Risk Assessment

Risk Assessment

- **Summary of Vulnerability Analysis**

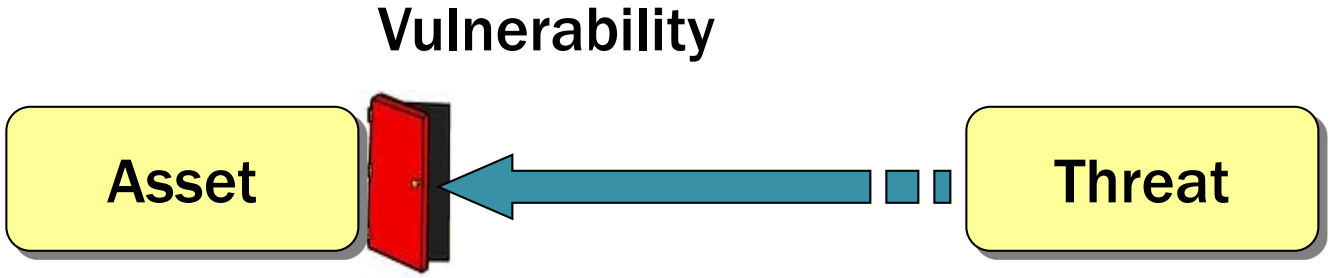
People
Procedure
Data
Software
Hardware
Networking

flaw or weakness in asset's design, implementation, or security procedure

cause damage (loss)

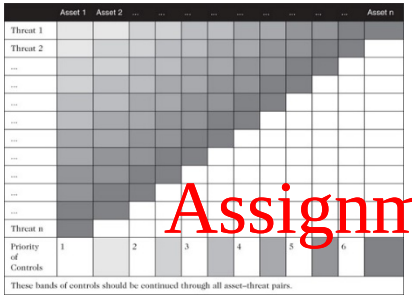
exploit

Act of human error or failure
Deliberate act of trespass
Deliberate act of extortion
Deliberate act of sabotage
Deliberate software attacks
Technical software failures
Technical hardware failures
Forces of nature
Etc.



Risk Assessment (cont.)

- **Risk Assessment** – provides relative numerical risk ratings (scores) to each vulnerability



  - in risk management, it is not the presence of a vulnerability that really matters, but the associated risk!

- (Security) **Risk** – quantifies/reflects:
  1) possibility that a threat successfully acts upon a vulnerability and
  2) how severe the consequences would be

$$R = P * V$$

  - P = probability of successful risk-event occurrence
  - V = value lost / cost to organization

Risk Assessment (cont.)

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 Webserver 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

Weighted score indicating the relative importance (associated loss) of the given asset.

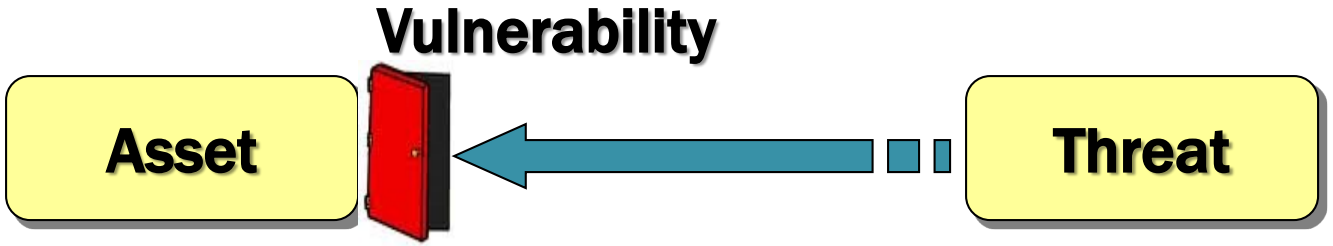
Should be used if concrete $ amounts are not available.

Risk Assessment (cont.)

- **Extended Risk Formula v.1.**

$$R = \underbrace{P_a \cdot P_s}_{P} \cdot V$$

- P_a = probability that an attack/ threat (against a vulnerability) takes place
- P_s = probability that the attack successfully exploits the vulnerability



Risk Assessment (cont.)

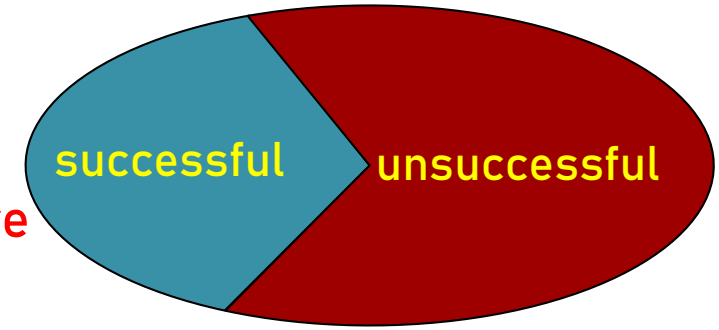
- **Extended Risk Formula v.2.**

$$R = P_a \cdot (1-P_e) \cdot V$$

P_s

- P_e = probability that the system's security measures effectively protect against the attack (reflection of system's security effectiveness)

possible outcomes of a conducted attack



P_s = probability that the attack is successfully executed

system defences are NOT effective

P_e = probability that the attack is **NOT** successfully executed, i.e.

system defences are effective

Risk Assessment (cont.)

