EECS 3482

Introduction to Computer Security

Security
Risk Management

Instructor: N. Vlajic, Fall 2021

Required Reading

Computer Security, Stallings: **Section 14.3 & 14.4**

Learning Objectives

Upon completion of this material, you should be able to:

- Define risk management and its role in an organization.
- Use risk management techniques to identify and prioritize risk factors for information assets.
- Asses risk based on the likelihood of adverse events and the effect on information assets when events occur.
- Document the results of risk identification.
- Detail risk treatment alternatives.

True Story

Company had set its offices in a place without sufficient 'physical security' !

A company suffered a catastrophic loss one night when its office burned to the ground.

As the employees gathered around the charred remains the next morning, the **president asked the secretary if she had been performing the daily computer backups.** To his relief **she replied that yes**, each day before she went home she backed up all of the financial information, invoices, orders ...

The president then asked the secretary to retrieve the backup so they could begin to determine their current financial status.

"**Well**", the secretary said, "**I guess I cannot do that. You see, I put those backups in the desk drawer next to the computer in the office.**"

M. Ciampa, "Security+ Guide to Network Sec. Fundamentals", 3rd Edition, pp. 303

Introduction

"Investing in stocks carries a risk …"

"**Bad hand hygiene (not washing hands) carries a risk …"**

"*Car speeding carries a risk …"*

"An outdate (not updated) anti-virus software carries a risk …"

Definition of Risk

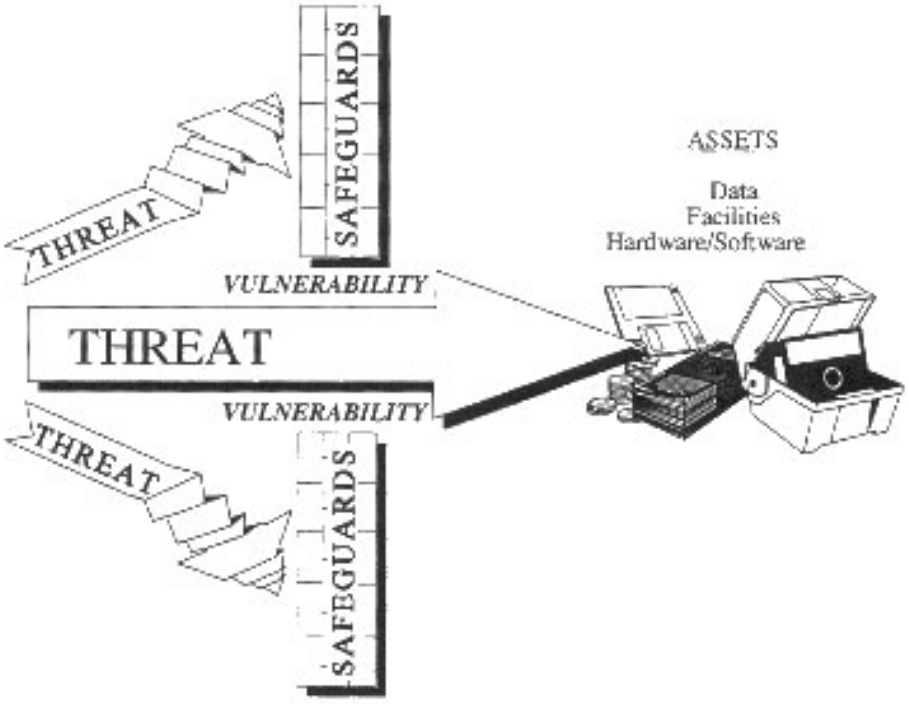
- **Risk** – **likelihood that a chosen action or activity** (including the choice of inaction) **will lead to a loss** (un undesired outcome)

- **Risk Management** – **identification, assessment, and prioritization of risks followed by coordinated use of resources to monitor, control or minimize the impact of risk-related events** or to maximize the gains.
  - examples: finances, industrial processes, public health and safety, insurance, etc.
  - one of the key responsibilities of every manager within an organization

http://en.wikipedia.org/wiki/Risk_management

Risk in Information Security

- **Risks in Info. Security** – risks which arise from an organization's use of info. technology (IT)
  - related concepts: asset, vulnerability, threat



http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter7.html

Risk in Information Security (cont.)

- **Asset** – anything that needs to be protected because it has value and/or contributes to the successful achievement of the organization's objectives

e.g., documents stored on a server

- **Threat** – any circumstance or event with the potential to cause harm to an asset and/or result in harm to organization

e.g., unauthorized person (e.g., bad actor) logging onto the server

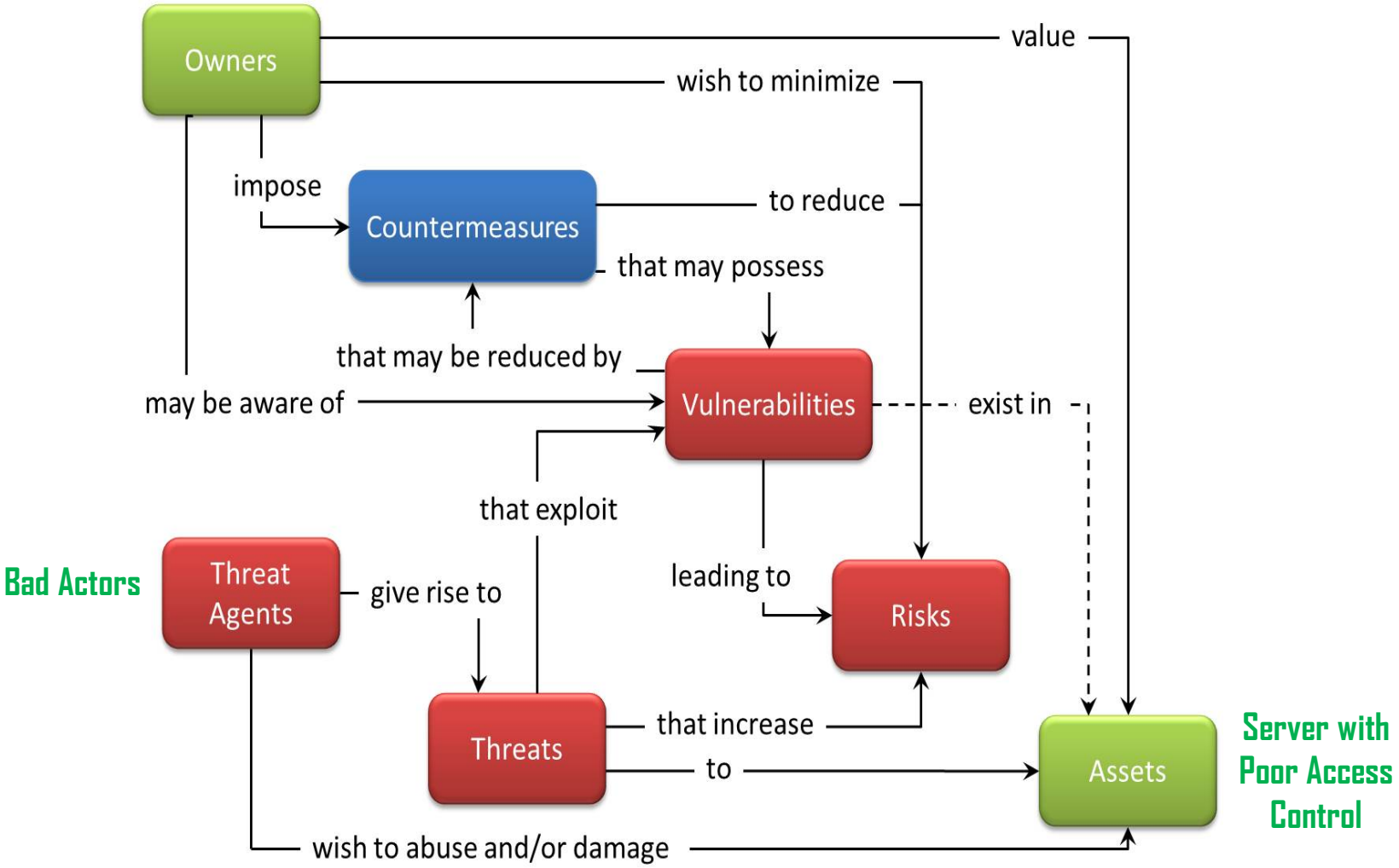
- **Vulnerability** – a weakness in an asset that can be exploited by threat and cause harm the asset and/or the organization

