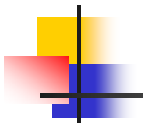
Risk Management

Dr.Talal Alkharobi

Risk Management

- Without an understanding of the security risks to an organization's information assets,
  - too many resources might be used
  - not enough resources might be used
  - resources might be used in the wrong way.
- By identifying risk, you learn the value of particular types of information and the value of the systems that contain that information.

3



Define Risk

- Risk is the potential for loss that requires protection.
- If there is no risk, there is no need for security.
- The two components for risk
  - vulnerabilities and
  - threats

4

Risk in insurance industry

- A person purchases insurance because a danger or peril is felt.
- The person may have a car accident that requires significant repair work.
- Insurance reduces the risk that the money for the repair may not be available.
- The insurance company sets the premiums for the person based on how much the car repair is likely to cost and the likelihood that the person will be in an accident.

Define Risk

5

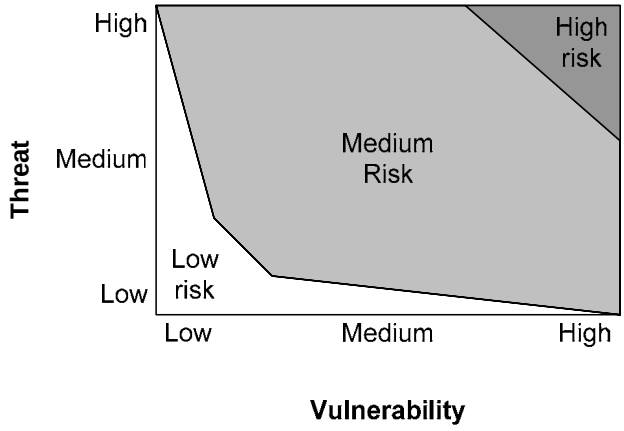
Risk in insurance industry

- Two components of risk:
  - The money needed for the repair.
    - The insurance company needs to pay this amount if an accident occurs.
    - This is the *vulnerability* of the insurance company.
  - The likelihood of the person to get into an accident.
    - This is the *threat* that will cause the vulnerability to be exploited (the payment of the cost of repair).

Define Risk

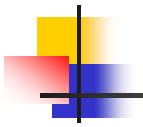
6

relationship between vulnerability and threat



Define Risk

7



Vulnerability

- A vulnerability is a potential avenue of attack.
- A vulnerability is characterized by the difficulty and the level of technical skill that is required to exploit it.
- The result of the exploitation should also be taken into account.

Define Risk

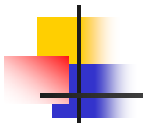
8

Vulnerability

- Vulnerabilities may exist in
  - Physical site security,
  - Computer systems : allowing the system to be open to a technical attack
  - Administrative procedures: allowing the environment to be open to a non-technical or social engineering attack
  - Networks, and the security of information in transit

Define Risk

9



high-danger Vulnerability

- Easy to exploit due to the existence of a script to perform the attack for example
- Allows the attacker to gain complete control over a system

Define Risk

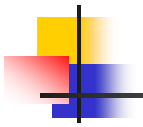
10

Low-danger Vulnerability

- Would require the attacker to invest significant resources for equipment and people
- Would only allow the attacker to gain access to insensitive information

Threats

11



Threat

- An action or event that might violate the security of an information systems environment.
- There are three components of threat:
  - Targets: The aspect of security that might be attacked
  - Agents: The people or organizations originating the threat
  - Events: The type of action that poses the threat
- To completely understand the threats to an organization, all three components must be examined.

Threats

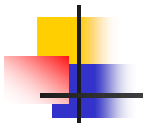
12

Targets

- The targets of threat or attack are generally the security services
  - confidentiality,
  - integrity,
  - availability, and
  - accountability.
- These targets correspond to the actual reason or motivation behind the threat.

