Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Distributed Analytics & Security Institute
Director, Center for Cyber Innovation
Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Outline
(Protecting Security of Assets) 10%

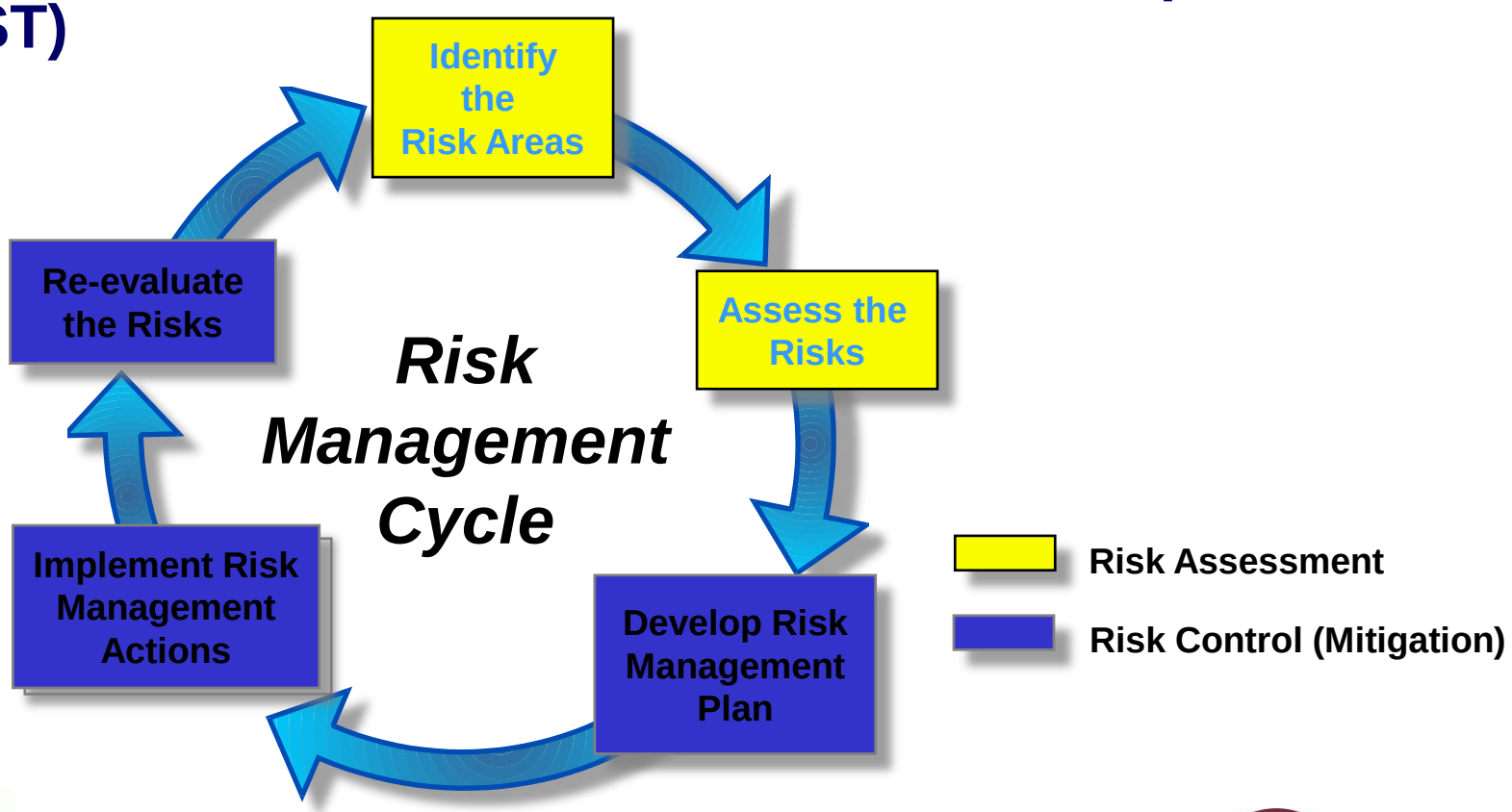
- Information and asset classification
- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)

Information and asset classification

Dr. Drew Hamilton

Risk Management

- **The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected (NIST)**



Risk Identification Process

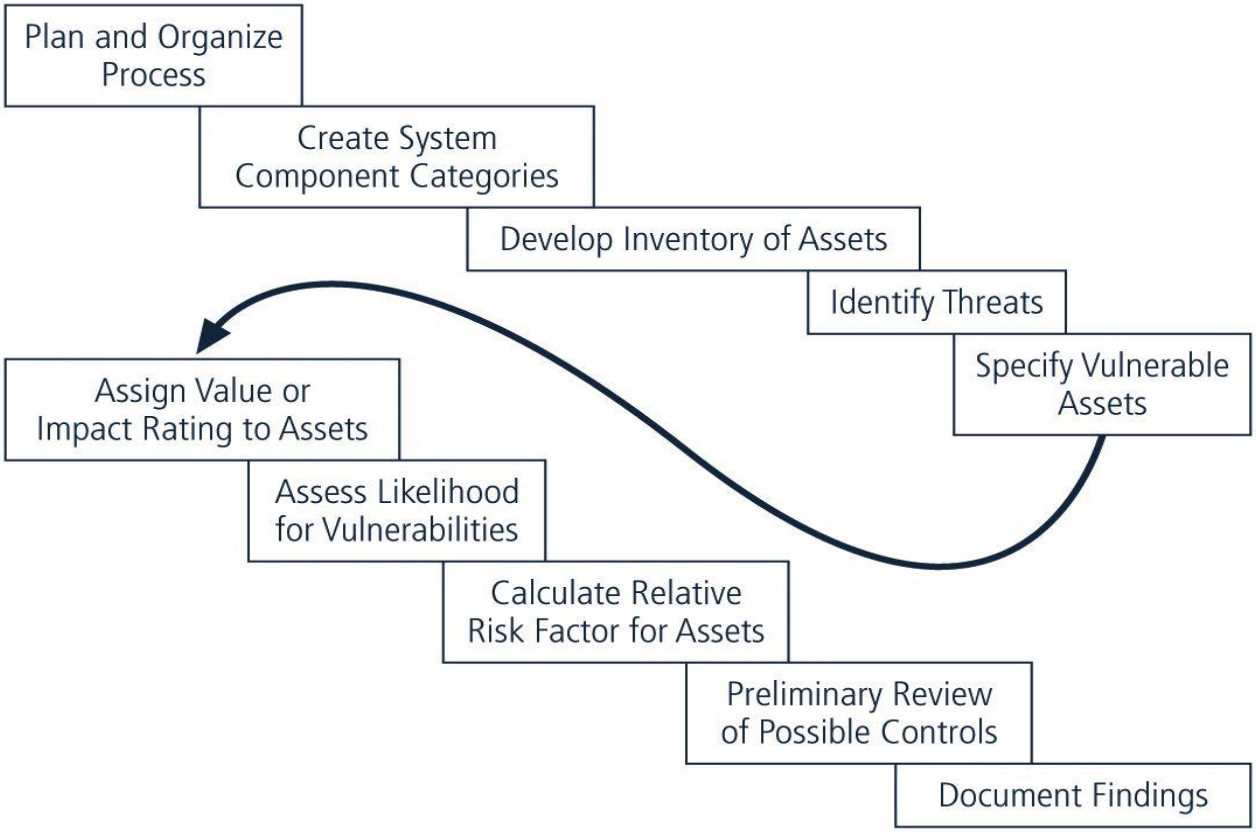


FIGURE 7-1 Risk Identification Process

Risk Identification

- **Risk identification**
  - **begins with the process of self-examination**
- **Managers**
  - **identify the organization's information assets,**
  - **classify them into useful groups, and**
  - **prioritize them by their overall importance**

Inventorying Information Assets

- **Identify information assets, including**
  - **people, procedures, data and information, software, hardware, and networking elements**
- **Should be done without pre-judging value of each asset**
  - **Values will be assigned later in the process**

Organizational Assets

TABLE 7-1 Organizational Assets Used in Systems

IT system components	Risk management components	
People	People inside an organization	Trusted employees Other staff
	People outside an organization	People at organizations we trust Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Data/Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	Hardware	Systems and peripherals Security devices
Networking	Networking components	Intranet components Internet or Extranet components

Attributes for Assets

- **Potential attributes:**
  - Name
  - IP address
  - MAC address
  - Asset type
  - Manufacturer name
  - Manufacturer's model or part number
    - Software version, update revision,
  - Physical location
  - Logical location
  - Controlling entity

Identifying People, Procedures, and Data Assets

- **Whose Responsibility ?**
  - **managers who possess the necessary knowledge, experience, and judgment**
- **Recording**
  - **use reliable data-handling process**

Suggested Attributes

- People
  - Position name/number/ID
  - Supervisor name/number/ID
  - Security clearance level
  - Special skills
- Procedures
  - Description
  - Intended purpose
  - Software/hardware/networking elements to which it is tied
  - Location where it is stored for reference
  - Location where it is stored for update purposes
- Data
  - Classification
  - Owner/creator/manager
  - Size of data structure
  - Data structure used
  - Online or offline
  - Location
  - Backup procedures

Classifying and Categorizing Assets

- Determine whether its asset categories are meaningful
  - After initial inventory is assembled,
- Inventory should also reflect sensitivity and security priority assigned to each asset
- A classification scheme categorizes these information assets based on their sensitivity and security needs