- **Extended Whitman's Risk Formula ***

$$R = P \cdot V - CC \cdot (P \cdot V) + UK \cdot (P \cdot V)$$

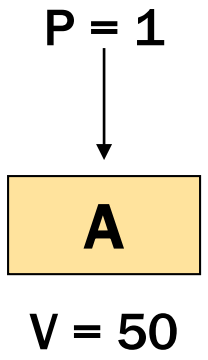
$$= P \cdot V \cdot [1 - CC + UK]$$

- P = probability that certain vulnerability (affecting a particular asset) gets exploited <u>if no control</u> is applied
- V = value of information asset $\in$ [1, 100]
- CC = current control = percentage/fraction of risk already mitigated by current control
- UK = uncertainty of knowledge = fraction of risk that is not fully known

Risk Assessment (cont.)

Risk = P · V · [1 – CC + UK]

Example: Risk determination



Asset A

Has a value of 50.

Has one vulnerability with a likelihood of 1.0.

No current control for this vulnerability.

Your assumptions and data are 90% accurate.

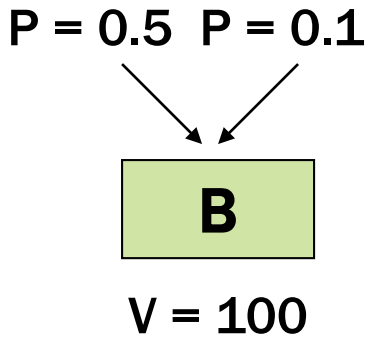
Asset B

Has a value of 100.

Has two vulnerabilities:

* vulnerability #2 with a likelihood of 0.5, and
  a current control that addresses 50% of its risk;
* vulnerability #3 with a likelihood of 0.1 and
  no current controls.

Your assumptions and data are 80% accurate.



Which asset/vulnerability should be dealt with first ?!

Risk Assessment (cont.)

Risk = P · V · [1 – CC + UK]

Example: Risk determination

The resulting ranked list of risk ratings for the three vulnerabilities is as follows:

Asset A:

Vulnerability 1 rated as **55** = 50*1* (1.0 - 0 + 0.1)

Asset B:

Vulnerability 2 rated as **35** = 100*0.5* (1 - 0.5 + 0.2)

Asset B:

Vulnerability 3 rated as **12** = 100*0.1* (1 – 0 + 0.2)

Risk Assessment (cont.)

vulnerable assets

V: weighted asset value

each asset's vulnerability

P: likelihood of vulnerability realization

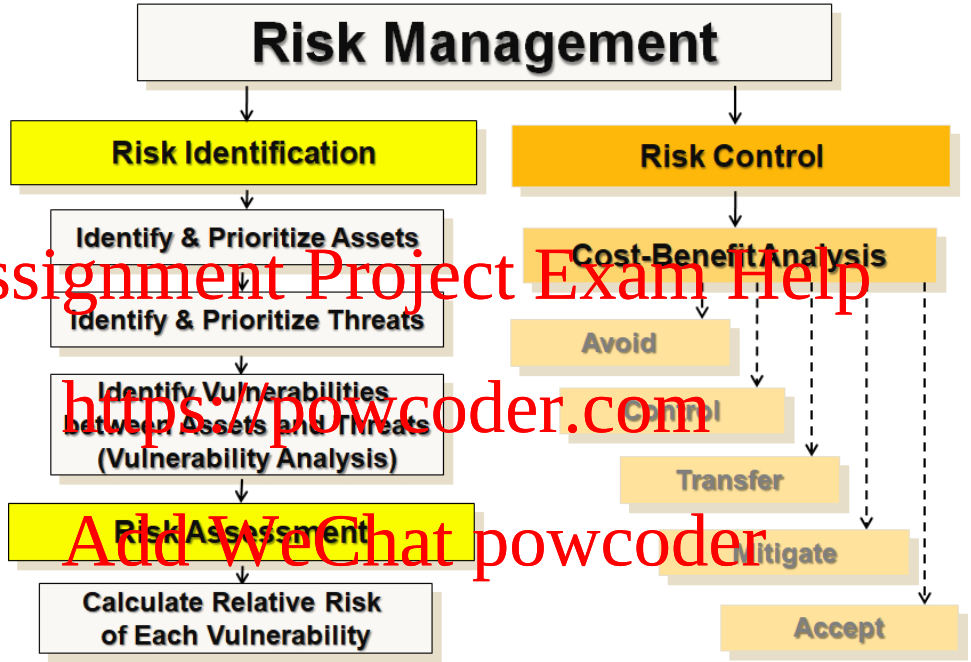
V x P

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 service email has relatively low value but represents most pressing issue due to high vulnerability likelihood.

- **At the end of risk assessment process, the TVA and/or ranked-vulnerability worksheets should be used to develop a prioritized list of tasks.**

Risk Control



What do we do with critical vulnerabilities ?!

If a 'technical fix' exists, should we implement that fix ?!