Threats - Targets

13



Confidentiality

- Confidentiality is targeted when the disclosure of information to unauthorized individuals or organizations is the motivation.
- In this case the attacker wishes to know something that would normally be kept from him, such as classified government information.
- Information that is normally kept private within commercial organizations, such as salary information or medical histories, *can* also be a target.

Threats - Targets

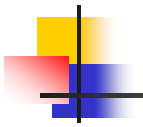
14

Integrity

- Integrity is the target when the threat wishes to change information.
- The attacker in this case is seeking to gain from modifying some information (increasing balance amount in a bank account)

Threats - Targets

15



availability

- Availability is targeted through the performance of a denial-of-service attack.
- Such attacks *can* target the availability of information, applications, systems, or infrastructure.
- Threats to availability can be short-term or long-term as well.

Threats -Targets

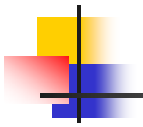
16

accountability

- Accountability is rarely targeted as an end unto itself.
- When accountability is targeted by a threat, the purpose of such an attack is to prevent an organization from reconstructing past events.
- Accountability may be targeted as a prelude to an attack against another target such as to prevent the identification of a database modification
- To cast doubt on the security mechanisms actually in place within an organization.

Threats

17



Targets

- A threat may have multiple targets.
- For example, accountability may be the initial target to prevent a record of the attacker's actions from being recorded, followed by an attack against the confidentiality of an organization's critical data

Threats

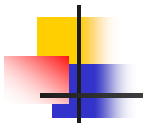
18

Agents

- The agents of threat are the people who may wish to do harm to an organization.
- To be a credible part of a threat, an agent must have three characteristics:
  - Access
  - Knowledge
  - Motivation
- A threat occurs when an agent with access and knowledge gains the motivation to take action.

Threats - Agents

19



Access

- An agent must have access to the system, network, facility, or information that is desired.
- This access may be direct (the agent has an account on the system) or indirect (the agent may be able to gain access to the facility through some other means).
- The access that an agent has directly affects the agent's ability to perform the action necessary to exploit a vulnerability
- A component of access is opportunity. Opportunity may exist in any facility or network just because an employee leaves a door propped open.

Threats - Agents

20

Knowledge

- An agent must have some knowledge of the target.
- The more familiar an agent is with the target, the more likely it is that the agent will have knowledge of existing vulnerabilities.
- Agents that have detailed knowledge of existing vulnerabilities will likely also be able to acquire the knowledge necessary to exploit those vulnerabilities.

Threats - Agents

21

Knowledge useful for an agent

- User IDS
- Passwords
- Locations of files
- Physical access procedures
- Names of employees
- Access phone numbers
- Network addresses
- Security procedures

Threats- Agents

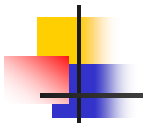
22

Motivation

- The reasons an agent might have for posing a threat to the target
- An agent requires motivation to act against the target.
- Motivation is usually the key characteristic to consider regarding an agent as it may also identify the primary target.

Threats - Agents

23



Motivation

- Motivations to consider include the following:
  - Challenge: A desire to see if something is possible and be able to brag about it
  - Greed: A desire for gain; this may be a desire for money, goods, services, or information
  - Malicious intent: A desire to do harm to an organization or individual

Threats - Agents

24

Agents to Consider

Type	Access	Knowledge	Motivation
Employee	Yes	Yes	Possible (L)
Ex-Employee	Maybe	Yes	Possible
Hacker			Yes
Commercial rivals		Some	Possible (H)
Terrorist	Maybe		Yes
Criminals			Yes
Public			Possible
Service Providers	Maybe	Yes	Possible
Customers/Visitors	Some	Some	Possible
Natural Disasters	Yes	Not needed	Not needed

Threats

25

Events

- Events are the ways in which an agent of threat may cause the harm to an organization.
- A hacker may cause harm by maliciously altering an Web site.
- Another way of looking at the events is to consider what harm could possibly be done if the agent gained access.