Classifying and Categorizing Assets (Continued)

- **Categories**
  - **designates level of protection needed for a particular information asset**
- **Classification categories must be comprehensive and mutually exclusive**
- **Some asset types, such as personnel,**
  - **may require an alternative classification scheme that would identify the clearance needed to use the asset type**

Assessing Values for Information Assets

- **Assign a relative value**
  - **to ensure that the most valuable information assets are given the highest priority, for example:**
    - **Which is the most critical to the success of the organization?**
    - **Which generates the most revenue?**
    - **Which generates the highest profitability?**
    - **Which is the most expensive to replace?**
    - **Which is the most expensive to protect?**
    - **Whose loss or compromise would be the most embarrassing or cause the greatest liability?**
- **Final step in the RI process is to list the assets in order of importance**
  - **Can use a weighted factor analysis worksheet**

Asset Classification Worksheet

System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 — Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2 — Supplier orders (outbound)	Confidential	High
EDI Document Set 2 — Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-maill (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Weighted Factor Analysis Worksheet (NIST SP 800-30)

TABLE 7-2 Example Weighted Factor Analysis Worksheet

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	30	40	30	
EDI Document Set 1— Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2— Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2— Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Data Classification Model

- **Data owners must classify information assets for which they are responsible and review the classifications periodically**
- **Example:**
  - **Public**
  - **For official use only**
  - **Sensitive**
  - **Classified**

Data Classification Model

- **U.S. military classification scheme**
  - **more complex categorization system than the schemes of most corporations**
- **Uses a five-level classification scheme as defined in Executive Order 12958:**
  - **Unclassified Data**
  - **Sensitive But Unclassified (SBU) Data**
  - **Confidential Data**
  - **Secret Data**
  - **Top Secret Data**

Security Clearances

- **Personnel Security Clearance Structure:**
  - Complement to data classification scheme
  - Each user of information asset is assigned an authorization level that indicates level of information classification he or she can access
- **Most organizations have developed a set of roles and corresponding security clearances**
  - Individuals are assigned into groups that correlate with classifications of the information assets they need for their work
- **Need-to-know principle:**
  - Regardless of one's security clearance, an individual is not allowed to view data simply because it falls within that individual's level of clearance
  - Before he or she is allowed access to a specific set of data, that person must also need-to-know the data as well

Management of Classified Information Assets

- Managing an information asset includes
  - considering the storage, distribution, portability, and destruction of that information asset
- Information asset that has a classification designation other than unclassified or public:
  - Must be clearly marked as such
  - Must be available only to authorized individuals
- Clean Desk policy
  - To maintain confidentiality of classified documents, managers can implement a clean desk policy
- Destruction of sensitive material
  - When copies of classified information are no longer valuable or too many copies exist, care should be taken to destroy them properly to discourage dumpster diving

Threat Identification

- Any organization typically faces a wide variety of threats
- If you assume that every threat can and will attack every information asset, then the project scope becomes too complex
- To make the process less unwieldy, manage separately
  - each step in the threat identification and
  - vulnerability identification processes

  then coordinate them at the end

Identify And Prioritize Threats and Threat Agents

- **Each threat presents a unique challenge to information security**
  - **Must be handled with specific controls that directly address particular threat and threat agent's attack strategy**
- **Threat assessment**
  - **Before threats can be assessed in risk identification process, each threat must be further examined to determine its potential to affect targeted information asset**

Threats to Information Security

TABLE 7-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Source: ©2003 ACM, Inc., Included here by permission.

Threats to Information Security

Weighted Ranks of Threats to Information Security					
	Threat	Mean	Standard Deviation	Weight	Weighted Rank
1.	Deliberate software attacks	3.99	1.03	546	**2178.3**
2.	Technical software failures or errors	3.16	1.13	358	**1129.9**
3.	Acts of human error or failure	3.15	1.11	350	**1101.0**
4.	Deliberate acts of espionage or trespass	3.22	1.37	324	**1043.6**
5.	Deliberate acts of sabotage or vandalism	3.15	1.37	306	**962.6**
6.	Technical hardware failures or errors	3.00	1.18	314	**942.0**
7.	Deliberate acts of theft	3.07	1.30	226	**694.5**
8.	Forces of nature	2.80	1.09	218	**610.9**
9.	Compromises to intellectual property	2.72	1.21	182	**494.8**
10.	Quality–of-service deviations from service providers	2.65	1.06	164	**433.9**
11.	Technological obsolescence	2.71	1.11	158	**427.9**
12.	Deliberate acts of information extortion	2.45	1.42	92	**225.2**

Vulnerability Assessment

- **Steps revisited**
  - **Identify the information assets of the organization and**
  - **Document some threat assessment criteria,**
  - **Begin to review every information asset for each threat**
    - **Leads to creation of list of vulnerabilities that remain potential risks to organization**
- **Vulnerabilities**
  - **specific avenues that threat agents can exploit to attack an information asset**
- **At the end of the risk identification process,**
  - **a list of assets and their vulnerabilities has been developed**

Weighted Ranking of Threat-Driven Expenditures

Top Threat-Driven Expenses	Rating
Deliberate software attacks	12.7
Acts of human error or failure	7.6
Technical software failures or errors	7.0
Technical hardware failures or errors	6.0
QoS deviations from service providers	4.9
Deliberate acts of espionage or trespass	4.7
Deliberate acts of theft	4.1
Deliberate acts of sabotage or vandalism	4.0
Technological obsolescence	3.3
Forces of nature	3.0
Compromises to intellectual property	2.2
Deliberate acts of information extortion	1.0

Risk Identification Estimate Factors

Risk is:

The likelihood of the occurrence of a vulnerability

Multiplied by

The value of the information asset

Minus

The percentage of risk mitigated by current controls

Plus

The uncertainty of current knowledge of the vulnerability

Likelihood

- **Likelihood**
  - **of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event**
  - **is the overall rating - often a numerical value on a defined scale (such as 0.1 – 1.0) - of the probability that a specific vulnerability will be exploited**
- **Using the information documented during the risk identification process,**
  - **assign weighted scores based on the value of each information asset, i.e. 1-100, low-med-high, etc**

Assessing Potential Loss

- **To be effective, the likelihood values must be assigned by asking:**
  - **Which threats present a danger to this organization's assets in the given environment?**
  - **Which threats represent the most danger to the organization's information?**
  - **How much would it cost to recover from a successful attack?**
  - **Which threats would require the greatest expenditure to prevent?**
  - **Which of the aforementioned questions is the most important to the protection of information from threats within this organization?**

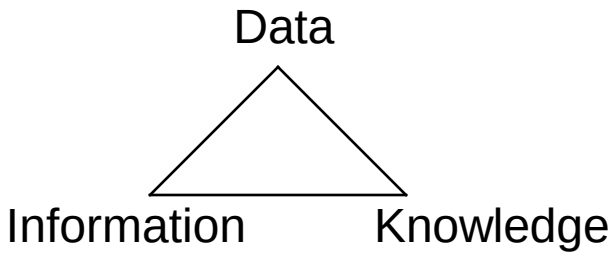
Ownership (e.g. data owners, system owners)

Reference NIST 800-14

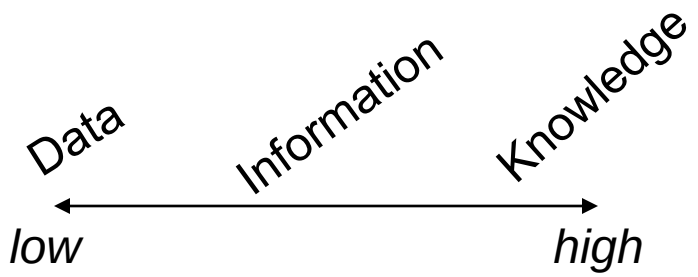
Reference: Bob Travica, U. Manitoba

Reference: TEL2813/IS2820 Security Management

Information Management



Size, Complexity, Management Cost):



Information Management

Data refers to sets of symbols (textual, visual, audio) that may have some generic meaning or no meaning.

(e.g., “bob” vs “cpc”; “client”)

Information refers to data with specific meaning. Usually implies putting data in some context (sentence, other data).

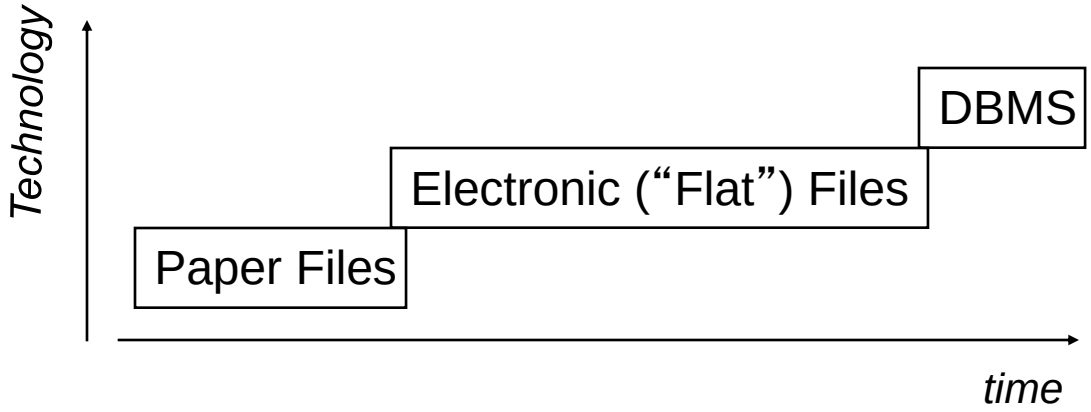
(e.g., “bob is my friend”, “bob not meaning beans in a Slavic language”; “cpc is encrypted ‘bob’ ”; “client device sends requests to the server; database record)

Knowledge refers to interconnected information that signifies what is/will be, why is/will be, and how to do.