Risk Control Strategies

Once all vulnerabilities/risks are evaluated, the company has to decide on the 'course of action' – often influenced by $$$ …

for each critical vulnerability we have identified an adequate risk-treatment (i.e., control)

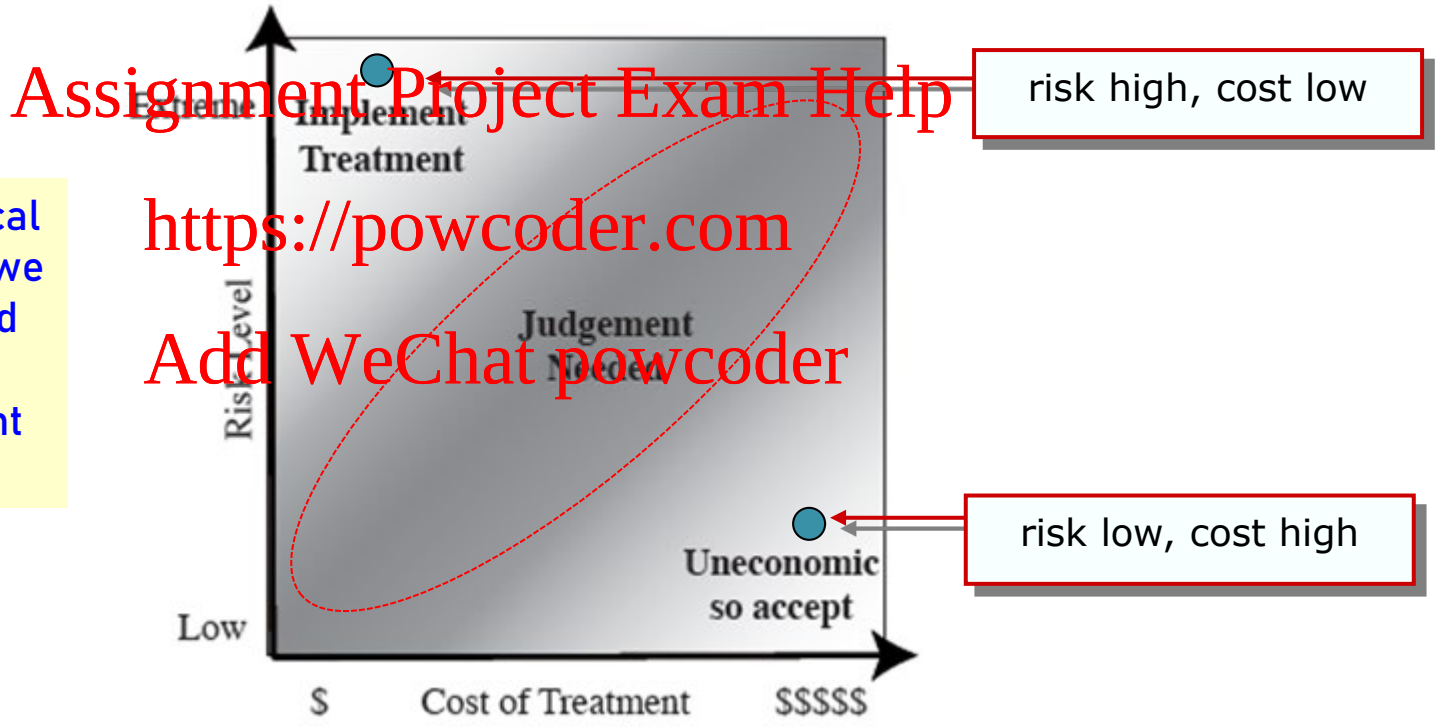


Figure 14.5 Judgment About Risk Treatment

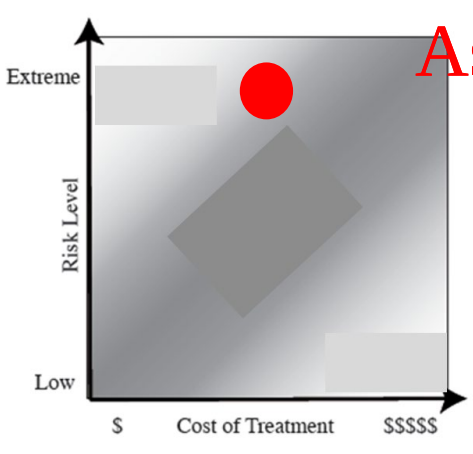
Computer Security, Stallings, pp. 487

Risk Control Strategies (cont.)

- **Basic Strategies to Control Risks**
  - **Avoidance**
    - do not proceed with the activity or system that creates this risk
  - **Reduced Likelihood** (**Control** / Implement the Fix)
    - by implementing suitable controls, lower the chances of the vulnerability being exploited
  - **Transference**
    - share responsibility for the risk with a third party
  - **Mitigation**
    - reduce impact should an attack still exploit the vulnerability
  - **Acceptance**
    - understand consequences and acknowledge risks without any attempt to control or mitigate

Risk Control Strategies (cont.)

