if there has been a breach of policy or a loss of information
- If information has been copied or stolen, action should be declared an incident and the appropriate policy followed

# Security Considerations For Nonemployees

- Individuals not subject to screening, contractual obligations, and eventual secured termination often have access to sensitive organizational information
- Relationships with these individuals should be carefully managed to prevent possible information leak or theft

# Temporary Employees

- Hired by organization to serve in temporary position or to supplement existing workforce
- Often not subject to contractual obligations or general policies; if temporary employees breach a policy or cause a problem, possible actions are limited
- Access to information for temporary employees should be limited to that necessary to perform duties
- Temporary employee's supervisor must restrict the information to which access is possible

# Contract Employees

- Typically hired to perform specific services for organization
- Host company often makes contract with parent organization rather than with individual for a particular task
- In secure facility, all contract employees escorted from room to room, as well as into and out of facility
- There is need for restrictions or requirements to be negotiated into contract agreements when they are activated



# Consultants

- Should be handled like contract employees, with special requirements for information or facility access integrated into contract
- Security and technology consultants must be prescreened, escorted, and subjected to non-disclosure agreements to protect organization.
- Just because security consultant is paid doesn't make the protection of organization's information the consultant's number one priority

# Business Partners

- Businesses find themselves in strategic alliances with other organizations, desiring to exchange information or integrate systems
- There must be meticulous, deliberate process of determining what information is to be exchanged, in what format, and to whom
- Non-disclosure agreements and the level of security of both systems must be examined before any physical integration takes place

# During Employment

- Current employee security objectives:
  - ensure employees, contractors, third party users are aware of info security threats & concerns
  - know their responsibilities and liabilities
  - are equipped to support organizational security policy in their work, and reduce human error risks
- Need for security policy and training
- Security principles:
  - least privilege
  - separation of duties
  - limited reliance on key personnel

# Separation of Duties and Collusion

- Cornerstone in protection of information assets and against financial loss
- Separation of duties: control used to reduce chance of individual violating information security; stipulates that completion of significant task requires at least two people
- Collusion: unscrupulous workers conspiring to commit unauthorized task

# Separation of Duties

- Separation: critical tasks are split into subtasks performed by different people. *“Two people are required to complete a critical task.”*
- Two-man control: two individuals review and approve each other’s work before the task is categorized as finished
- Job rotation: employees know each others’ job skills and tasks rotate

# Privacy and the Security of Personnel Data

- Organizations required by law to protect sensitive or personal employee information
- Includes employee addresses, phone numbers, social security numbers, medical conditions, and family names and addresses
- This responsibility also extends to customers, patients, and business relationships

# Email and Internet Use Policies

- E-mail and Web access for employees is common in offices and some factories
- It is necessary to have e-mail and Internet use policies in organization's security policy
- Due to concerns regarding:
  - work time lost
  - computer / bandwidth resources consumed (?)
  - risk of importing malware
  - possibility of harm, harassment, bad conduct

# Policy Considerations

- Business use only *or* reasonable personal use
- Policy scope (broad: all electronic communications, records thereof)
- Content ownership: electronic communications are company property
- Privacy (**none**)
- Company rights
- Standard of conduct
- Unlawful activity prohibited
- Security policy controls use
- Other company policies also apply
- Disciplinary action



# Positioning and Staffing the Security Function

- The security function can be placed within:
  - IT function
  - Physical security function
  - Administrative services function
  - Insurance and risk management function
  - Legal department
- Organizations balance needs of enforcement with needs for education, training, awareness, and customer service

# Staffing The Information Security Function

- Selecting personnel is based on many criteria, including supply and demand
- Many professionals enter security market by gaining skills, experience, and credentials
- At present, information security industry is in period of high demand

# Qualifications and Requirements

- The following factors must be addressed:
  - Management should learn about position requirements and qualifications
  - Upper management should learn about budgetary needs of information security function
  - IT and management must learn more about level of influence and prestige the information security function should be given to be effective
- Organizations typically look for technically qualified information security generalist

# Qualifications and Requirements

- Organizations look for information security professionals who understand:
  - How an organization operates at all levels
  - Information security is usually a management problem, not a technical problem
  - Strong communications and writing skills
  - The role of policy in guiding security efforts

# Qualifications and Requirements

- Organizations look for information security professionals who understand:
  - Most mainstream IT technologies
  - The terminology of IT and information security
  - Threats facing an organization and how they can become attacks
  - How to protect organization's assets from information security attacks
  - How business solutions can be applied to solve specific information security problems

# Entry into the Information Security Profession

- Many information security professionals enter the field through one of two career paths:
  - Law enforcement and military
  - Technical, working on security applications and processes
- Today, students select and tailor degree programs to prepare for work in information security
- Organizations can foster greater professionalism by matching candidates to clearly defined expectations and position descriptions

# Information Security Positions

- Use of standard job descriptions can increase degree of professionalism and improve the consistency of roles and responsibilities between organizations
- Charles Cresson Wood's book *Information Security Roles and Responsibilities Made Easy* offers set of model job descriptions

# Information Security Positions

- Chief Information Security Officer (CISO or CSO)
  - Top information security position; frequently reports to Chief Information Officer
  - Manages the overall information security program
  - Drafts or approves information security policies
  - Works with the CIO on strategic plans



# Information Security Positions

- Chief Information Security Officer (CISO or CSO)
  - Develops information security budgets
  - Sets priorities for information security projects and technology
  - Makes recruiting, hiring, and firing decisions or recommendations
  - Acts as spokesperson for information security team
  - Typical qualifications: accreditation; graduate degree; experience

# Security Manager

- Accountable for day-to-day operation of information security program
- Accomplish objectives as identified by CISO
- Typical qualifications: not uncommon to have accreditation; ability to draft middle and lower level policies, standards and guidelines; budgeting, project management, and hiring and firing; manage technicians

# Security Technician

- Technically qualified individuals tasked to configure security hardware and software
- Tend to be specialized
- Typical qualifications:
  - Varied; organizations prefer expert, certified, proficient technician
  - Some experience with a particular hardware and software package
  - Actual experience in using a technology usually required

# Credentials of Information Security Professionals

- Many organizations seek recognizable certifications
- Most existing certifications are relatively new and not fully understood by hiring organizations
- Certifications include: CISSP and SSCP; CISA and CISM; GIAC; SCP; TICSA; Security+; Certified Information Forensics Investigator

# Cost of Being Certified

- Better certifications can be very expensive (CISSP exam is \$599.)
- Even experienced professionals find it difficult to take an exam without some preparation
- Many candidates teach themselves through trade press books; others prefer structure of formal training
- Before attempting a certification exam, do all homework and review exam criteria, its purpose, and requirements in order to ensure that the time and energy spent pursuing certification are well spent

# Advice for Information Security Professionals

- Always remember: business before technology
- Technology provides elegant solutions for some problems, but adds to difficulties for others
- Never lose sight of goal: protection
- Be heard, but not an impediment
- Know more than you say; be more skillful on
- Speak to users, not at them
- Your education is never complete



# Questions