Threats - Events

26

Events to be considered (1)

- Misuse of authorized access to information, systems, or sites
- Malicious alteration of information
- Accidental alteration of information
- Unauthorized access to information, systems, or sites
- Malicious destruction of information, systems, or sites
- Accidental destruction of infomation, systems, or sites
- Malicious physical interference with systems or operations

Threats - Events

27

Events to be considered (2)

- Accidental physical interference with systems or operations
- Natural physical events that may interfere with systems or operations
- Introduction of malicious software (intentional or not) to systems
- Disruption of internal or external communications
- Passive eavesdropping of internal or external communications
- Theft of hardware or software

28

Threats List (1)

- T01 Access (Unauthorized to System - logical)
- T02 Access (Unauthorized to Area - physical)
- T03 Airborne Particles (Dust)
- T04 Air Conditioning Failure
- T05 Application Program Change (Unauthorized)
- T06 Bomb Threat
- T07 Chemical Spill
- T08 Civil Disturbance
- T09 Communications Failure
- T10 Data Alteration (Error)

29

Threats List (2)

- T11 Data Alteration (Deliberate)
- T12 Data Destruction (Error)
- T13 Data Destruction (Deliberate)
- T14 Data Disclosure (Unauthorized)
- T15 Disgruntled Employee
- T16 Earthquakes
- T17 Errors (All Types)
- T18 Electro-Magnetic Interference
- T19 Emanations Detection
- T20 Explosion (Internal)

30

Threats List (3)

- T21 Fire, Catastrophic
- T22 Fire, Major
- T23 Fire, Minor
- T24 Floods/Water Damage
- T25 Fraud/Embezzlement
- T26 Hardware Failure/Malfunction
- T27 Hurricanes
- T28 Injury/Illness (Personal)
- T29 Lightning Storm
- T30 Liquid Leaking (Any)

31

Threats List (4)

- T31 Loss of Data/Software
- T32 Marking of Data/Media Improperly
- T33 Misuse of Computer/Resource
- T34 Nuclear Mishap
- T35 Operating System Penetration/Alteration
- T36 Operator Error
- T37 Power Fluctuation (Brown/Transients)
- T38 Power Loss
- T39 Programming Error/Bug
- T40 Sabotage

32

Threats List (5)

- T41 Static Electricity
- T42 Storms (Snow/Ice/Wind)
- T43 System Software Alteration
- T44 Terrorist Actions
- T45 Theft (Data/Hardware/Software)
- T46 Tornado
- T47 Tsunami (Pacific area only)
- T48 Vandalism
- T49 Virus/Worm (Computer)
- T50 Volcanic Eruption

Example Vulnerabilities
P*hysical*

33

- *Susceptible to unauthorized building access*
- *Computer Room susceptible to unauthorized access*
- *Media Library susceptible to unauthorized access*
- *Inadequate visitor control procedures*
- *and many more*

Example Vulnerabilities
Administrative

34

- *Lack of management support for security*
- *No separation of duties policy*
- *Inadequate/no emergency action plan*
- *Inadequate/no computer security plan policy*

Example Vulnerabilities *Personnel*

35

- *Inadequate personnel screening*
- *Personnel not adequately trained in job*
- *Bad or no termination policy*

Example Vulnerabilities *Software*

36

- *Inadequate/missing audit trail capability*
- *Audit trail log not reviewed weekly*
- *Inadequate control over application/program changes*

Example Vulnerabilities *Communications*

37

- *Inadequate communications system*
- *Lack of encryption*
- *Potential for disruptions*

Example Vulnerabilities *Hardware*

38

- *Lack of hardware inventory*
- *Inadequate monitoring of maintenance personnel*
- *No preventive maintenance program*
- *Susceptible to electronic emanations*

Risk

39

Threat + Vulnerability = Risk

- Risk is the combination of threat and vulnerability.
- Threats without vulnerabilities pose no risk.
- Vulnerabilities without threats pose no risk.
- In the real world, neither of these conditions actually exists.
- The measurement of risk, therefore, is an attempt to identify the likelihood that a detrimental event will occur.
- Risk can be qualitatively defined as Low, Medium or High

Risk

40

Low Risk

- The vulnerability poses a level of risk to the organization, though it is unlikely to occur.
- Action to remove the vulnerability should be taken if possible, but the cost of this action should be weighed against the small reduction in risk.