Information Management

- Data – raw unprocessed stream of facts.
- Information – data processed and arranged in a meaningful form.
- Knowledge – extracted from information and data to which is added expert opinion, skills and experience.
- We can also define knowledge by type in terms of function
  - Declarative knowledge (knowledge about)
  - Procedural knowledge (know-how)
  - Causal (know why)
  - Conditional (know when)
  - Relational (know with).
- Information management (IM) is the collection and management of information from one or more sources and the distribution of that information to one or more audiences.
- Knowledge Management (KM) is the *capabilities* by which communities within an organization *capture* the knowledge that is critical to them, *constantly improve* it and *make it available* in the most effective manner to those people who need it, so that they can *exploit it creatively* to add value as part of their work.

Data Hierarchy



- **DBMS models**
  - **(hierarchical, network, relational, object)**
- **Challenges of multimedia data**

Mitigated Risk / Uncertainty

- **If it is partially controlled,**
  - **Estimate what percentage of the vulnerability has been controlled**
- **Uncertainty**
  - **is an estimate made by the manager using judgment and experience**
  - **It is not possible to know everything about every vulnerability**
  - **The degree to which a current control can reduce risk is also subject to estimation error**

Risk Determination Example

- **Asset A has a value of 50 and has vulnerability #1,**
  - **likelihood of 1.0 with no current controls**
  - **assumptions and data are 90% accurate**
- **Asset B has a value of 100 and has two vulnerabilities**
  - **Vulnerability #2**
    - **likelihood of 0.5 with a current control that addresses 50% of its risk**
  - **Vulnerability # 3**
    - **likelihood of 0.1 with no current controls**
    - **assumptions and data are 80% accurate**

Risk Determination Example

- **Resulting ranked list of risk ratings for the three vulnerabilities is as follows:**
  - **Asset A: Vulnerability 1 rated as 55 =**
    - **(50 × 1.0) – 0% + 10%**
  - **Asset B: Vulnerability 2 rated as 35 =**
    - **(100 × 0.5) – 50% + 20%**
  - **Asset B: Vulnerability 3 rated as 12 =**
    - **(100 × 0.1) – 0 % + 20%**

Identify Possible Controls

- For each threat and its associated vulnerabilities that have residual risk, create a preliminary list of control ideas
- Three general categories of controls exist:
  - Policies
  - Programs
  - Technical controls

Access Controls

- **Access controls specifically**
  - address admission of a user into a trusted area of the organization
- **These areas can include**
  - information systems,
  - physically restricted areas such as computer rooms, and
  - even the organization in its entirety
- **Access controls usually consist of**
  - a combination of policies, programs, and technologies

Types of Access Controls

- **Mandatory Access Controls (MACs):**
  - **Required**
  - **Structured and coordinated with a data classification scheme**
  - **When implemented, users and data owners have limited control over their access to information resources**
  - **Use data classification scheme that rates each collection of information**
- **Access Control Matrix**
- **Access Control List**
  - **the column of attributes associated with a particular object is called an access control list (ACL)**
- **Capabilities**
  - **The row of attributes associated with a particular subject**

Types of Access Controls (Continued)

- **Nondiscretionary controls are determined by a central authority in the organization**
  - **Can be based on roles—called role-based controls—or on a specified set of tasks—called task-based controls**
  - **Task-based controls can, in turn, be based on lists maintained on subjects or objects**
  - **Role-based controls are tied to the role that a particular user performs in an organization, whereas task-based controls are tied to a particular assignment or responsibility**

Types of Access Controls (Continued)

- Discretionary Access Controls (DACs) are
  - implemented at the discretion or option of the data user
- The ability to share resources in a peer-to-peer configuration allows
  - users to control and possibly provide access to information or resources at their disposal
- The users can allow
  - general, unrestricted access, or
  - specific individuals or sets of individuals to access these resources

Documenting the Results of Risk Assessment

- The goal of the risk management process:
  - Identify information assets and their vulnerabilities
  - Rank them according to the need for protection
- In preparing this list, collect
  - wealth of factual information about the assets and the threats they face
  - information about the controls that are already in place
- The final summarized document is the ranked vulnerability risk worksheet

Ranked Vulnerability Risk Worksheet

TABLE 7-5 Ranked Vulnerability Risk Worksheet

Asset	Asset Impact	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer service request via e-mail (inbound)	55	E-mail disruption due to software failure	0.2	11
Customer order via Secure Sockets Layer (SSL) (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to power failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1
Customer order via SSL (inbound)	100	Lost orders due to Web server buffer overrun attack	0.01	1

Documenting the Results of Risk Assessment (Continued)

- What are the deliverables from this stage of the risk management project?
- The risk identification process should designate
  - what function the reports serve,
  - who is responsible for preparing them, and
  - who reviews them

Risk Identification and Assessment Deliverables

TABLE 7-6 Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns a ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns a risk-rating ranked value to each uncontrolled asset–vulnerability pair

Protect privacy

Reference: Corby Anderson

Why Is Privacy Important?

- Data is a corporate asset, like any other
- Corporate data is at a higher risk of theft or misuse than ever before
- Companies have obligations to protect data
  - Laws, regulations, guidelines
  - Contracts with third parties
  - Privacy policies for users of websites, other online features

CMU Privacy Statistics

- A matter of corporate governance:
  - Does your board review and approve top-level policies on privacy and IT security risks?
    - 23% - regularly
    - 28% - occasionally
    - 42% - rarely or never
  - Does your board review and approve annual budgets for privacy and IT security programs?
    - 28% - regularly
    - 10% - occasionally
    - 54% - rarely or never

Carnegie Mellon CyLab 2012 Report

Information Privacy, Security

- **Data privacy, data security risks are not limited to financial, healthcare, utility sectors. Retail sector is vulnerable as well**
  - **Zaxby's reported finding malware at 100 of its 560 locations in 10 states that could extract names, credit and debit card numbers**
  - **Papa John's agreed to pay $16.5 million to settle a class action over claims that it sent unauthorized texts to customers in violation of the Telephone Consumer Protection Act**
- **Breaches of data privacy, data security can result in**
  - **Damage to reputation**
  - **Disruption of operations**
  - **Legal liability under new and amended laws, regulations, and guidelines, as well as under contracts**
  - **Financial costs**

Types of Information

- "Personally identifiable information" (PII) can be linked to a specific individual
  - Name, e-mail, full postal address, birth date, Social Security number, driver's license number, account numbers
- "Non-personally identifiable information" (non-PII) cannot, by itself, be used to identify a specific individual
  - Aggregate data, zip code, area code, city, state, gender, age

PII or not PII?

- "Anomyzed" data that is "de-anomyzed"
  - IP address linked to domain name that identifies a person

- Non-PII that, when linked with other data, can effectively identify a person – "persistent identifiers"
  - Geolocation data
  - Site history and viewing patterns

PII Protections

- Data privacy laws govern businesses' collection, use, and sharing of information about individuals
- Federal, state, and foreign laws apply
- Laws govern both physical and electronic security of information

Legal Protections for PII

- U.S. laws are a patchwork, developed by sector (compared to European Community's uniform, centralized law)
  - Challenges in determining
    - Which laws apply to which activities
    - How to comply when multiple, sometimes inconsistent, laws apply.

Federal Trade Commission

- Prohibits "unfair or deceptive practices in or affecting commerce." No need to prove intent.
  - A practice is "unfair" if:
    - It causes or is likely to cause substantial injury to consumers
    - It cannot reasonably be avoided by consumers
    - It is not outweighed by countervailing benefits to consumers or to competition
  - A representation, omission, or practice is "deceptive" if:
    - It misleads, or is likely to mislead, consumers
    - Consumers' interpretation of it is reasonable under circumstances
    - It is material

Federal Trade Commission

- Practices attacked by FTC as "deceptive":
  - Violating published privacy policies
  - Downloading spyware, adware onto unsuspecting users' computers
  - Failing to verify identity of persons to whom confidential consumer information was disclosed
- Practices attacked by FTC as "unfair":
  - Failing to implement reasonable safeguards to protect privacy of consumer information

Securities and Exchange Commission

- Public companies must report “material” events to shareholders
  - Events are reasonable
  - or would consider important to an investment decision
- Guidance clarifies
  - “Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky.”
    - Disclosure of risk factors should be tailored, not generic.
  - “We expect registrants to evaluate their cyber security risks.”