- **Reduced Likelihood (Control)** – risk control strategy that attempts to prevent exploitation of vulnerability by means of following techniques:

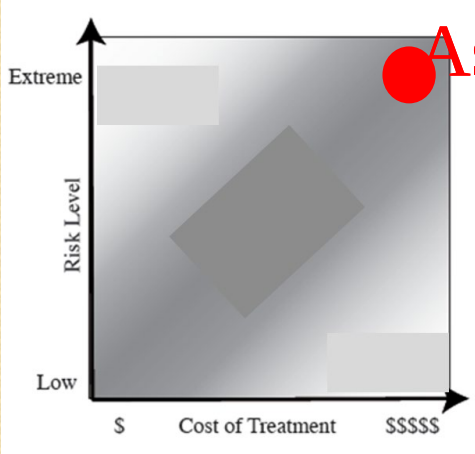


- application of technology
  - implementation of security controls & safeguards, such as: anti-virus software, firewall, secure HTTP and FTP servers, etc.
- policy
  - e.g. insisting on safe procedures
- training and education
  - change in technology and policy must be coupled with employee's training and education

Recommended for vulnerabilities with high risk factor that are moderately costly to fix.

Risk Control Strategies (cont.)

- **Avoidance** – strategy that results in complete abandonment of activities or systems due to overly excessive risk

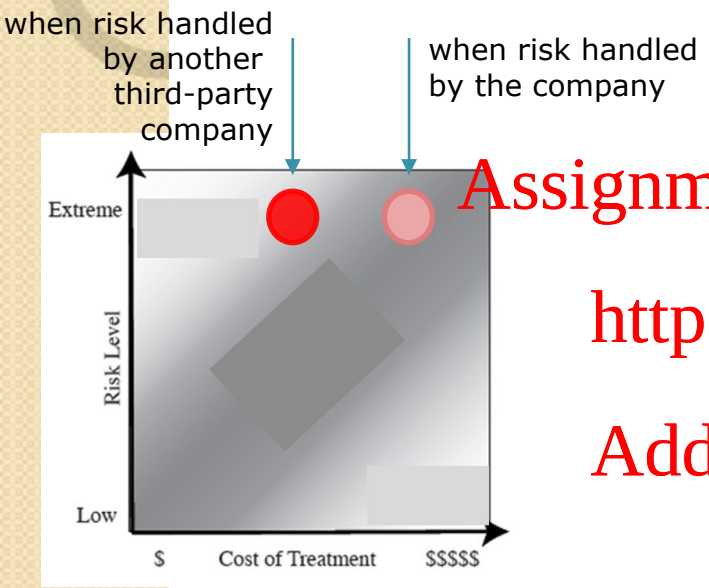


  - usually results in loss of convenience or ability to perform some function that is useful to the organization
  - the loss of this capacity is traded off against the reduced risk profile

Recommended for vulnerabilities with very high risk factor that are very costly to fix.

Risk Control Strategies (cont.)

- **Transference** – risk control strategy that attempts to shift risk to other assets, other processes or other organizations

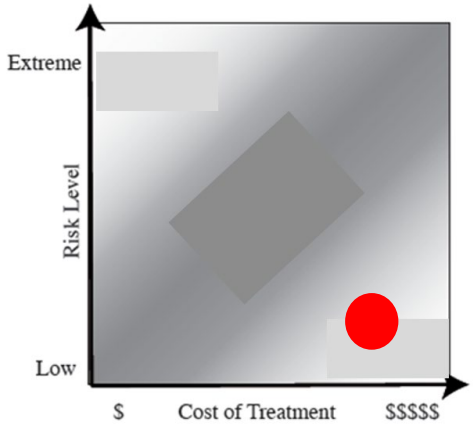


  - if organization does not have adequate security experience, hire individuals or firms that provide expertise
    - e.g., by hiring a Web consulting firm, risk associated with domain name registration, Web presence, Web service, … are passed onto organization with more experience

Recommended for vulnerabilities with high risk factor that are moderately costly to fix if employing outside expertise.

Risk Control Strategies (cont.)

- **Mitigation** – risk control strategy that attempts to reduce the significance of impact caused by a vulnerability – includes 3 plans:

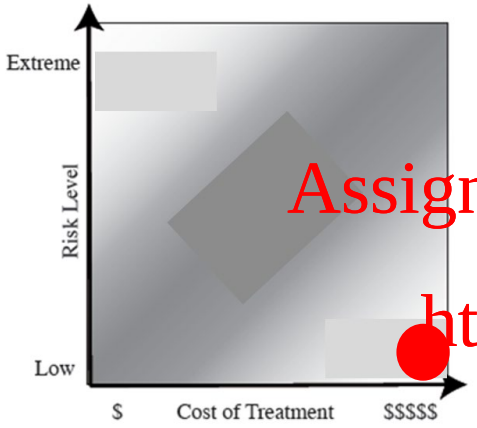


Plan	Description	Example	When deployed	Timeframe
Incident Response (IR) Plan	Actions an organization takes during incidents (attacks)	• List of steps to be taken during disaster • Intelligence gathering • Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster Recovery (DR) Plan	• Preparations for recovery should a disaster occur • Step-by-step instructions to regain normalcy	• Procedures for the recovery of lost data • Procedures for the … to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business Continuity (BC) Plan	Steps to ensure continuation of the overall business when the scale of a disaster exceeds the DRP's ability to quickly restore operations	• Preparation steps for activation of secondary data centers • Establishment of a hot site in a remote location	Immediately after the disaster is determined to affect the continued operations of the organization	Long-term organization

Recommended for vulnerabilities that are low-risk and moderately costly to fix.