Risk

41

Medium Risk

- The vulnerability poses a significant level of risk to the confidentiality, integrity, availability, and/or accountability of the organization's information, systems, or physical sites.
- There is a real possibility that this may occur.
- Action to remove the vulnerability is advisable.

Risk

42

High Risk

- The vulnerability poses a real danger to the confidentiality, integrity, availability, and/or accountability of the organization's information, systems, or physical sites.
- Action should be taken immediately to remove this vulnerability.

Risk

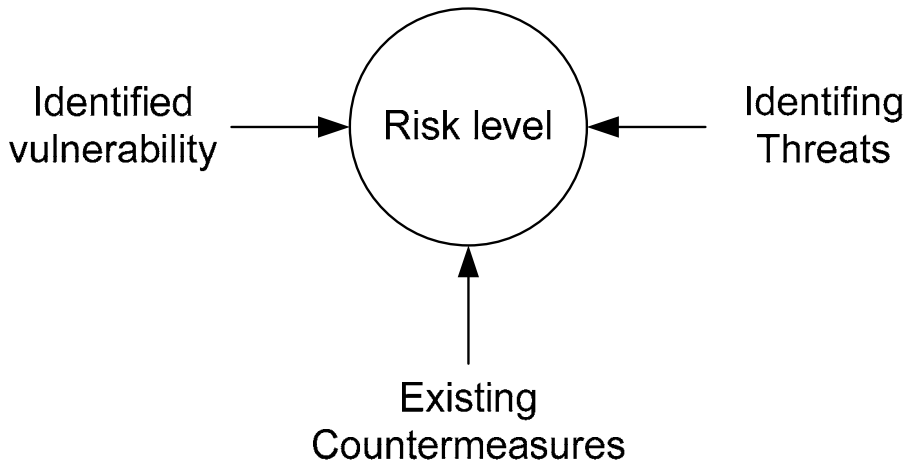
43

Risk

- When available, the ramification of a successful exploitation of vulnerability by a threat must be taken into account.
- If the cost estimates are available, they should be applied to the risk level to better determine the feasibility of taking corrective action

44

Identify the Risk to an Organization



Identify the Risk

45

Identifying Vulnerabilities

- When identifying specific vulnerabilities, begin by locating all the entry points to the organization.
- In other words, find all the access points to information (in both electronic and physical form) and systems within the organization.

Identify the Risk

46

Identifying Vulnerabilities

- This means identifying the following:
  - Internet connections
  - Remote access points
  - Connections to other organizations
  - Physical access to facilities
  - User access points
  - Wireless access points

Identify the Risk

47

Identifying Vulnerabilities

- For each of these access points,
  - Identify the information and systems that are accessible.
  - Identify how the information and systems may be accessed.
  - Include known vulnerabilities in operating systems and applications
- This will identify the major vulnerabilities of the organization.

48

Identifying Real Threats

- Threat assessment is a very detailed and difficult task.
- Some threats are obvious such as competitors.
- True threats will attempt to remain hidden (until an event has occurred)
- A threat is the combination of a known agent having known access with a known motivation performing a known event against a known target.

49

Identifying Real Threats

- Example
  - disgruntled employee (the agent)
  - who desires knowledge of the latest designs an organization is working on (the motivation).
  - has access to the organization's information systems (access)
  - knows where the information is located (knowledge).
  - is targeting the confidentiality of the new designs and may attempt to force his way into the files he wants (the event).

50

Identifying Real Threats Generic level of threat

- A generic level of threat is that we are not paranoid, somebody is out to get us.
- This threat would be comprised of anyone with potential access to an organization's systems or information.
- The threat exists because a human (employee, customer, supplier, and so on) must access the system and information used in the organization in order to be useful.