e.g., poor access control on the server

- **Risk** – probability of a threat acting upon a vulnerability causing harm to an asset

Risk in Information Security (cont.)

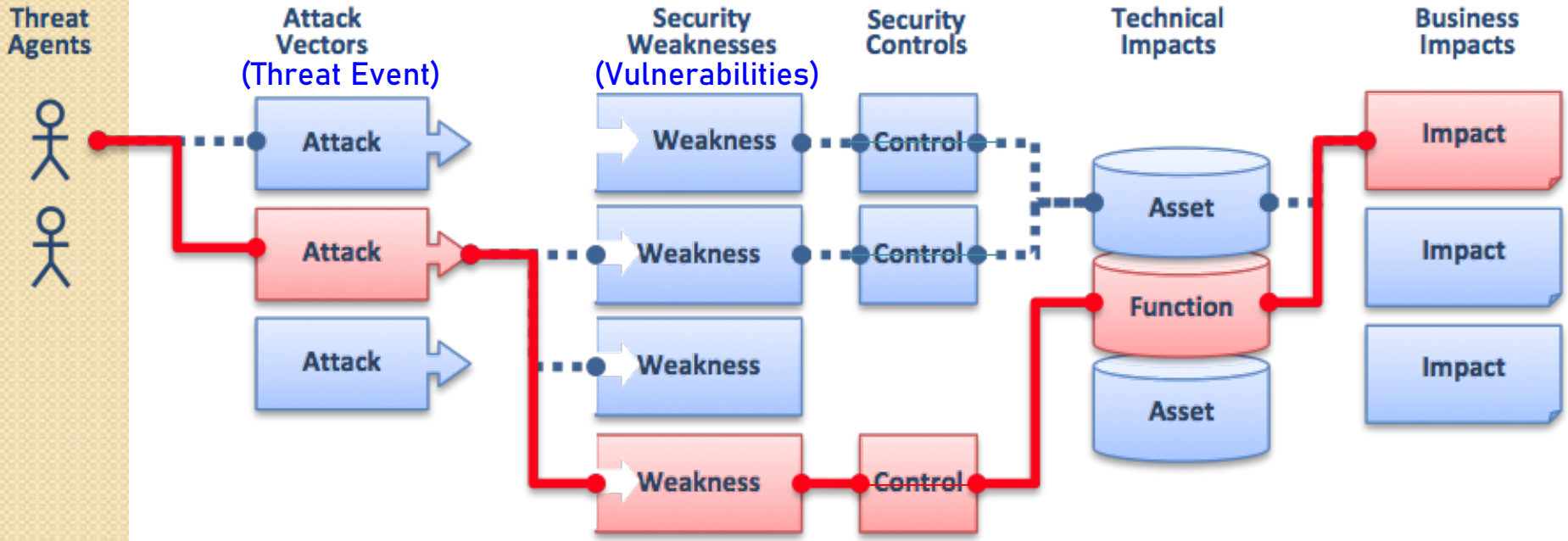
- **Interplay between Risk & other Info. Sec. Concepts**
  http://blog.patriot-tech.com/



Risk in Information Security (cont.)

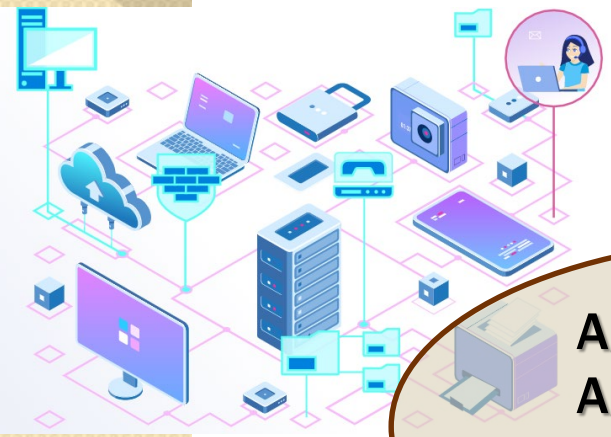
- **Asset, Threat, Vulnerability & Risk in Info. Sec.**

  http://en.wikipedia.org/wiki/File:2010-T10-ArchitectureDiagram.png



Risk in Information Security (cont.)

- **Key Risk-Related Question: Which vulnerabilities, in which assets, should we worry about (i.e., remove)?**



threat agents:
- cyber criminals
- foreign governments, …

Asset
vulnerability 1
vulnerability 2
…
vulnerability n

server vulnerab.:
- malware infection
- unauthorized access
- DDoS attack, …

malware infect. exploit.:
- through open net. ports/services
- through a USB port, …

Agent 1
Agent 2
…
Agent m

Threat (Risk)

Threat Event 1
Threat Event 2
…
Threat Event k

each company has many assets …
each asset may have many vulnerabilities …
each vulnerability may be associated with multiple threats …
each threat could be exploited by various agents …