Risk Control Strategies (cont.)

- **Acceptance** – assumes NO action towards protecting an an information asset – accept outcome …



  - should be used only after doing all of the following

steps to be discussed:

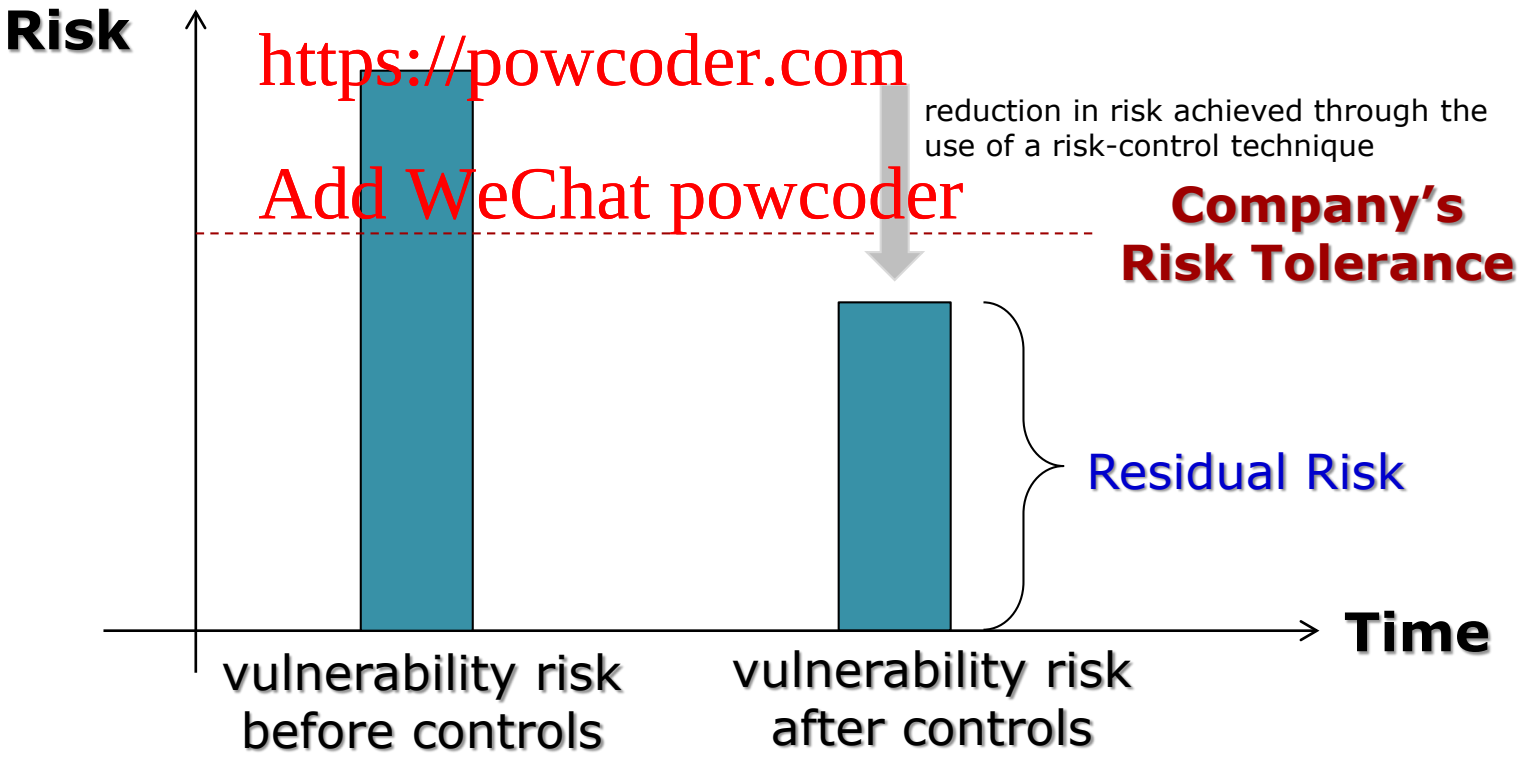
  - ➢ assess the probability of attack and likelihood of successful exploitation of a vulnerability
  - ➢ approximate annual occurrence of such an attack
  - ➢ estimate potential loss that could result from attacks
  - ➢ perform a thorough cost-benefit analysis assuming various protection techniques
  - ➢ **determine that particular asset did not justify the cost of protection!**

Recommended when vulnerability risk < cost of any control.

Risk Control Strategies (cont.)

How do we know whether risk control techniques have worked / are sufficient?!