Children's Online Privacy Protection Act

- Applies to operators of commercial websites and online services that collect information from children under age 13
  - "No one knows you're a dog on the internet."
- Requires reasonable efforts to get verifiable consent of parent or guardian or to notify parent or guardian
- Requires notice of
  - What information is collected from children
  - How information is used
  - How information is shared

Children's Online Privacy Protection Act

- Prohibits conditioning child's participation in an activity on disclosure of more PI than is necessary
- Amendments effective July 1, 2013
  - Include geo-location information, photos, and videos in types of PI that cannot be collected without parental notice and consent
  - Provide streamlined approval process for new ways to get parental consent
  - Require website operators to take reasonable steps to release children's PI only to companies capable of keeping it secure

CAN-SPAM Act

- Controlling the Assault of Non-Solicited Pornography and Marketing
- Prohibits fraudulent, abusive, deceptive commercial email
- "One-bite" rule:
  - Business may send unsolicited commercial email message, properly labeled, to consumer, with easy means for consumer to opt out.
  - If the consumer opts out, business may no longer send emails

CAN-SPAM Act

- Commercial email broadly defined as having primary purpose to advertise or promote commercial product or service
- Does not apply to transactional emails, which facilitate or give update on agreed-upon transaction
- Business must monitor third party handling email marketing to ensure compliance
- Pre-empts state statutes, but states may enforce sections of Act addressing fraudulent or deceptive acts, computer crimes, other advertising restrictions

Telephone Consumer Protection Act

- Established national "Do Not Call" registry
- Regulates use of "automated telephone equipment" such as auto-dialers, artificial or pre-recorded voice messages, fax machines
- Prohibits transmission of a "call" using an "automatic telephone dialing system" without prior consent of called party
- Per FCC, "call" covers both voice calls and text messages (even texts for which called party is not charged)
- Enforcement by federal or state authorities
- Individuals may bring civil actions
  - Papa John's class action over text messages claimed violations of TCPA, Washington Consumer Protection Act
- Relief can include injunction, actual damages, statutory damages of $500 per violation, treble damages

Other Key Federal Statutes

- **Financial**
  - Gramm-Leach-Bliley Act
  - Fair Credit Reporting Act
  - Fair and Accurate Credit Transactions Act
- **Health**
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic & Clinical Health Act (HITECH)

DoD and States

- DoD contracts require notification of security breaches
- Nearly all states, require notification of data security breach
- Many states also have sector-specific statutes
- Statutes apply to businesses that own or maintain PII of a state's residents
  - When PII of another state's residents is involved, must consider that state's notification requirements

Class action suits over privacy

- Raft of litigation since 2010
  - Redressing data breaches
  - Asserting rights under federal, state consumer privacy statutes
- Brought against companies that advertise online or by email or text messaging
  - Example: Papa John's recent $16.5 million settlement over unauthorized texts
- Brought against companies that have data security breaches
- Litigation often follows investigations, enforcement actions by FTC, state Attorneys General

Website Privacy

- Do you need one?
  - No, if your website:
    - Is merely static
    - Is business-to-business (B2B) only, and collects no PII from consumers
  - Yes, otherwise
- What must it cover?
  - Actual practices for PII and information that reasonably could be associated with a person or device, regarding
    - Collection
    - Storage
    - Use
    - Sharing

Website Privacy Policies

- Special concerns if information involves
  - Financial information
  - Medical information
  - Children's information
- Special concerns for specific jurisdictions
  - European Union
  - California
- Opt outs from information collection available?
- Caution regarding links to third party sites
- Notice whenever privacy practices change
- Do not overpromise: "We will never share your information . . ."

Best Practices: Privacy Audit

- Review, assess policies and practices for data
  - Collection
  - Storage
  - Use
  - Disclosure
  - Protection
  - Destruction
- Identify exposure to data privacy, data security risks
- Consider, implement changes to minimize risks
- Develop, adopt best practices going forward

Best Practices: Privacy Audit

- **Key benefit: Shows that data privacy and security are not just IT issues; instead, they touch on all parts of the company**
  - **Audit gathers information not only from IT/IS personnel, but also from personnel with responsibility for legal, marketing, development, sales, supply chain, human resources, international**
- **Helps ensure visibility, responsibility, accountability for privacy, security issues**

Best Practices: Privacy Audit

- Review contracts with vendors that collect or provide PI to company
  - Do contracts have indemnification provisions? Does vendor have resources to indemnify?
- Review potential insurance coverage
  - Property, liability (E&O, D&O, general liability, umbrella), computer crime, business owner package
    - Errors and Omissions
    - Directors and Officers

Best Practices: Privacy Audit

- Consider class action waivers, arbitration provisions in terms of use, other consumer contracts
- Conduct annual reviews of
  - Data security
  - Data privacy
  - Risk management programs
- Develop contingency plans

Best Practices

- Take stock
  - What information do you have?
  - Where is it stored?
  - Who has access to it?
  - Who should have access to it?
- Scale down
  - Collect only what you need
  - Keep it only as long as you need it
  - Don't use Social Security numbers unnecessarily
  - Restrict access
- Keep it safe
  - Train employees about safe practices
  - Implement
    - Firewalls
    - Strong passwords
    - Antivirus software
  - Use extra caution with laptops, PDAs, cell phones
  - Lock desks, drawers
  - Limit access to sensitive files
  - Secure data shipped or stored offsite

Best Practices (2)

- Destroy what you can
  - Shred, burn, pulverize paper records
  - Use wipe utility programs on computers, portable storage devices
  - Make shredders easily accessible
- Plan ahead
  - Develop contingency plans for a security breach
  - Designate senior staff to coordinate response
  - Investigate right away
  - Take steps to eliminate vulnerabilities
  - Be aware of data breach statutes

Handling a Breach

- Do not panic or overreact
- Get facts: nature, scope of breach
- Determine whether, when to notify affected individuals
- Prevent further unauthorized access
- Preserve evidence, deal with law enforcement
- Notify vendors (such as payment processors)
- Notify insurers
- Offer contact person
- Do not forget to alert those “on the front lines”

Appropriate Retention

Reference Angela M. Verzosa

Retention Scheduling

- determining the length of time that the records should remain in the originating office
- usually influenced by such factors as their administrative values to the creator
- as a general rule, records are to remain in the originating office as long as they are active
- records that are inactive should remain in a storage facility; while records with no archival value should be disposed of
- records with archival values should be transferred to the archives

Suggested Retention Periods

- Keep permanently and preserve.
- Keep permanently (transfer to Archives at intervals of 5 years)
- Keep for 10 years, then destroy.
- Keep for 5 years, then destroy.
- Keep for two years, then destroy.
- Review at intervals, keeping only those with continuing value.

Keep Permanently and Preserve

- annual reports
- minutes of meetings
- papers relating to policies & decisions, development plans, budget approvals, etc.)
- property/investment records
- contracts/agreements
- personnel records (201 files)

Keep Permanently and Transfer to Archives

- accreditation records
- employment contracts
- ledgers (summaries of receipts and disbursements)
- audit reports
- building maintenance and operations files (including plans, blueprints, cost records)
- Students' transcripts of records (inactive) reports / plans (including working papers)
- projects (proposals, progress reports, etc)
- government permits
- court records/decisions
- photo/clippings files
- publications

Keep for ten years then destroy

- budget records and ledgers (including vouchers, requisitions, cancelled checks, payroll records, etc.)
- building maintenance inventories
- purchase orders, requisitions, invoices for major items
- accounts (audited after 5 years)

Keep for five years then destroy

- purchase orders, requisitions, etc.
- payroll transactions
- credit investigation reports
- job evaluation reports
- school calendars
- price lists/maps/brochures/flyers

Keep for two years then destroy

- acknowledgements
- application records
- attendance / job performance reports
- duplicate/multiple copies of minutes, reports, plans, printed material (catalogs, brochures), etc.
- survey questionnaires
- unused forms

Subject to Regular Review/Appraisal

- correspondence and other papers (review every five years, keeping/ transferring to Archives those with continuing value)
- accreditation records/government permits
- projects/program proposals
- student files (correspondence, etc.)
- student accounts

Records for Disposal

- drafts
- routine transmittals
- acknowledgments
- specific financial transactions
- requests/replies to questionnaires
- blank/unused forms
- multiple copies

Inactive Records Management

- A Records Center ensures the protection, access and retrieval of institutional records until their retention value has been met. It includes accession and inventory control, security and access provisions, and environmental controls.
- The records manager should work with the data manager and information technology staff to ensure the retention of electronic data, and that data remain accessible and retrievable throughout their life cycle.

Records Disposition

- ensures the destruction of records according to approved retention policies
- requires appropriate handling of confidential materials
- requires the transfer of records designated for permanent preservation to the institution's archives
  - inventorying
  - appraising
  - scheduling
- Retiring
  - disposal policies
  - transfer guidelines
  - archival procedures

Implementing Retention Policies

- Make them available to those in the working offices; i.e., office administrative staffs.
- Publicize them using the most accessible communication vehicle; e.g., administrative manuals, Web pages or other online communication technologies.
- Share retention and disposition policies with information technology staffs and with those responsible for the institution's information resource planning.
- Implementation should include provision for periodic audits and reviews to insure that the retention policies are up to date and that campus offices are implementing them appropriately.

What is Media Sanitization?
(NIST SP 800-88)

Dispose: (not really sanitized) Just tossed away.

Clear: Resistant to keyboard attacks.

Purge: Resistant to laboratory attacks.