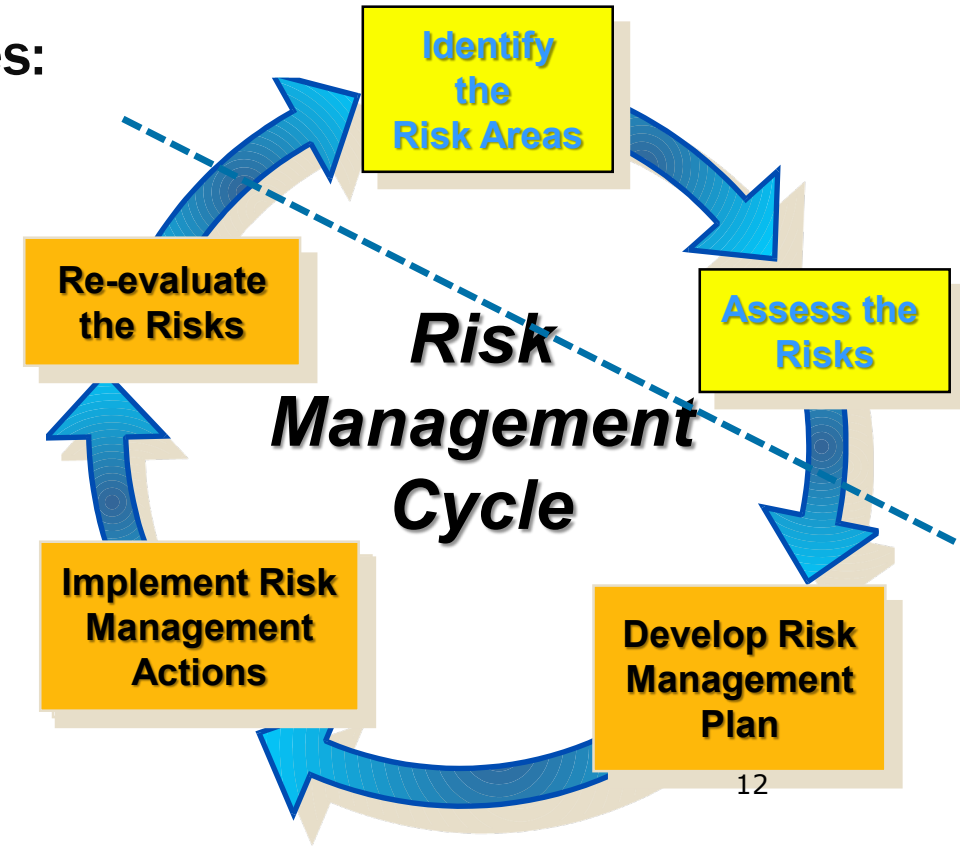
Where do we start dealing with Info. Sec. Risk ?!

Security Risk Management

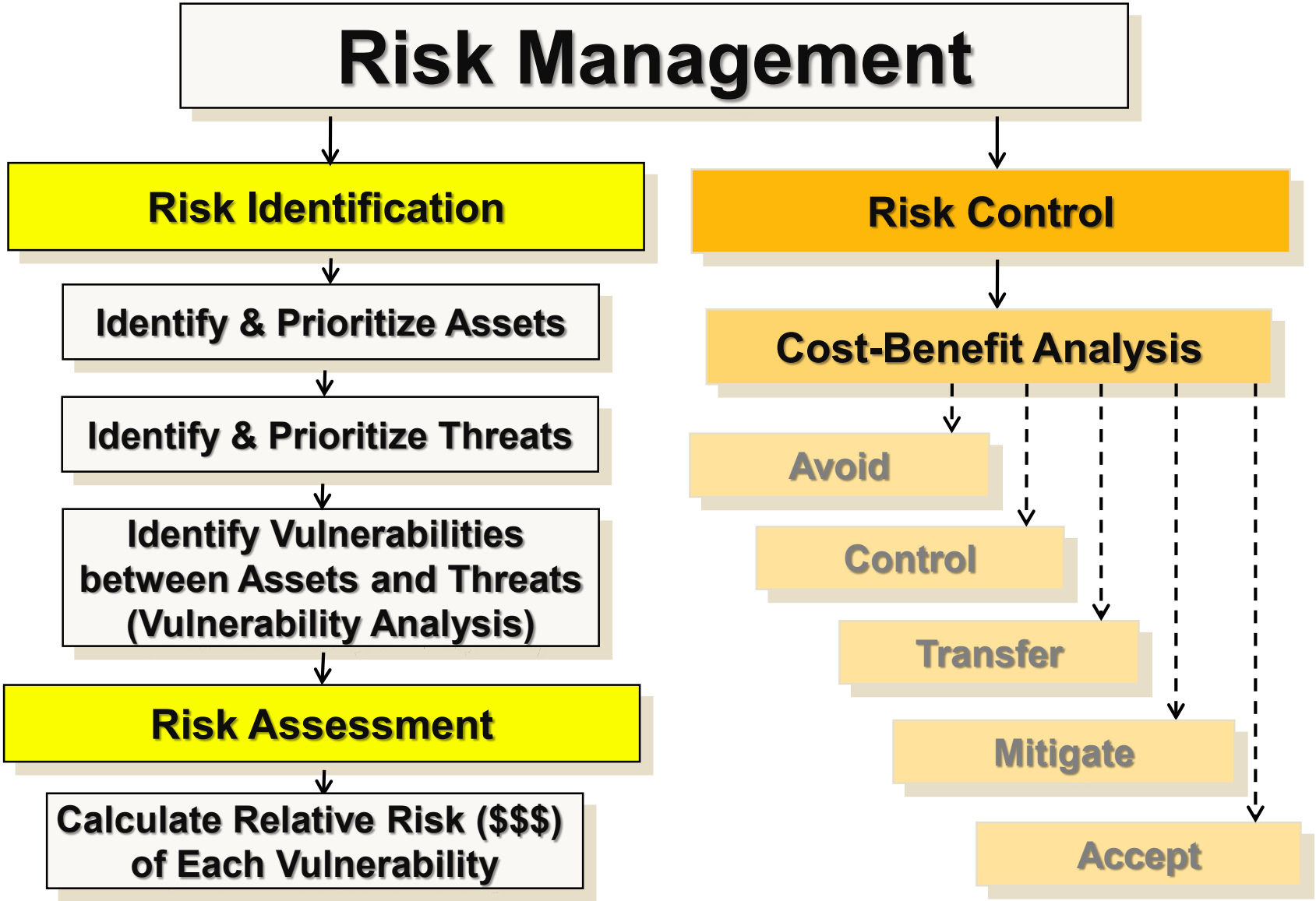
- **Security Risk Management** – process of identifying vulnerabilities in an organization's info. system and taking steps to protect the CIA of all of its components.
  - two major sub-processes:

Risk Identification & Assessment

Risk Control (Mitigation)