Example: Risk tolerance vs. residual risk



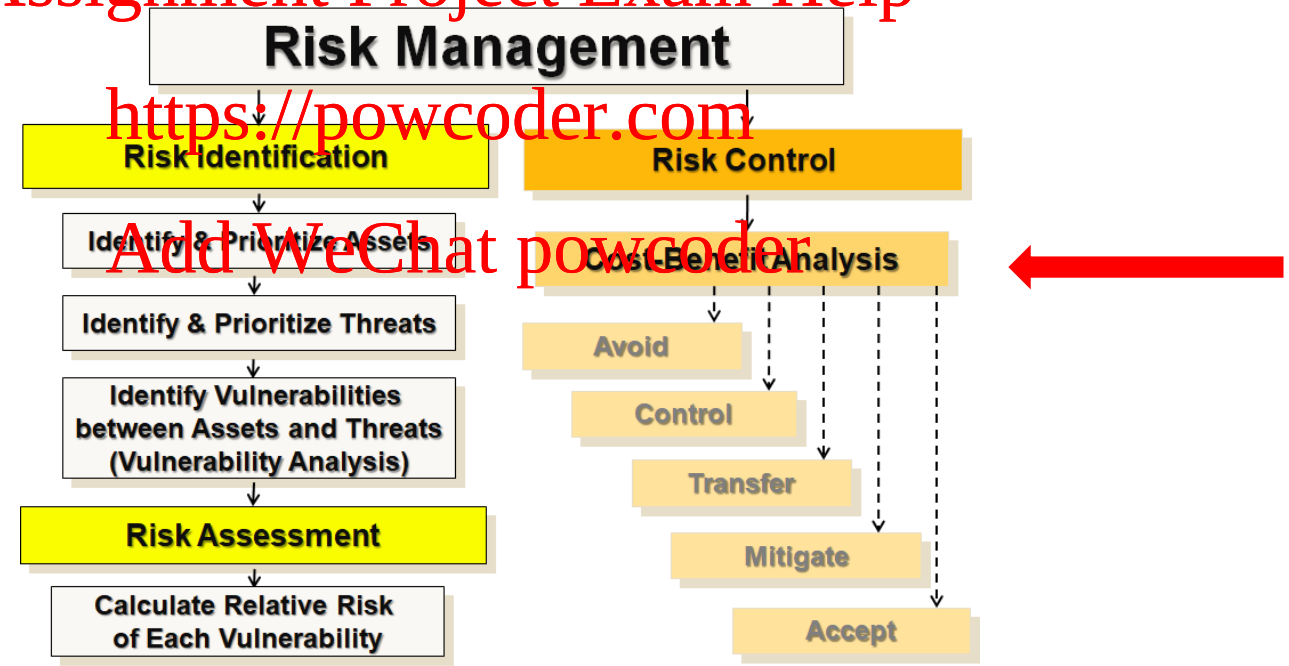
Risk Control Strategies (cont.)

- **Risk Tolerance** – risk that organization is willing to accept after implementing risk-mitigation controls

- **Residual Risk** – risk that has not been completely removed, reduced or planned for, after (initial) risk-mitigation controls have been employed

  - goal of information security is not to bring residual risk to 0, but to bring it in line with companies risk tolerance
  - risk-mitigation controls may (have to) be reinforced until residual risk falls within tolerance

Cost-Benefit Analysis



Cost-Benefit Analysis

- **Cost-Benefit Analysis** – aka **economic feasibility** study - quantitative decision-making process that:

  - determines the loss in value if the asset remained unprotected
  - determines the cost of protecting an asset
  - helps prioritize actions and spending on security ...

Company should not spend more to protect an asset than the asset is worth!

Quantitative Risk Analysis (cont.)

- **Asset Value (AV)** – combination of the following:
  - cost of buying/developing hardware, software, service
  - cost of installing, maintaining, upgrading hardware, software, service
  - cost to train and re-train personnel
  - direct profit gained from the utilization of the asset

- **Exposure Factor (EF)** – percentage loss that would occur from a given vulnerability being exploited by a given threat in a single attack

Quantitative Risk Analysis (cont.)

- **Single Loss Expectancy (SLE)** – most likely loss (in value) from an attack

SLE = AV * EF

Example: A Web-site's SLE due to a DDoS Attack

Estimated value of a Web-site: AV = $ 1,000,000.

A DDoS on the site would result in 10% losses of the site value (EF=0.1).

SLE for the site: AV * EF = $ 100,000.

Would it be worth investing in anti-DDoS system that costs $100,000 a year?

Quantitative Risk Analysis (cont.)

- **Annualized Rate of Occurrence (ARO)** – indicates how often an attack is expected to successfully occur in a year
  - if an attack occurs 2 times every years ⇒ ARO = 2
  - if an attack occurs once every 2 years ⇒ ARO = 0.5

- **Annualized Loss Expectancy (ALE)** – overall loss incurred by an attack (i.e. by exploiting a vulnerability) in each year

ALE = ARO * SLE

Quantitative Risk Analysis (cont.)

Example: Determining ARO, SLE, ALE

Table 3.2 How SLE, ARO, and ALE Are Used

Asset	Threat Risk	Asset Value	Exposure Factor	SLE	Annualized Frequency	ALE
Customer database	Hacked	$432,000	.74	$320,000	.25	$80,000
Word documents and data files	Virus	$9,450	.17	$ 1,650	.9	$1,485
Domain controller	Server failure	$82,500	.88	$ 72,500	.25	$18,125
E-commerce website	DDoS	$250,000	.44	$110,000	.45	$49,500

http://www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/samplechapter/078973446X.pdf

Quantitative Risk Analysis (cont.)