Destroy: Resistant to recreation of media

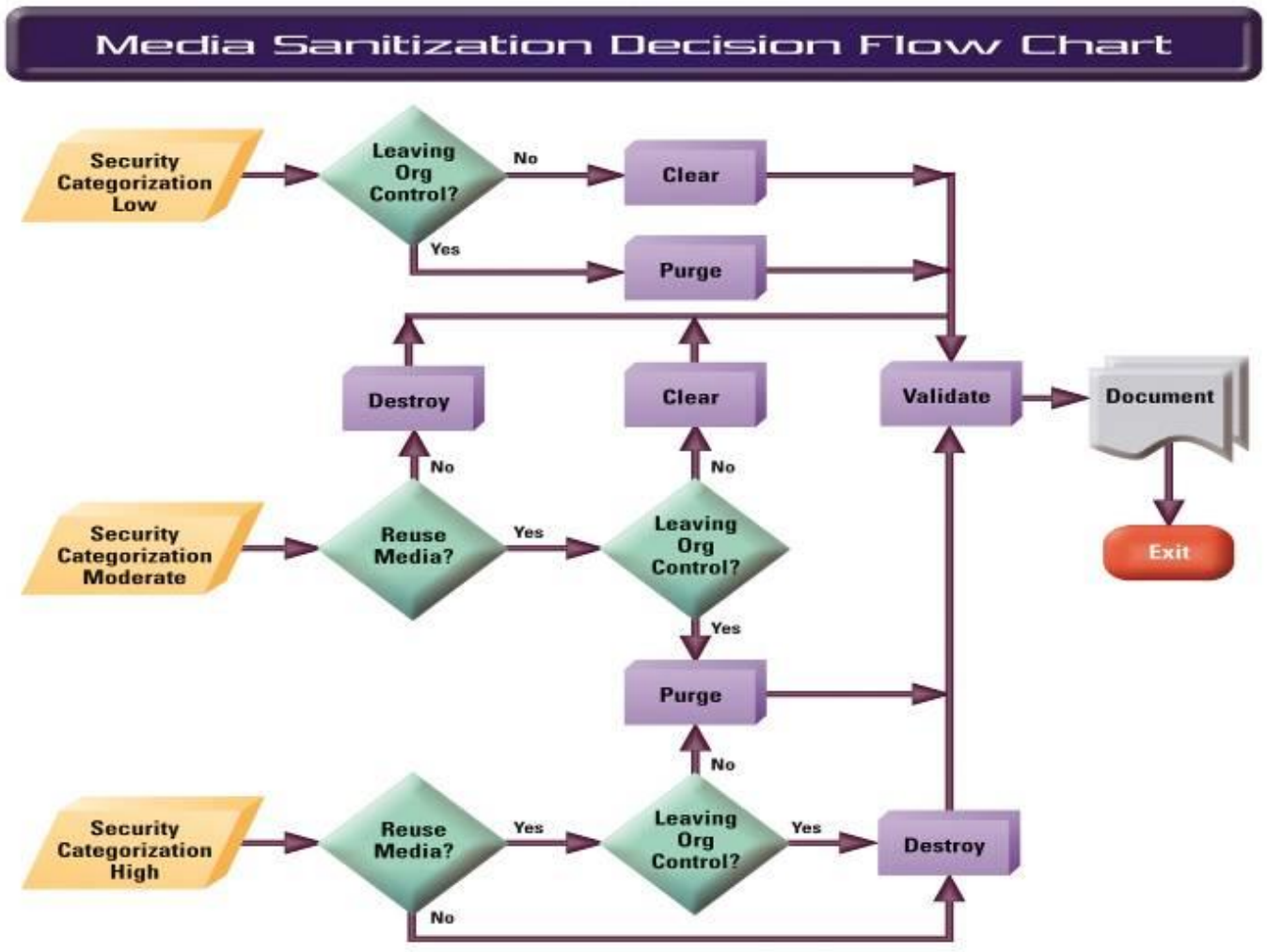
NIST SP800-88 is not intended to replace a sanitization program that is:

- Effective
- Operational
- Compliant with FIPS 200 and satisfies SP 800-53 Rev 1 and 800-53A.

Media Sanitation (NIST SP 800-88)

- How to sanitize media?
  - Identify your media and know your information.
  - Decide on a sanitization method.
  - Find supportive tools.
  - Validate your tools/policies/procedures.
- What is reasonable?
  - Don't degauss the paper or spend $5K to sanitize a $50 HD.
  - Scale it up for ease, risk, resources.
  - Make cost effective risk based decisions weighing environmental factors that may be unique to your agency.
- Know what information is where.
  - What media are you using across your agency.
    - Is there non agency media on your systems?
  - What information is on that media.
  - What information is not on media.
  - Loose control of your information locations = loose control of your sanitization.

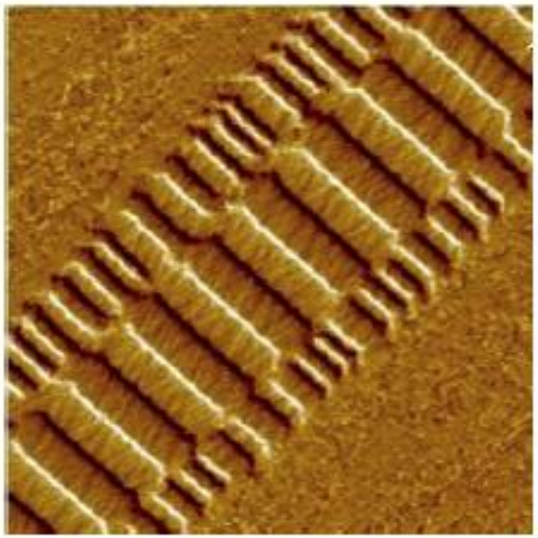
Media Sanitation



Remanence

- **Data Remanence Threats and Vulnerabilities:**
  - **Confidentiality may be compromised if data is not encrypted or sanitized properly**
    - **Must overwrite data multiple times**
    - **Must encrypt data for protection of data at rest**
  - **Access Control does not exist on discarded media**
    - **Unencrypted data on discarded media is vulnerable to snooping and compromise**
  - **Classified information is at risk when media is not properly sanitized**

Magnetic Remanance



Residuals of overwritten information on the side of magnetic disk tracks. Reproduced with permission of VEECO

Data security controls

Dr. Devin Cook

Shon Harris

Security Management

- **Objective of a Security Program:**
  - **Protect the company and its assets**
  - **Protect the recognized assets from their identified threats**
- **This is hard because security management has changed over the years.**
- **Management must first determine security goals by evaluating business objectives, security risks, user productivity, and functionality requirements and objectives.**
- **This means it must be addressed from the highest levels of management. It's their job to get the ball rolling and to monitor the security program's accomplishments.**

Security Administration and Supporting Controls

- Fundamental Principles of Security
- Security Definitions
- Security Through Obscurity

Security Administration and Supporting Controls

Information owners should dictate which users can access their resources and what those users can do with those resources.

The security administration's job is to make sure these objectives are implemented through:

- **Administrative controls**
- **Technical controls (logical controls)**
- **Physical controls**

Definition: *due care* - legal term; if someone is practicing due care, they are acting responsibly and will have a lower probability of being found negligent and liable if something bad happens

Security Administration and Supporting Controls

Common reasons for inadequate management:

- **management does not understand the necessity of security**
- **security is in competition with other management goal**
- **management views security as expensive and unnecessary**
- **management applies lip service instead of real support to security**

Security Administration and Supporting Controls

Fundamentals: the *CIA triad*

Confidentiality

- **Compromised by network monitoring, shoulder surfing, stealing passwords, and social engineering**
- **Use encryption, strict access control, data classification, and training personnel**

Integrity (accuracy and reliability of information and systems)

- **Unauthorized modification is prevented**
- **Strict access controls, intrusion detection, and hashing**
- **Input validation**
- **Encryption of data in transit**

Availability

- **Single points of failure should be avoided**
- **Backup measures and redundancy**
- **Environmental components**

Security Administration and Supporting Controls

- **Security Definitions**

- ***Vulnerability*** **- software, hardware, or procedural weakness that can be exploited**

- ***Threat*** **- any potential danger to information systems. The threat is that someone (*threat agent)* will identify a specific vulnerability and actually exploit it.**

- ***Risk*** **- likelihood of a threat agent exploiting a vulnerability and the corresponding business impact**

Security Administration and Supporting Controls

- **Security Definitions (cont'd)**
- ***Exposure*** **- an instance of being exposed to losses from a threat agent**
- ***Countermeasure/Safeguard*** **- software config, hardware device, or a procedure that mitigates certain risks**
- **Can we give examples of each of these?**