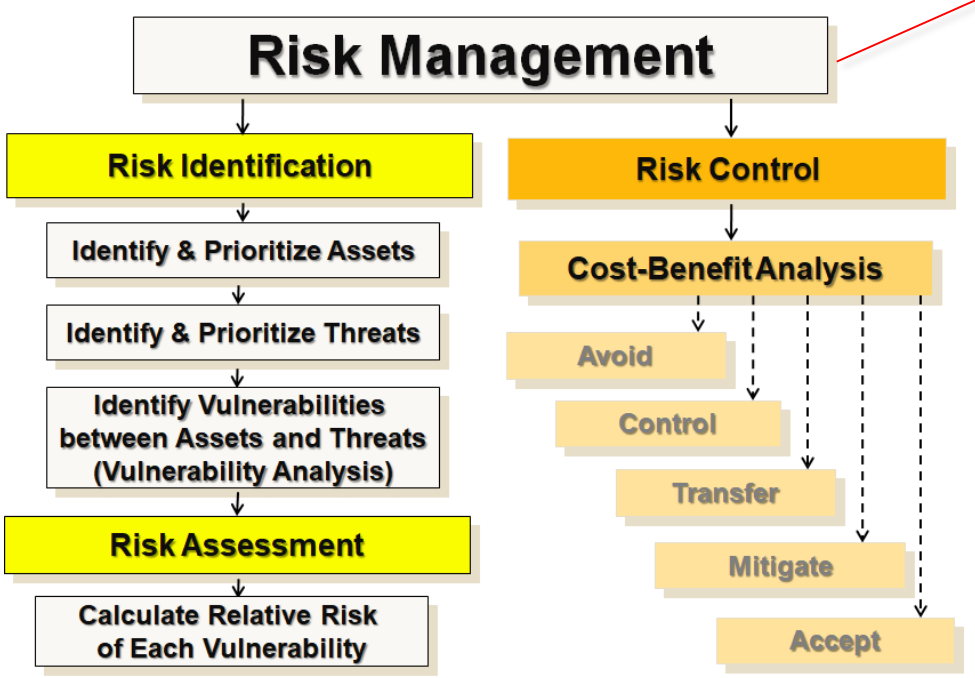


Security Risk Management (cont.)



Many organizations have 1000s of potentially vulnerable components in their IT/computer system.

Most companies, also, have limited time and budgets …

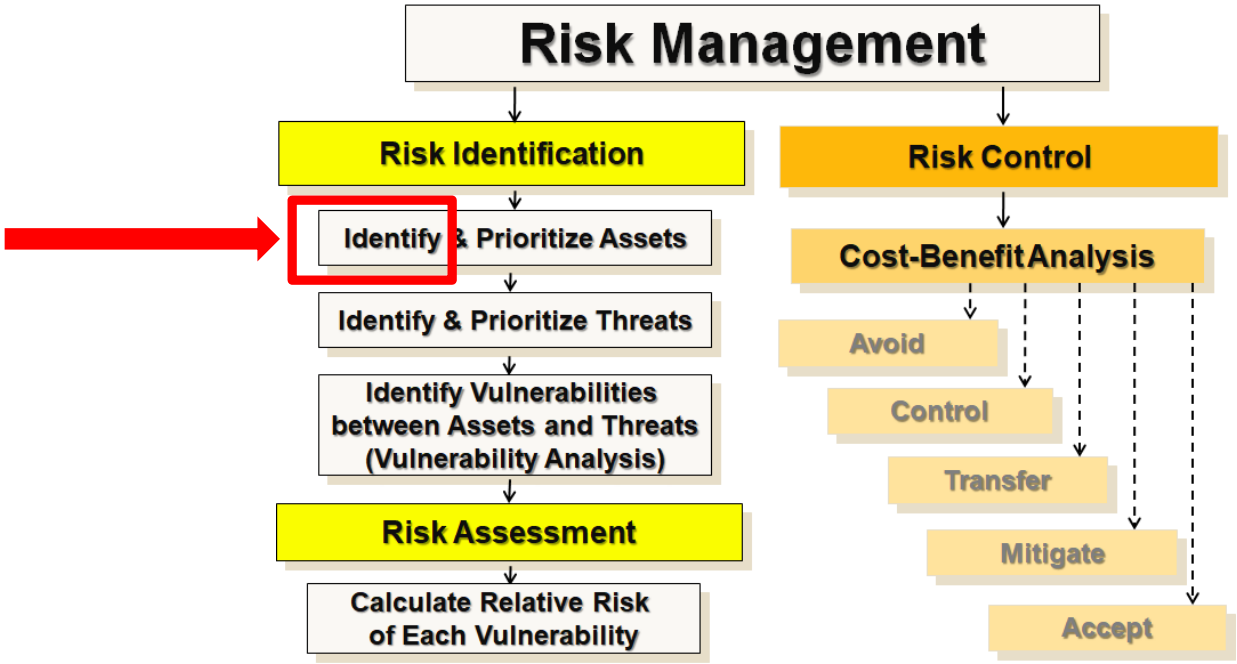


What exactly, from which danger, and how should we protect in our computer system in order to avoid $$$ losses.

Risk Identification

Risk Identification:

Asset Inventory



Risk Identification: Asset Inventory

What are 'information assets' for/in a company ??

Any entity that produces profit, BUT also
any entity whose failure (to properly operate)
may end up causing losses for the company !!

Example: Server vs. Router in e-Commerce company

Risk Identification: Asset Inventory

- **Risk identification begins with identification of all information assets, including:**

Traditional System Components	SesSDLC Components	Risk Management System Component
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

1) What to do with customer emails and orders?

2) Backup procedure.

- No prejudging of asset values should be done at this stage – values are assigned later!

Risk Identification: Asset Inventory (cont.)

- **Identifying Hardware, Software (& Networking Assets)**
  - Can be done automatically (using specialized software) or manually.
  - Needs certain planning – e.g. which attributes of each asset should be tracked, such as:
    - **name** – tip: naming should not convey critical info to potential attackers
    - **asset tag** – unique number assigned during acquisition process
    - **IP address**
    - **MAC address**
    - **software version**
    - **serial number**
    - **manufacturer name**
    - **manufacturer model or part number**

Risk Identification: Asset Inventory (cont.)

Example: Network Asset Tracker

NETWORK INVENTORY SOFTWARE

Quick and simple network inventory with Network Asset Tracker Pro. Our software enables you to collect hardware and software inventory data from remote computers with variety of audit methods like agentless and agent-based methods.

http://www.misutilities.com/

Risk Identification: Asset Inventory (cont.)

- **Identifying People, Procedures and Data Assets**
  - Not as readily identifiable as other assets – require that experience and judgment be used.
  - Possible attributes:
    - **people** – avoid personal names, as they may change, use:
      - position name
      - position number/ID
      - computer/network access privileges
    - **procedures**
      - description
      - intended purpose
      - software/hardware/networking elements to which it is tied
      - location of reference-document, …
    - **data**
      - owner
      - creator
      - manager
      - location, …

Risk Identification:

Asset Ranking/Prioritization

Risk Identification: Asset Ranking

- **Assets should be ranked so that most valuable assets get highest priority when managing risks.**
  - **Questions to consider when determining asset value/rank:**
    1) **Which info. asset is most critical for the overall operation and success of organization?**

Example: Amazon's ranking assets

Amazon's network consists of regular desktops and web servers.

Web servers that advertise company's products and receive orders 24/7 - critical.

Desktops used by customer service department – not so critical.

Risk Identification: Asset Ranking (cont.)

2) Which info. asset generates most revenue?

3) Which info. asset generates highest profit?