Example: Determining ALE to Occur from Risks

http://www.windowsecurity.com/articles/Risk_Assessment_and_Threat_Identification.html

A widget manufacturer has installed new network servers, changing its network from P2P, to client/server-based network.

The network consists of 200 users who make an average of $20 an hour, working on 200 workstations.

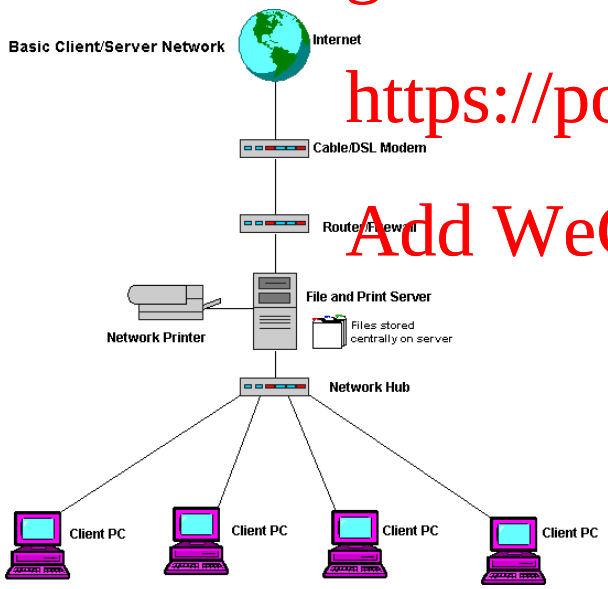
Previously, none of the workstations involved in the network had an anti-virus software installed on the machines. This was because there was no connection to the Internet and the workstations did not have USB/disk drives, so the risk of viruses was deemed minimal.

One of the new servers provides a broadband connection to the Internet, which employees can now use to send and receive email, and surf the Internet.

Quantitative Risk Analysis (cont.)

Example: Determining ALE to Occur from Risks (cont.)

- 200 employees
- 200 workstations
- $20 hour



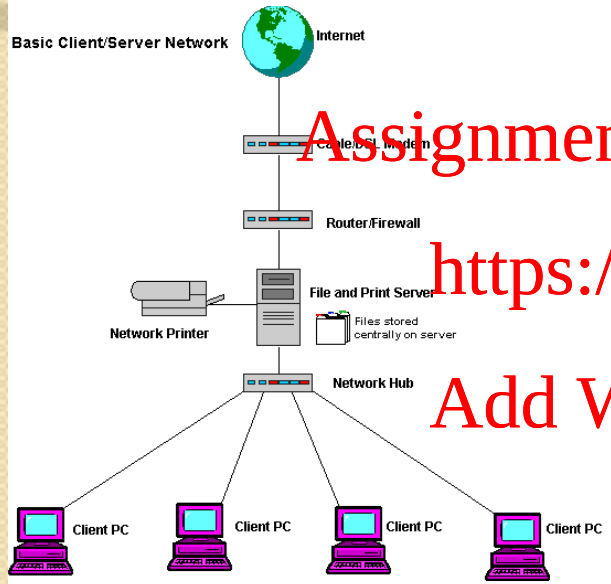
One of the managers read in a trade magazine that other widget companies have reported an annual 75% chance of virus infection after installing T1 lines, and it may take up to 3 hours to restore the system.

A vendor will sell licensed copies of antivirus for all servers and the 200 workstations at a cost of $4,700 per year.

The company has asked you to determine the annual loss that can be expected from viruses, and whether it is cost effective to purchase licensed copies of anti-virus software.

Quantitative Risk Analysis (cont.)

Example: Determining ALE to Occur from Risks (cont.)



Based on the provided data:

ARO = 0.75

SLE = 200 user * ($ 20 / user-hour) * 3 hours = $ 12,000

ALE = SLE * ARO = $ 9,000

ACS = $ 4,700

Because the ALE is $9,000, and the cost of the software that will minimize this risk is $4,700 per year, this means the company would save $4,300 per year by purchasing the software ($9,000 - $4,700 = $4,300).

Quantitative Risk Analysis (cont.)

- **Cost-Benefit Analysis Formula** – expresses cost benefit of a safeguard – i.e., determines whether a particular control is worth its cost