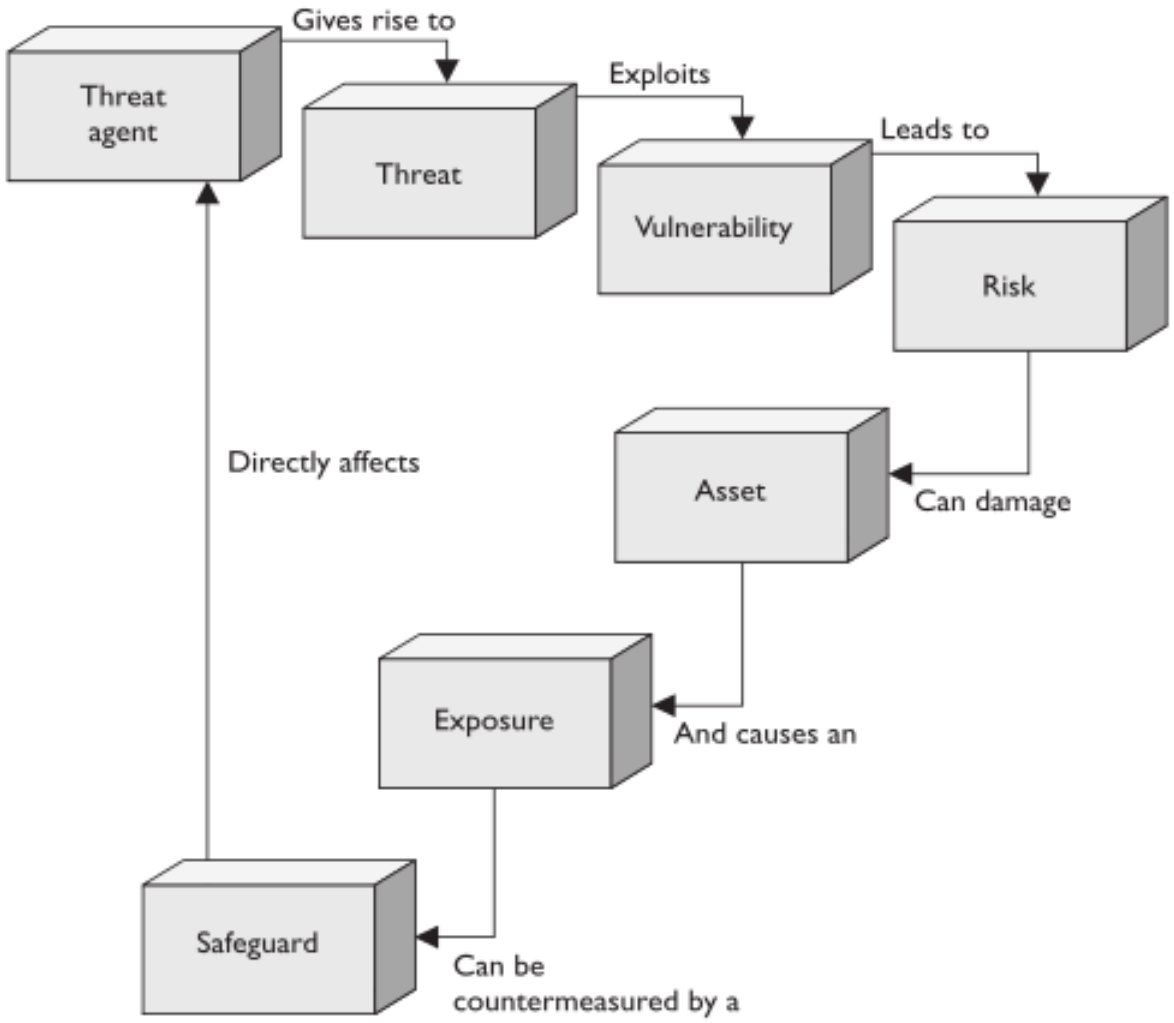


Figure 3-3 The relationships among the different security components

Evaluate in order:
threat, exposure, vulnerability, countermeasures, and risk

Security Administration and Supporting Controls

Security Through Obscurity

Obviously not a valid method of securing an organization:

- **flaws can't be exploited if they're not common knowlege**
- **compiled code is more secure than open-source code**
- **moving HTTP traffic to port 8088 will provide protection**
- **developing personal encryption algorithms will stop the crackers**
- **if we all wear Elvis costumes, no one can pick us out to conduct social engineering attacks**

Granted, although these don't decrease your attack surface, they may decrease attack volume. Don't be fooled into a false sense of security, though. You still need standard defense-in-depth security practices.

Organizational Security Model

Security planning can be broken down into three areas:

- **strategic - long term goals**
- **tactical - medium term goals**
- **operational - short term goals**

A security program is more than just having a security policy and annual network assessment.

There are existing security frameworks that can be utilized:

- **ISACA's COBIT defines goals for controls for managing IT and insuring it maps to business needs. Four domains:**
  - **Plan and Organize**
  - **Acquire and Implement**
  - **Deliver and Support**
  - **Monitor and Evaluate**

Organizational Security Model

Security Frameworks (cont'd):

- **ISO 17799 - made up of 10 domains, that are similar to those in the CISSP Common Body of Knowledge**
- **IT Infrastructure Library (ITIL)**

CobiT really provides "what is to be achieved," and ISO 17799 and ITIL tell you "how to achieve it."

You'll likely see ISO 17799 and ISO 27001 on the exam.

Definition:
***Security Governance* - basically the same as corporate/IT governance, but as it applies to security**

Organizational Security Model

Security Program Development

You really need to follow a life cycle approach:

1. **Plan and Organize**
2. **Implement**
3. **Operate and Maintain**
4. **Monitor and Evaluate**

For each specific business need outlined, you should create security blueprints that will lay out security solutions, processes, and components that will be used to match security and business needs. These blueprints will be covered later in another chapter.

Information Risk Management (IRM)

- **Who Really Understands Risk Management?**
- **Information Risk Management Policy**
- **The Risk Management Team**

Information Risk Management (IRM)

IRM is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level.

You must be aware of the several types of risk and address them all:

- **Physical damage**
- **Human interaction**
- **Equipment malfunction**
- **Inside and outside attacks**
- **Misuse of data**
- **Loss of data**
- **Application error**

Real risk is hard to measure, but prioritizing the potential risks is possible.

Information Risk Management (IRM)

Applications, devices, protocols, viruses, and hacking should be considered small pieces of the overall security puzzle.

Businesses operate to make money, not to just be secure. While understanding individual threats is important, it is more important to be able to calculate the risk of these threats and map them to business drivers.

IRM policy should provide direction on how the IRM team relates information on risks to senior management and how to execute management's decisions on risk mitigation tasks.

Risk Analysis

- The Risk Analysis Team
- The Value of Information and Assets
- Costs That Make Up the Value
- Identifying Threats
- Failure and Fault Analysis
- Quantitative Risk Analysis
- Qualitative Risk Analysis
- Quantitative vs. Qualitative
- Protection Mechanisms
- Putting It Together
- Total Risk vs. Residual Risk
- Handling Risk

Risk Analysis

Four main goals:

1. **Identify assets and their values**
2. **Identify vulnerabilities and threats**
3. **Quantify the probability and business impact of these potential threats**
4. **Provide an economic balance between the impact of the threat and the cost of the countermeasure**

Risk analysis provides a cost/benefit comparison. If management determines early on in the risk analysis process that certain assets are not important, the risk assessment team should not spend additional time or resources evaluating those assets.

Risk Analysis

Questions to ask when performing a risk assessment:

- **What event could occur (threat event)?**
- **What could be the potential impact (risk)?**
- **How often could it happen (frequency)?**
- **What level of confidence do we have in the answers to the first three questions (certainty)?**

The value of an asset should reflect all identifiable costs that would arise if there were an actual impairment of the asset, not just the replacement cost.

Definitions:

***Loss potential* - what the company would lose if a threat agent were to exploit a vulnerability**

***Delayed loss* - any loss that occurs after the initial exposure**

Risk Analysis

Failure and Fault Analysis

You want to pinpoint where a vulnerability exists, as well as determine exactly what kind of scope the vulnerability entails. What could be the secondary ramifications of its exploitation?

Failure Mode and Effect Analysis (FMEA):

1. **Start with a block diagram of a system or control**
2. **Consider what happens if each block of the diagram fails**
3. **Draw up a table in which failures are paired with their effects and an evaluation of the effects**
4. **Correct the design of the system and adjust the table until the system is not known to have unacceptable problems**
5. **Have several engineers review the failure modes and effects analysis**

Risk Analysis

FMEA was first developed for systems engineering. It proved to be successful and has been more recently adapted for use in evaluating risk management priorities.

For working with more complex systems, you may want to do fault tree analysis:

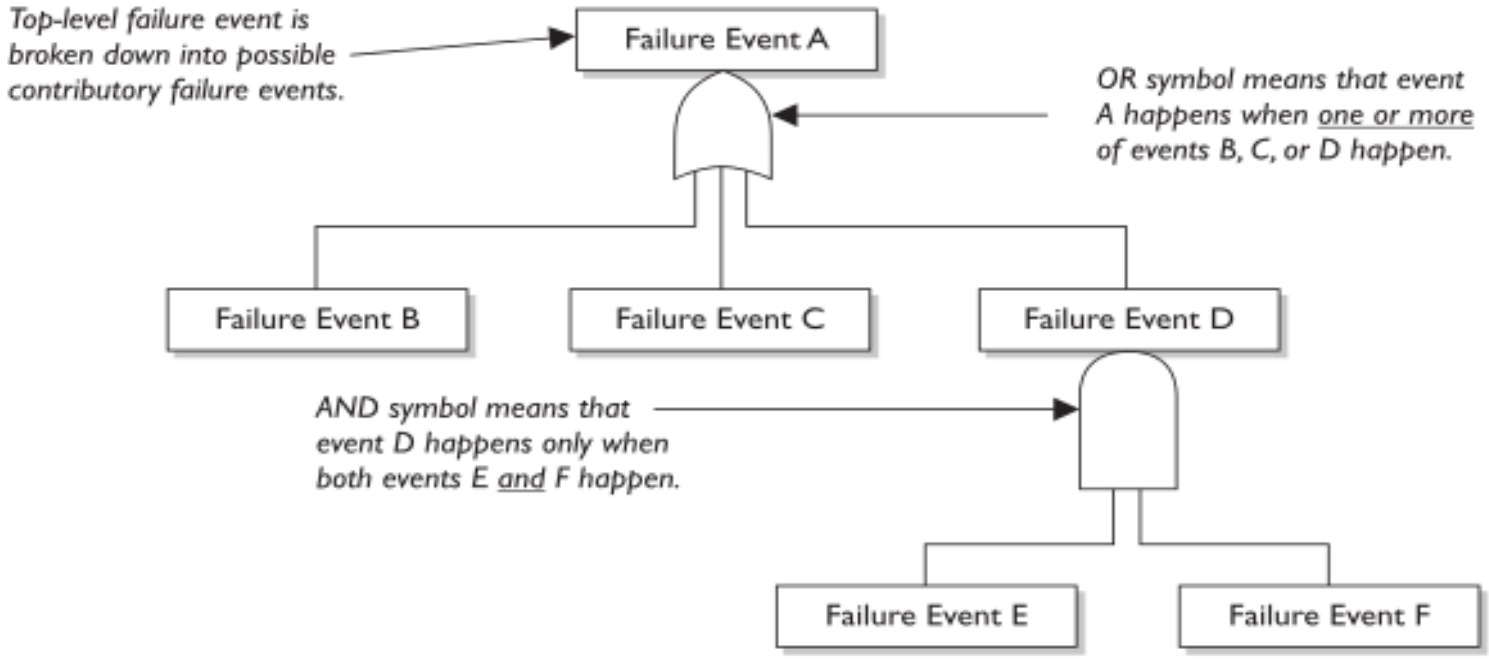


Figure 3-7 Fault tree and logic components

Risk Analysis

Quantitative Risk Analysis

This attempts to assign real and meaningful numbers to all elements of the risk analysis process.

Purely quantitative risk analysis is not possible because the method attempts to quantify qualitative items.

Most automated systems store base data in a database and then can run scenarios with that data with different parameters to give a view of the outcomes for different exposures.

Risk Analysis

Steps of a Quantitative Risk Analysis

1. Assign Value to Assets
2. Estimate Potential Loss per Threat
3. Perform a Threat Analysis
4. Derive the Overall Annual Loss Potential per Threat
5. Reduce, Transfer, Avoid, or Accept the Risk

Definitions:

***exposure factor (EF)*: percentage loss of an asset**

***single loss expectancy (SLE)* = asset value * EF**

***annualized rate of occurrence (ARO)*: frequency of exposure**

***annualized loss expectancy (ALE)* = SLE * ARO**

Risk Analysis

Results of a Risk Analysis

- Monetary values assigned to assets
- Comprehensive list of all possible and significant threats
- Probability of the occurrence rate of each threat
- Loss potential the company can endure per threat in a 12-month time span
- Recommended safeguards, countermeasures, and actions

Risk Analysis

Qualitative Risk Analysis

Techniques include judgement, best practices, intuition, and experience

1. **A risk analysis team is built consisting of members from across many departments with experience and education on the threats being evaluated**
2. **A scenario is written for each major threat**
3. **Safeguards that diminish the damage of the threat are evaluated and the scenario is played out for each**

Risk Analysis

Qualitative Risk Analysis

Benefits

- communication must happen among team members
- risks and safeguards are ranked
- strengths and weaknesses are identified
- those who know the subjects best provide their opinions to management

Risk Analysis

Countermeasure Selection

Again, you need to do a cost/benefit analysis.

Example:
If the ALE of a threat is $12,000 before applying the safeguard, and $3,000 after applying it, and the annual cost of the safeguard is $650, then the value of the safeguard is $8,350/year.

Remember that the cost of a countermeasure is more that just the purchase price. Also, note that you will likely never reduce the ALE to $0. This is due to residual risk.

Risk Analysis

Total Risk vs. Residual Risk

No system or environment is 100% secure, which means there is always some risk left over to deal with.

Total risk is the risk a company faces if it chooses not to implement a certain safeguard. Residual risk is the risk left over after implementing that safeguard.

threats * vulnerability * asset value = *total risk*
total risk * controls gap = *residual risk*

Risk Analysis

Handling Risk

Risk can be dealt with by:

- **transferring it - through insurance or delegating**
- **rejecting it - also called risk avoidance, you do this by terminating the activity that is introducing the risk**
- **reducing it - also called risk mitigation**
- **accepting it**

Risk acceptance:

- **Is the potential loss lower than the countermeasure?**
- **Can the organization deal with the "pain" that will come with accepting the risk?**

This "pain" can be more than just financial

Risk Analysis

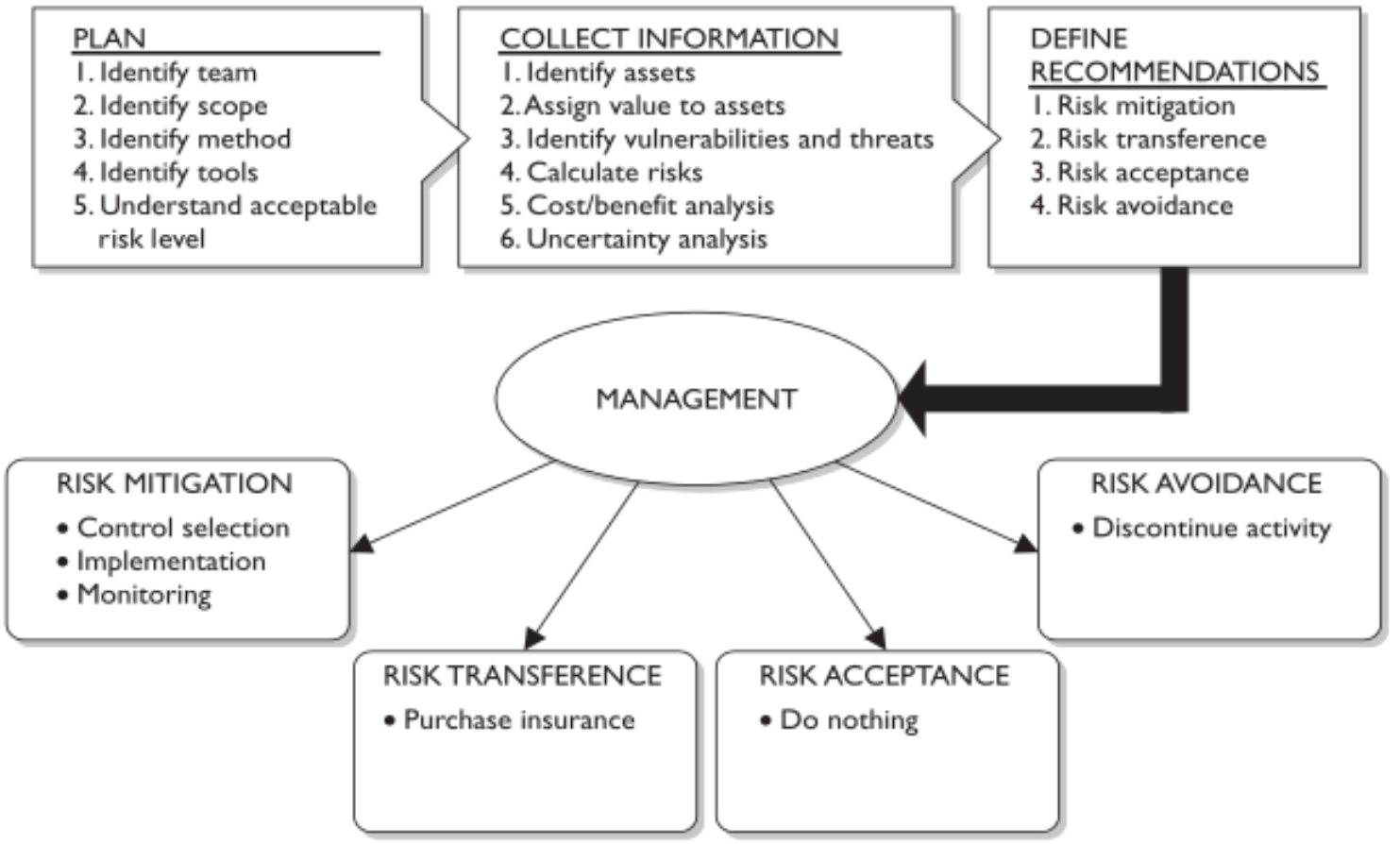


Figure 3-10 How a risk management program can be set up

Policies, Standards. Baselines, Guideline and Procedures

- Security Policy
- Standards
- Baselines
- Guidelines
- Procedures
- Implementation

Policies, Standards. Baselines, Guideline and Procedures

Why have policies in place?