51

Examining Countermeasures

- Vulnerabilities cannot be examined in a vacuum.
- A potential avenue of attack must be examined in the context of the environment, and compensating controls must be taken into account when determining if vulnerability truly exists.

52

Countermeasures

- Firewalls
- Anti-virus software
- Access controls
- Authentication systems
- Badges
- Biometric
- Card readers for access to facilities
- Guards
- File access controls
- Encryption
- Conscientious, well-trained employees
- Intrusion detection systems
- Automated patch and policy management systems

53

Examining Countermeasures

- For each access point within an organization, countermeasures should be identified.
- Internet connection provides potential access to the systems.
- This access point is protected by a firewall.
- Examination of the rule set on the firewall will identify the extent to which an external entity can actually access internal systems.
- Therefore, some of the vulnerabilities via this access point may not be available to an external attacker since the firewall prevents access to those vulnerabilities or systems in their entirety.

54

Identifying Risk

- Once vulnerabilities, threats, and countermeasures are identified, we can identify specific risks to the organization.
- The question is now simple: Given the identified access points with the existing countermeasures, what could someone do to the organization through each access point?
- For the answer to this question, we take the likely threats for each access point (or a generic threat) and examine the potential targets (confidentiality, integrity, availability, and accountability) through each access point.

55

Identifying Risk

- Based on the damage that can be done, each risk is then rated as a high risk medium risk, or low risk.
- Same vulnerability may have different levels of risk based on the access point.

56

Identifying Risk Example

- An internal system has a vulnerability in its mail system.
- From the outside,
  - An attacker must find the system through the Internet firewall.
  - The system is not accessible so there is no risk.

Identifying Risk Example

57

- Internal employees
  - have access to the system since they do not need to enter the network through the firewall.
  - Any internal employee could exploit this vulnerability and gain access to the system.
  - Employees are not considered a likely source of threat, so the risk is classified as a medium risk level.

Identifying Risk Example

58

- At the physical access to the facility
  - physical controls are weak and an individual could walk in off the street and gain access to a system on the network.
  - Controls on the network do not prevent an unauthorized system from plugging in and coming up on the internal network.
  - An individual with the motivation could gain physical access to the network and bring up an unauthorized system.
  - This system would exploit the vulnerable mail system.
  - The risk should now be classified as a high risk.

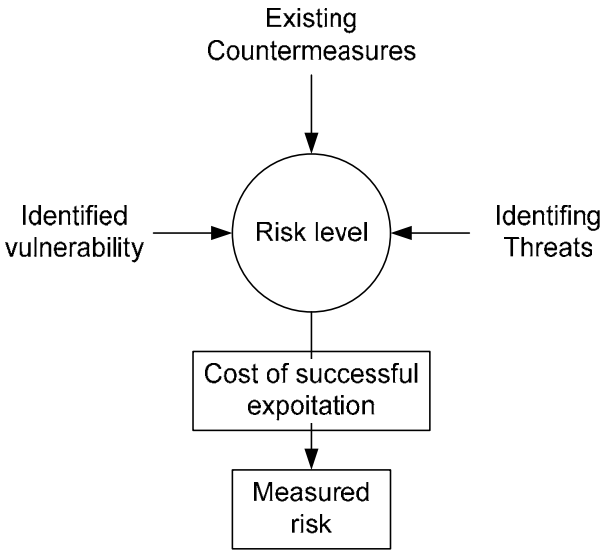
59

Measure Risk

- To be valuable, a risk assessment must identify the costs to the organization if an attack is successful.
- The cost to the organization if a risk is realized is the deciding factor for any decision on how to manage the risk.
- Remember, risk can never be completely removed, risk must be managed.