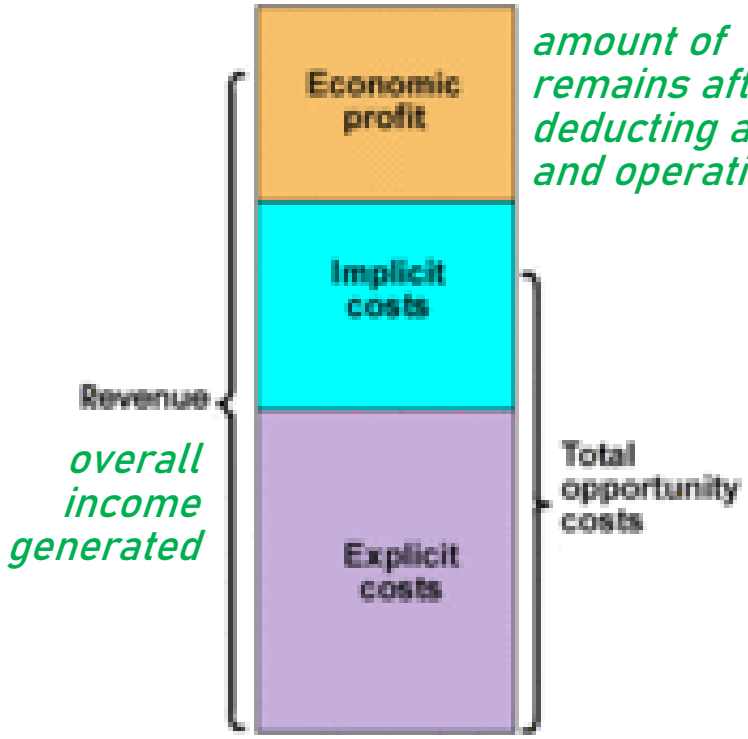
Example: Ranking assets in an 'online store' (e.g., Amazon)

Some servers may support book sales (resulting in highest revenue), while others may support sales of beauty products (resulting in highest profit).

4) Which info. asset is most expensive to replace?

5) Which info. asset's loss or compromise would be most embarrassing or cause greatest liability?

Risk Identification: Asset Ranking (cont.)



amount of income that remains after deducting all expenses and operational costs

overall income generated

Four-Way Fight

Latest performance of these four tech giants and plans for the future.

	APPLE	amazon.com	Google	FACEBOOK
Last quarterly revenue	$36 billion	$13.8 billion	$14.0 billion	$1.26 billion
Last quarterly profit/loss	$8.2 billion	-$274 million	$2.2 billion	-$59 million

Risk Identification: Asset Ranking (cont.)

Example: Weighted asset ranking (NIST SP 800-30)

Not all asset ranking questions/categories may be equally important to the company.
A weighting scheme could be used to account for this …

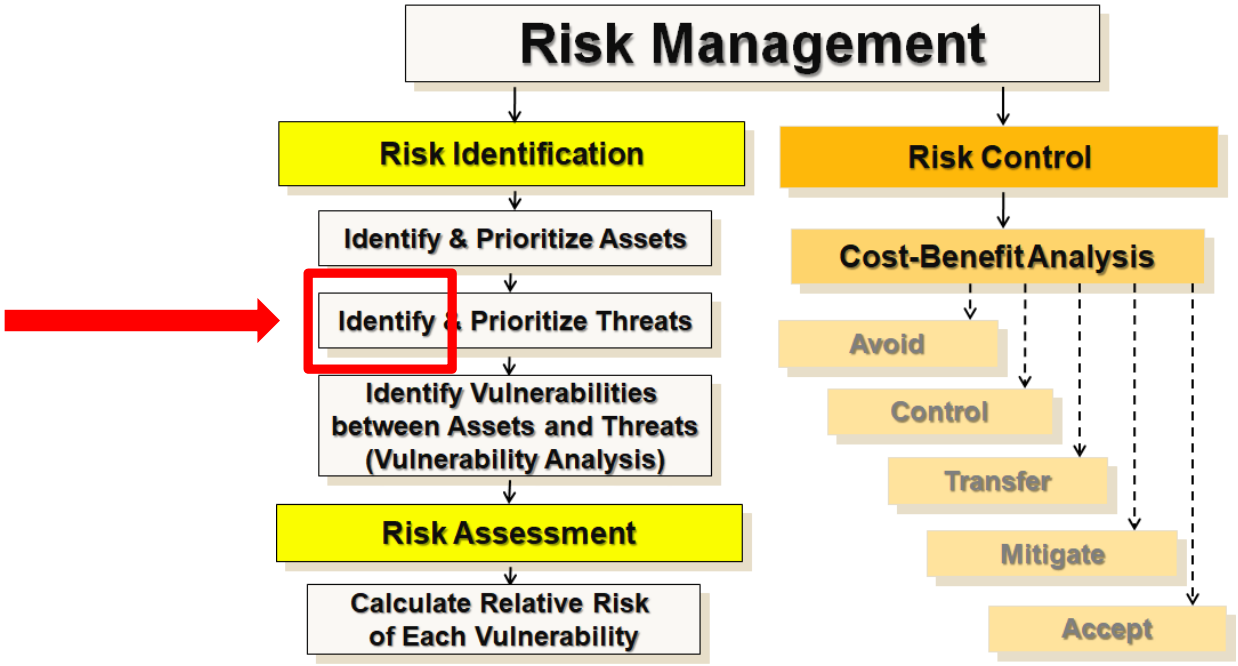
Each criteria is assigned a weight (0 – 100), must total 100!

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

Data asset / information transmitted:

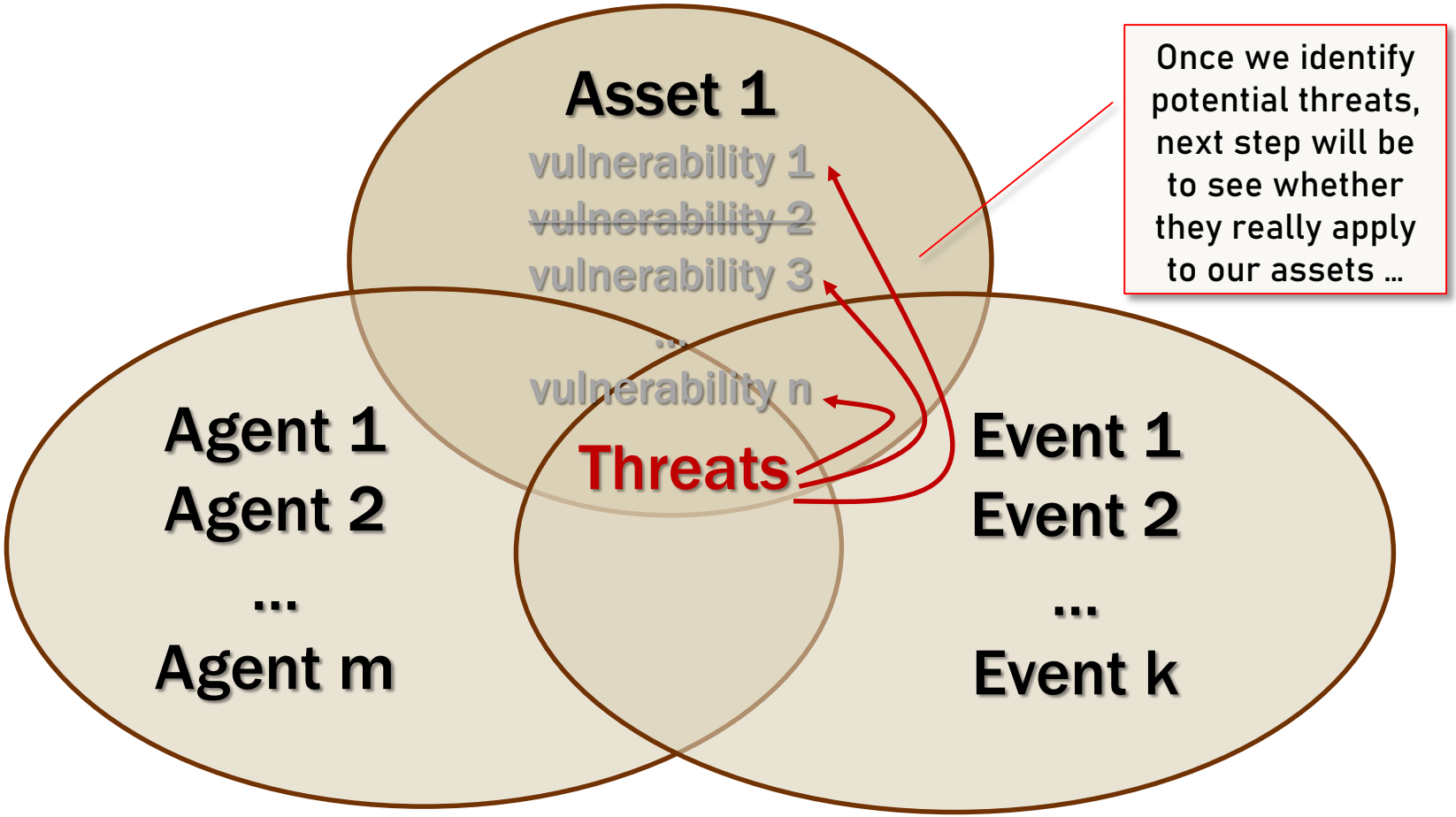
Each asset is assigned a score (0.0 -1.0) for each critical factor.

Threat Identification & Prioritization



Risk Identification: Threat Identification

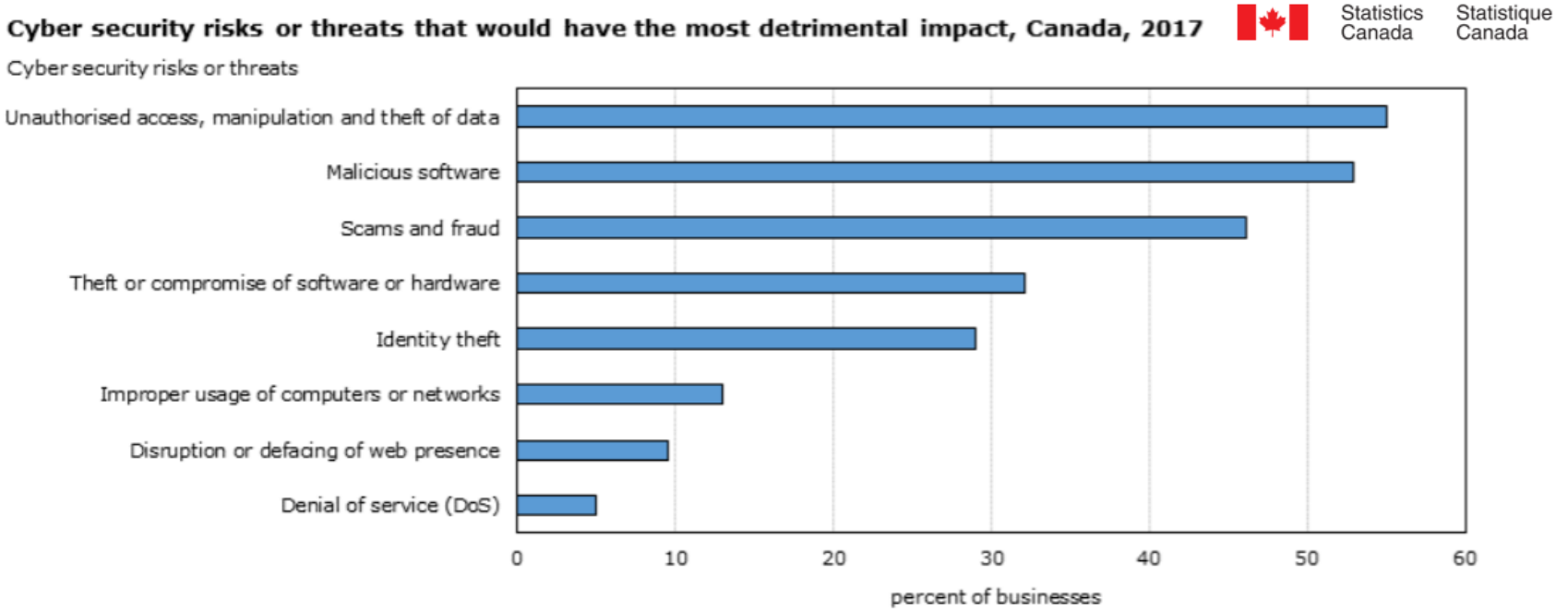
- Now that assets are known, we should see if there are any known potential threats/dangers for our company that exist out there ...



Risk Identification: Threat Identification

- **Any organization faces a wide variety of threats.**
- **To keep risk management 'manageable' …**
  - realistic threats must be identified and further investigated, while unimportant threats should be set aside

Example: government surveys of types of threats/attacks



ENISA Threat Landscape
15 Top Threats in 2020

EUROPEAN UNION AGENCY FOR CYBERSECURITY

The 9 top threats

During the reporting period (April 2020 to July 2021), the prime threats identified include:

1. Ransomware;
2. Malware;
3. Cryptojacking;
4. E-mail related threats;
5. Threats against data;
6. Threats against availability and integrity;
7. Disinformation – misinformation;
8. Non-malicious threats;
9. Supply-chain attacks

www.enisa.europa.eu
For more information: https://www.enisa.europa.eu/topics/etl

https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

Risk Identification: Threat Identification

Example: reports published by computer security companies

2019 Internet Security Threat Report by Symantec

Top 10 biggest cyber threats to organizations
1. Phishing (22%)
2. Malware (20%)
3. Cyberattacks (to disrupt) (13%)
4. Cyberattacks (to steal money) (12%)
5. Fraud (10%)
6. Cyberattacks (to steal IP) (8%)
7. Spam (6%)
8. Internal attacks (5%)
9. Natural disasters (2%)
10. Espionage (2%)