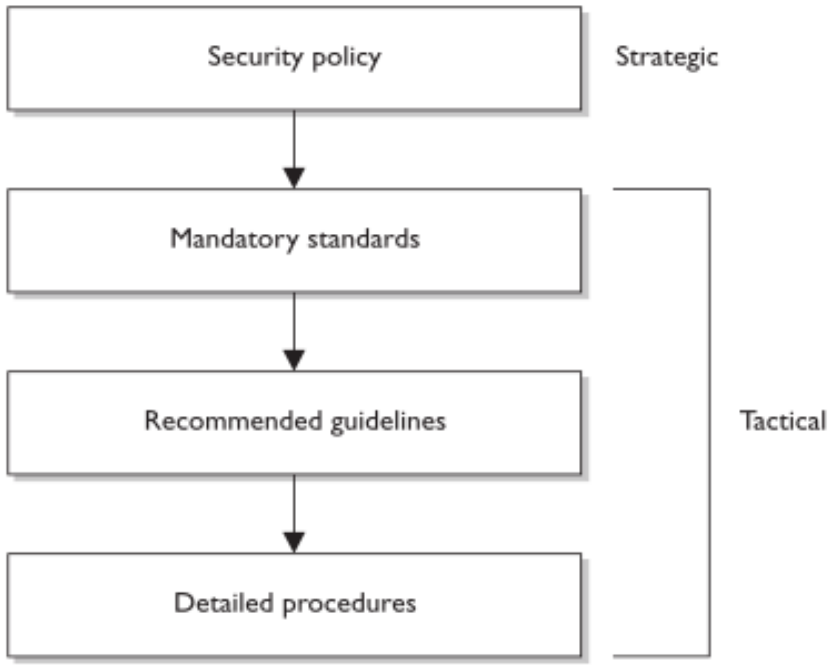
- **Identifies assets the company considers valuable**
- **Provides authority to the security team and its activities**
- **Provides a reference to review when conflicts pertaining to security arise**
- **States the company's goal and objectives pertaining to security**
- **Outlines personal responsibility**
- **Helps to prevent unaccounted-for events (surprises)**
- **Defines the scope for the security team and its functions**
- **Outlines incident response responsibilities**
- **Outlines the company's response to legal, regulatory, and standards of due care**

Remember, a policy should be technology- and solution-independent.

Policies, Standards. Baselines, Guideline and Procedures

Standards refer to mandatory activities, actions, or rules. They may be internal, or externally mandated.

Figure 3-11
Policy establishes the strategic plans, and the lower elements provide the tactical support.



The term *baseline* can have several definitions. It can refer to a point in time used as comparison for future changes, or it can be used to define the minimum level of protection required.

Policies, Standards. Baselines, Guideline and Procedures

Guidelines are recommended actions and operational guides to users, IT staff, operations staff, and others when a specific standard does not apply.

Procedures are detailed step-by-step tasks that should be performed to achieve a certain goal. They spell out how the policy, standards, and guidelines will actually be implemented in an operating environment.

Standards, guidelines, and baselines should be kept modular and in separate documents as they each have a specific purpose and a different audience.

Information Classification

- **Private Business vs. Military Classifications**
- **Classification Controls**

Information Classification

Data classification indicates the level of confidentiality, integrity, and availability protection that is required for each type of data set.

Each classification should have separate handling requirements and procedures pertaining to how that data is accessed, used, and destroyed.

To properly implement data classifications, a company must first decide upon the sensitivity scheme it is going to use. You're probably familiar with the one used in the military (top secret, secret, confidential, sensitive but unclassified, and unclassified).

The classification rules must apply to data no matter what format it is in.

Information Classification

Developing an Information Classification Program

1. Define classification levels
2. Specify criteria that will determine how data are classified
3. Data owners indicate the classification of data they own
4. Identify the data custodian who will be responsible for maintaining data and its security level
5. Identify the security controls required for each level
6. Document any exceptions to the previous issues
7. Indicate methods to transfer custody of data between owners
8. Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian
9. Indicate procedures for declassifying data
10. Integrate these issues into the security-awareness program so all employees understand how to handle data at different classification levels.

Layers of Responsibility

- Who's Involved?
- List of Roles
- Why So Many Roles?
- Personnel
- Structure
- Hiring Practices
- Employee Controls
- Termination

Layers of Responsibility

Players involved

- **Board of directors - ensure the shareholders' interests are being protected and the organization is being run properly**
- **Chief Executive Officer (CEO) - day-to-day management responsibilities, highest ranking officer**
- **Chief Financial Officer (CFO) - responsible for financial activities**
- **Chief Information Officer (CIO) - bridges the gap between IT and upper management, usually pretty technical**
- **Chief Privacy Officer (CPO) - usually an attorney responsible for ensuring data is kept safe**
- **Chief Security Officer (CSO) - creates and maintains a security program that facilitates business drivers and provides security and compliance**

Layers of Responsibility

Players involved (cont'd)

- **Security steering committee - makes decisions on tactical and strategic security issues, not tied to any business unit**
- **Audit committee - provide independent and open communications among the board, management, internal, and external auditors**
- **Data owner - due care responsibilities for protecting data**
- **Data custodian - maintains and protects the data**
- **System owner - integrates security considerations into application and system purchasing decisions and development projects**
- **Security administrator - executes security-related tasks**
- **Security analyst - develops policies, standards, guidelines, and baselines**

Layers of Responsibility

Players involved (cont'd)

- Application owner - dictates who can and cannot access their applications
- Supervisor - responsible for all user activity
- Change control analyst - approves or rejects requests to make changes to the network, systems, or software
- Data analyst - ensures that data is stored in a reasonable manner and those who require access have access
- Process owner - responsible for properly defining, improving, and monitoring processes
- Solution provider - works with management and data owners to deploy solutions that reduce pain points

Layers of Responsibility

Players involved (cont'd)

- **The User - routinely uses the data, must have necessary level of access to perform their duties**
- **Product Line Manager - evaluates products in the market, works with vendors**
- **Auditor - brought in to determine if the controls have reached and comply with the security objectives identified by the organization or legislation**

Most environments won't contain all these roles, but the responsibilities still must be carried out.

Layers of Responsibility

Personnel

Definition:
Separation of duties - makes sure one individual cannot complete a critical task by themselves

In an organization with good separation of duties, collusion must occur in order for fraud to be committed.

Hiring Practices

- **NDAs should be used to protect company information.**
- **References should be checked, military records reviewed, education verified, and if necessary, a drug test should be given.**

You want to mitigate risk, lower hiring costs, and lower turnover rates.

Layers of Responsibility

Employee Controls

Rotation of duties - no person should stay in one position too long (they may gain too much control)

Mandatory vacation - allows time for other individuals to come in and detect any errors or fraudulent activities

Separation of duties - split knowledge, dual control

Layers of Responsibility

Termination

When terminating an employee, follow the following rules:

- **The employee must leave immediately under supervision of a manager or security guard.**
- **The employee must surrender any ID badges or keys, complete an exit interview, and return company supplies.**
- **That user's accounts and passwords should be disabled or changed immediately.**

Security-Awareness Training

- Different Types of Security-Awareness Training
- Evaluating the Program
- Specialized Security Training

Security-Awareness Training

- Security-awareness training should be comprehensive, tailored for specific groups, and organization-wide.
- By using a formalized process for security-awareness training, you can establish a method that will provide you with the best results for making sure policies and procedures are presented to the right people in an organization.
- Typically, you create a training program for three types of audiences:
  - management
  - staff
  - technical employees
- Each group should know who to report suspicious activities to, and how to handle those situations.

Security-Awareness Training

Evaluating the Program

Security-awareness training is a type of control, and as such it should be monitored and evaluated for its effectiveness.

A good indication of the effectiveness of the program is the number of reports of security incidents made before and after the training. If more incidents are reported, you know the employees are paying attention to the training (or perhaps the opposite).

Handling requirements (e.g. markings, labels, storage)

Dr. C.W. Perr

Shon Harris

Information Marking

- **Markings and designations serve these purposes:**
  - **a. Alert holders to the presence of classified information.**
  - **b. Identify, as specifically as possible, the exact information needing protection.**
  - **c. Indicate the level of classification assigned to the information.**
  - **d. Provide guidance on downgrading (if any) and declassification.**
  - **e. Give information on the source(s) of and reasons for classification of the information.**
  - **f. Warn holders of special access, control, or safeguarding requirements.**

Information Marking Exceptions

- No classification or other security markings may be applied to any article or portion of an article that has appeared in a newspaper, magazine, or other public medium.
- If such an article is evaluated to see if it contains classified information, the results of the review shall be kept separate from the article.
- However, the article and the evaluation may be filed together. Exceptions to specific marking requirements are included with the discussions of the markings.

Marking Classified Documents and Other Material (1)

- **Classified documents must bear the following markings. Material other than ordinary paper documents must have the same information either marked on it or made immediately available to holders by another means.**
  - **(Specific requirements for each type of marking are found in Requirements for special types of documents are covered in Section 3.**
  - **Marking material other than paper documents is covered in Section 4**

Marking Classified Documents and Other Material (1)

(1) The overall classification of the document.
(2) The agency, office of origin, and date of the document.
(3) Identification of the source(s) of classification of the information contained in the document and, for originally classified information, a concise reason for classification.

Marking Classified Documents and Other Material (3)

(4) Declassification instructions, and any downgrading instructions that apply. This requirement does not apply to documents containing Restricted Data (RD) or Formerly Restricted Data (FRD). This information is not marked with declassification instructions. SEP

(5) Identification of the specific classified information in the document and its level of classification (page markings and portion markings). SEP

(6) Control notices and other markings that apply to the document.

The holder of an improperly marked classified document should

Summary

- Information and asset classification
- Ownership (e.g. data owners, system owners)
- Protect privacy
- Appropriate retention
- Data security controls
- Handling requirements (e.g. markings, labels, storage)