safeguard is justified if it results in NRRB>0

Gross risk reduction benefit

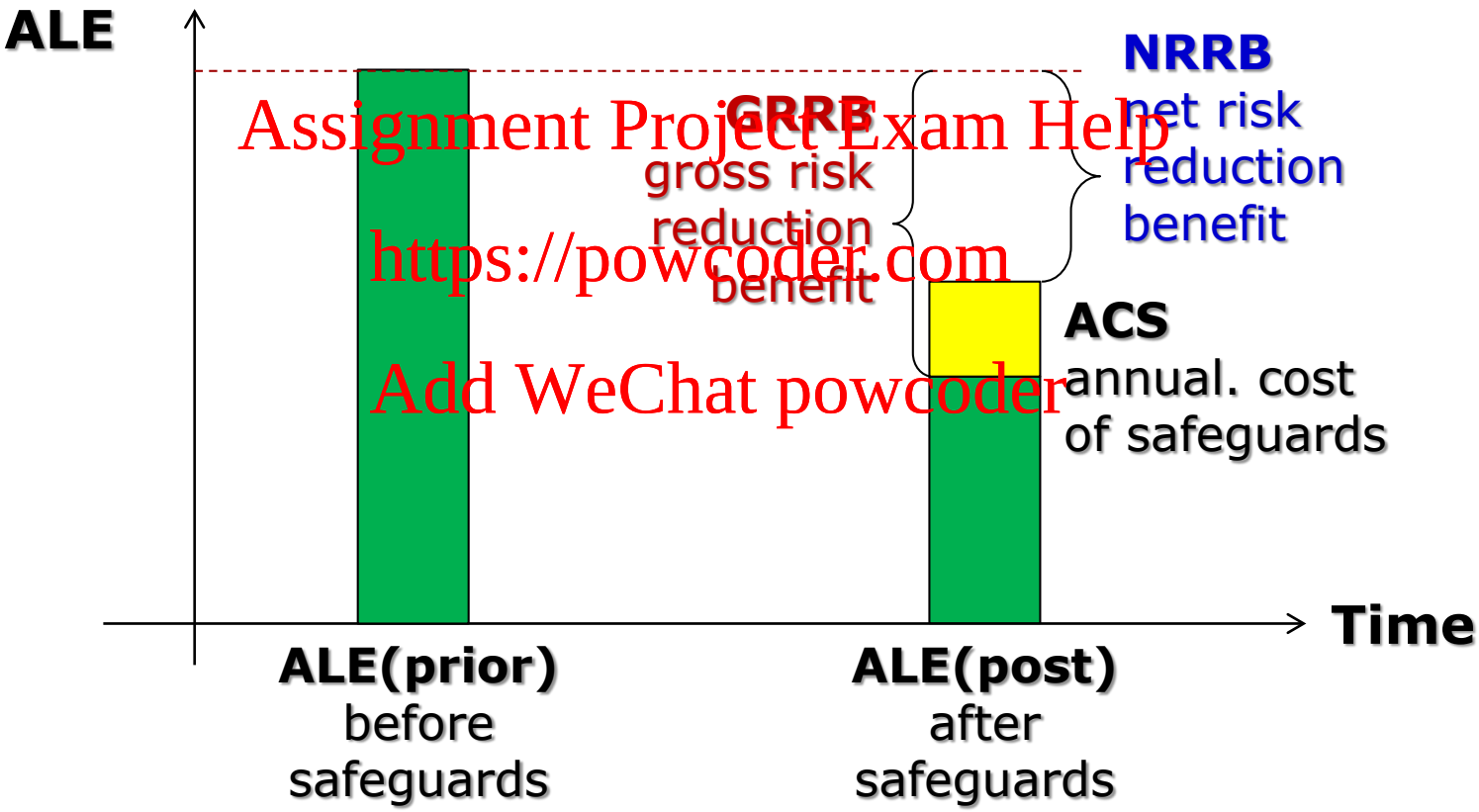
$$NRRB = [ALE(prior) - ALE(post)] - ACS$$

NET Risk Reduction Benefit (money saved)

- **ALE**(prior) – **ALE before implementing control**
- **ALE**(post) – **ALE after implementing control**
- **ACS – annual cost of safeguard**

Quantitative Risk Analysis (cont.)

Example: Cost-Benefit Analysis



Only NRRB>0 justifies the use of safeguard(s)!

Quantitative Risk Analysis (cont.)

Example: Determining NRRB

Your organization has decide to centralize anti-virus support on a server which automatically updates virus signatures on user's PCs.

When calculating risk due to viruses, the annualized loss expect. (ALE) is $145,000. The cost of this anti-virus countermeasure is estimated to $24,000/year, and it will lower the ALE to $65,000.

Is this a cost-effective countermeasure? Why or why not?

ALE (prior) = $145 k
ALE (post) = $65 k
ACS = $24 k

NRRB = ALE (prior) – ALE (post) – ACS =
= $145 k - $65 k - $24 k =
= $56 k, so there are + cost benefits of this solution

You are not required to study the remaining slides!

They are provided only for your reference!

Risk Analysis (cont.)

- **Qualitative Risk Analysis** – scenario based approach - uses labels & relative values (high/low) rather than numbers; blends in experience & personal judgment

- **Quantitative Risk Analysis** – predicts level of monetary loss for each threat, and monetary benefit of controlling the treat

  - each element is quantified and entered into equations, e.g.:
    - asset value
    - threat frequency
    - severity of vulnerability
    - damage impact
    - safeguard cost …

Risk Analysis (cont.)

	Qualitative Analysis	Quantitative Analysis
pros	• Requires simple (if any) calculations. • Considers hands-on opinions of individuals who know the process best.	• Easier to automate and evaluate. • Very useful in performance tracking - provide credible **cost/benefit analysis.**
cons	• Assessment and results are subjective. • Does not enable dollar cost/benefit discussion. • Difficult to track performance.	• Very detailed information about environment need to be gathered. • Complex calculations – may not be understood by all.