Risk Identification: Threat Identification

From January 2019 to April 2020

Sectoral/ thematic threat analysis

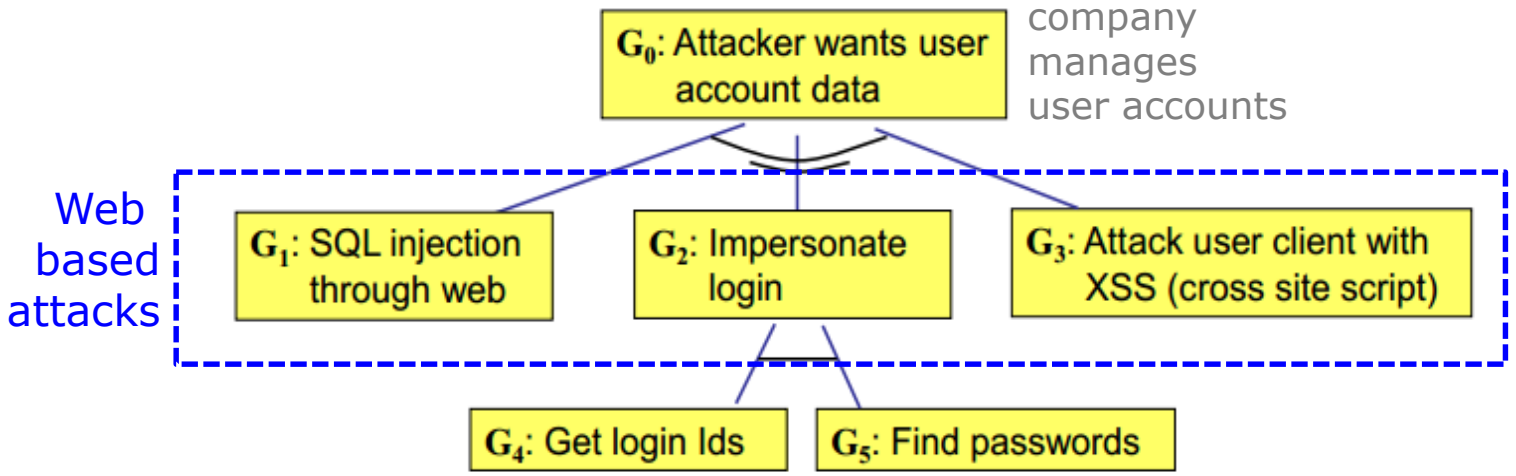
Example: threats/attacks by sector

SECTOR	MOST POPULAR THREATS/ATTACKS	INCIDENTS TRENDS
Individual		
Multiple indu		
Public Administrati Defence, Soc Services		
Financial/Ba Insurance		
Health/Medi		
Education	• Malware • Ransomware • Web based attacks	Stable slightly decreasing
Information and Communication	• Web application attacks • Insider threat (unintentional abuse/error) • Malware	Stable
Professional/Digital Services	• Web application attack • Insider threat (unintentional abuse/error) • Malware	Stable
Arts, Entertainment and gaming[8]	• Web application attacks • Malware • Phishing	Stable
Manufacturing	• Malware • Web application attacks • Insider threat (unintentional abuse/error)	Stable

Risk Identification: Threat Identification (cont.)

- **Threat Modeling/Assessment** – **practice of building an abstract model of how an attack may proceed and cause damage** [attacker-, system-, or asset- centric]

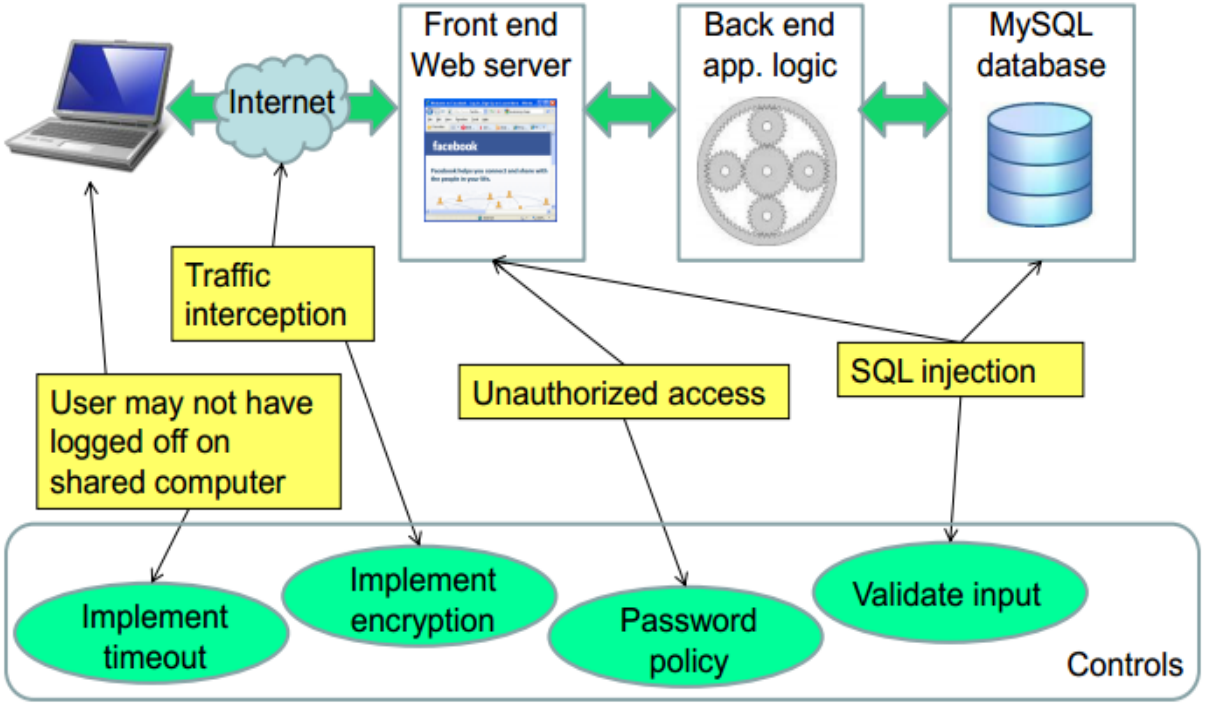
  - **Attacker-centric** – starts from attackers, evaluates their motivations and goals, and how they might achieve them through attack tree.



http://www.uio.no/studier/emner/matnat/ifi/INF3510/v12/learningdocs/INF3510-2012-L03.pdf

Risk Identification: Threat Identification (cont.)