60

Measuring risk



61

Money

- The most obvious way to measure risk is by the amount of money a successful penetration of an organization might cost.
- This cost can include the following:
  - Lost productivity
  - Stolen equipment or money
  - Cost of an investigation
  - Cost to repair or replace systems
  - Cost of experts to assist
  - Employee overtime

62

Measure risk

- As you can see from just this partial list, the costs of a successful penetration can be large.
- Some of these costs need to be estimated as they will be unknown until an actual event occurs.
- Perhaps the most difficult category to estimate is lost productivity:.
  - lost work that will never be recovered, or
  - costs to recovering the work that could have been done when the systems were down?

63

Measure risk

- The accounting or finance department of an organization can assist in identifying some of these costs.
- In many cases, however, the cost may not be available.

64

Measuring cost Example

- Manufacturing organization depends on a computer system to schedule work, order raw materials, and track jobs as they progress through the plant.
- If the system is unavailable, raw materials may run out in 24 hours and work schedules become unavailable after only 8 hours
- The cost could
  - Overtime required to get back on schedule
  - Costs of having the plant idle
  - Costs associated with late delivery

Measure risk Time

65

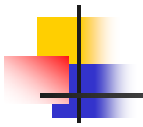
- Time is a measurement that is difficult to quantify.
- The time measurement may include
  - the amount of time a technical staff member is unavailable to perform normal tasks due to a security event (can be computed as the hourly cost of the technical person)
  - The time that other staff may be waiting for their computers to be fixed (how can this time be accounted for?)

Measure risk Time

66

- Time may also mean the downtime of a key system.
- If a Web site is compromised, it should be taken offline to rebuild
- What is the effect of this downtime on the organization?
- Perhaps a successful attack on an organization's systems leads to a delay in a product or service.
- How can this delay be measured and the cost to the organization be determined?
- Clearly, time, or perhaps lost time, must be included in the measurement of risk.

67



Resources

- Resources can be people, systems, communication lines, applications, or access.
- If an attack is successful, how many resources will have to be deployed to correct the situation?
- Obviously, the monetary cost of using a resource to correct a situation can be computed.
- However, how is the non-monetary cost of not having a particular staff person available to perform other duties measured?

68

Resources

- Assigning a dollar value to this situation is not easy and intangible
- The same issue exists for defining the cost of a slow network connection.
- Does it mean that employees are waiting longer for access to the Internet and therefore slowing down their work?
- Or does it mean that some work or some research is not being performed because the link is too slow?

69

Reputation

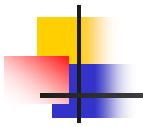
- The loss or degradation of reputation is a critical cost.
- What is the true cost to an organization of a lost reputation?
- Reputation can be considered equivalent to trust.
- This is the trust that the general public puts in the organization.
- For example, the reputation of a bank equates to the trust that the public will place in the safety of money placed in the bank.
- If the bank has a poor reputation or if evidence is released to the public that money placed in the bank is not safe, the bank is likely to lose customers.

70

Reputation

- In the extreme case, there may be a run on the bank.
- What if news that a bank was successfully penetrated is released?
- Will the public want to place money in such a bank?
- Will existing customers leave the bank?
- How can this damage be measured?

71



Reputation

- Reputation is an intangible asset that is built and developed over the course of time.
- The loss of reputation may not be easy to value, but such a loss will certainly impact the organization.

72

Lost Business

- Lost business is unrealized potential.
- The organization had the potential to serve some number of new customers or the potential to build and sell some number of products.
- If this potential is unrealized, how is this cost measured?
- It is certainly possible to show how projected revenues or sales were not achieved, but how was the failure to achieve linked to security risk?
- Can the realization of the risk impact the organization so that business is lost?

73

Lost Business Example

- An organization sells products over the Internet.
- The organization's Web site is down for four days.
- Since this Web site is the primary sales channel, it can be shown that four days of sales did not occur.
- What about the case where a disaster caused a manufacturer to halt production for four days?
- This means that four days' worth of goods were not produced.
- Would these goods have been sold if they were available?
- Can this loss be measured in a meaningful way?

74

Methodology for Measuring Risk

- Clearly, there are a lot more questions than answers when measuring risk.
- If all risks could be translated into monetary terms this process would be much easier.
- The reality of the situation does not allow for this.
- Therefore, we must use the information that is available in order to measure risk.

75

Methodology for Measuring Risk

- For each risk, identify a best case, worst case, and most likely case scenario.
- Then for each risk measurement (money, time, resources, reputation, and lost business), identify the damage in each scenario.
- Scenarios should be built based on these criteria:
  - Best case
  - Worst case
  - most likely case

76

Methodology for Measuring Risk Best case

- The penetration was noticed immediately by the organization.
- The problem was corrected quickly and the information was contained within the organization.
- Overall damage was limited.

Methodology for Measuring Risk Worst case

77

- The penetration was noticed by a customer who notified the organization.
- The problem was not immediately corrected.
- Information about the penetration was provided to the press who broadcast the story.
- Overall damage was extensive.

Methodology for Measuring Risk Most likely case

78

- The penetration was noticed after some amount of time.
- Some information about the event leaked to customers but not the whole story, and the organization was able to control much of the information.
- Overall damage was moderate.
- The characteristics of the most likely case should be modified based on the true security conditions within the organization.
- In some cases, the most likely case will be the worst case.

79

Risk Management

- Now for each identified risk examine the potential results in each risk measurement area.
- Ask the following questions:
  - How much money will a successful penetration cost?
  - Track staff time, consultant time, and new equipment costs.
  - How long will a successful penetration take to correct?
  - Will a successful penetration impact new product or existing production schedules?

80

Risk Management

  - What resources will be impacted by a successful penetration?
  - What parts of the organization rely on these resources?
  - How will this event impact the organization's reputation?
  - Will a successful penetration cause any business to be lost?
  - If so, how much and what type?
- Once each question is answered, construct a table that shows the potential results for each risk.
- This information can then be used to develop appropriate risk management approaches.

81

Things will help

- Vulnerability Detection Tools
- Keeping up with Security Publications
- Avoid Single Point of Failure
- Control: Mechanisms or procedures for mitigating vulnerabilities

82

Vulnerability Detection Tools

- Computer Oracle and Password System (COPS) – FREE
  - Checks vulnerabilities of UNIX systems
- Secure Analysis Tool for Auditing Networks (SATAN) – FREE
- SAFEsuite (Internet Security Systems, Inc.)
  - Family of network security assessment tools (web security scanner, firewall scanner, intranet scanner, system security scanner)
  - Keyed to the IP address of the customer

83

Keeping up with Security Publications

- Legal publications: how to remove vulnerabilities
  - CERT advisories
  - SANS Security Digest
- Hacker publications: “how to” exploit known vulnerabilities
- Security mailing lists

84

Avoid Single Point of Failure

- Critical information resources
  - Identification
  - Backup
  - Hiding
- Separation of duties
  - Multi-person requirements
  - Limit temptations

85

Example Controls (1)

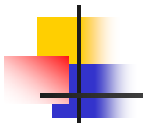
- Access control devices - physical
- Access control lists - physical
- Access control - software
- Assign ADP security and assistant in writing
- Install-/review audit trails
- Conduct risk analysis
- Develop backup plan
- Develop emergency action plan
- Develop disaster recovery plan
- Install walls from true floor to true ceiling

86

Example Controls (2)

- Develop visitor sip-in/escort procedures
- Investigate backgrounds of new employees
- Restrict numbers of privileged users
- Develop separation of duties policy
- Require use of unique passwords for logon
- Make password changes mandatory
- Encrypt password file
- Encrypt data/files
- Hardware/software training for personnel
- Prohibit outside software on system3

87



Example Controls (3)

- Develop software life cycle development program
- Conduct hardware/software inventory
- Designate critical programs/files
- Lock PCs/terminals to desks
- Update communications system/hardware
- Monitor maintenance personnel
- Shield equipment from electromagnetic interference/emanations
- Identify terminals