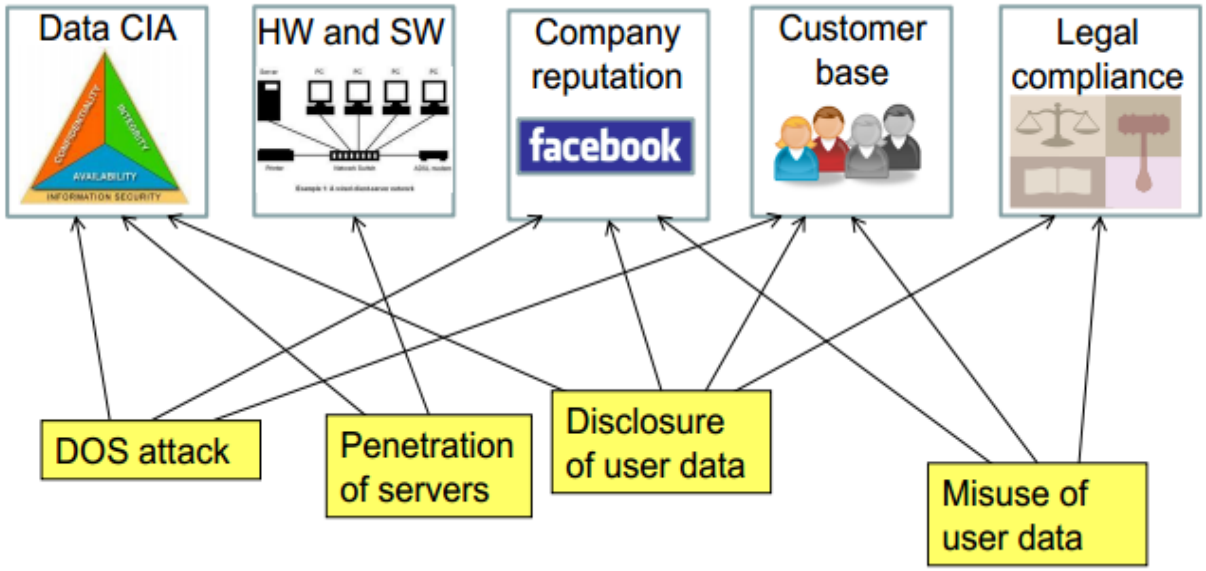
- Threat Modeling/Assessment
  - **System-centric** – starts from model of system, and attempts to follow model dynamics and logic, looking for types of attacks against each element of the model.



http://www.uio.no/studier/emner/matnat/ifi/INF3510/v12/learningdocs/INF3510-2012-L03.pdf

Risk Identification: Threat Identification (cont.)

- Threat Modeling/Assessment
  - **Asset-centric** – starts from assets entrusted to a system, such as a collection of sensitive personal information, and attempts to identify how CIA security breaches can happen.



http://www.uio.no/studier/emner/matnat/ifi/INF3510/v12/learningdocs/INF3510-2012-L03.pdf

Threat Identification & Prioritization

Risk Identification: Threat Prioritization

- **Questions used to prioritize threats:**
  - **Which threats present a realistic danger to organization's assets in its current environment?** (**'pre-step'**)
    - **Goal:** reduce the risk management's scope and cost.
    - Examine each category from CSI/FBI list, or as identified through threat assessment process, and eliminate any that do not apply to your organization.
  - **Which threats represent the most severe danger … ?**
    - **Goal:** provide a rough assessment of each threat's potential impact given current level of organization's preparedness.
    - **'Danger' might be a measured of:**
      1) **probability** that the threat attacks organization
      2) **severity**, i.e. overall damage that the threat could create

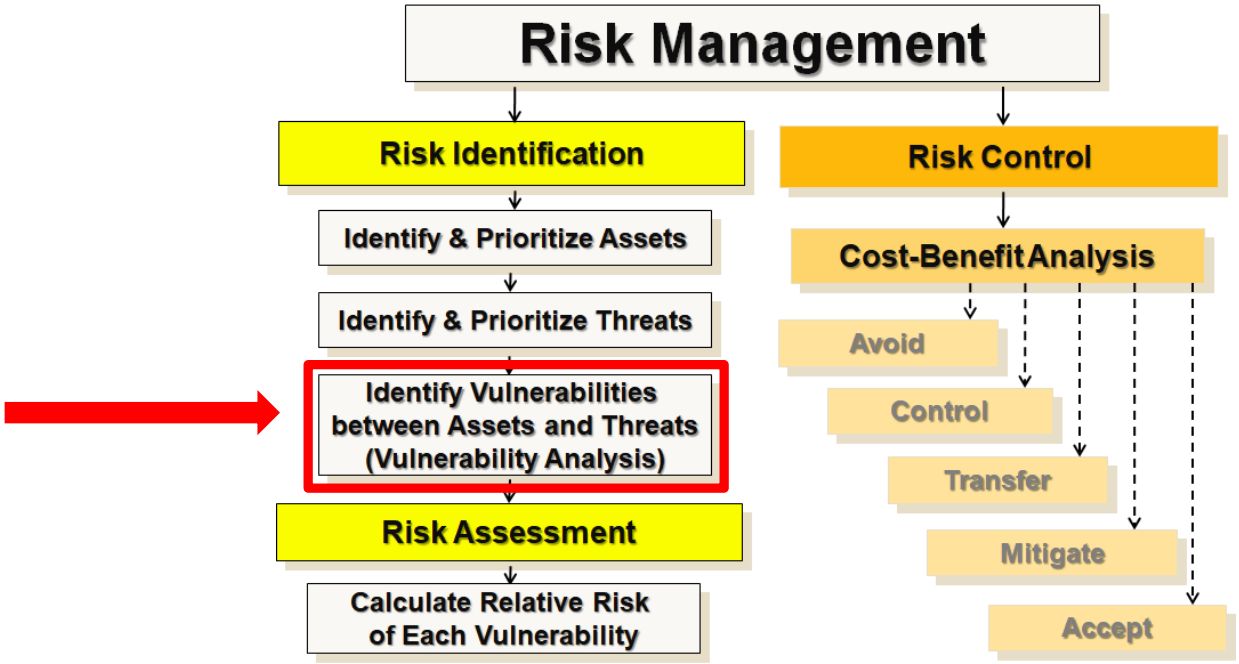
Risk Identification: Threat Prioritization (cont.)

- **Other questions used to assess/prioritize threats:**
  - **How much would it cost to recover from a successful attack?**
  - **Which threats would require greatest expenditure to prevent?**

- **Threat ranking can be quantitative or qualitative.**

- **Once threats are prioritized, each asset should be reviewed against each threat to create a specific list of vulnerabilities.**

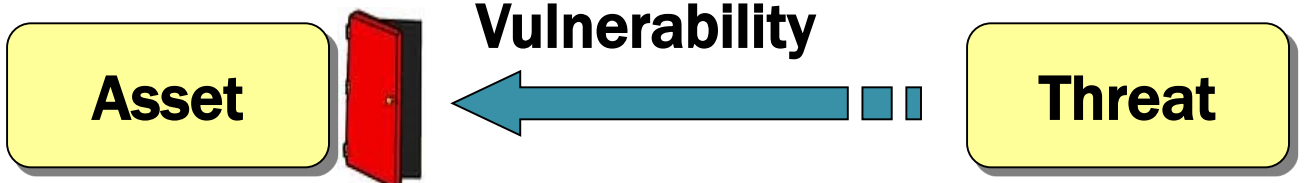
Risk Identification:
Vulnerability Analysis



Vulnerability Analysis

- **Vulnerability** – flaw or weakness in an info. asset, its design, implementation or security procedure that can be exploited accidentally or deliberately by a threat
  - a known threat is a real 'threat' to an organization only if there is an actual vulnerability it can exploit
  - sheer existence of a vulnerability does not mean harm WILL be caused – threat agent is required
  - vulnerability that is easy to exploit is often a high-danger vulnerability

Only component we can really do something about!

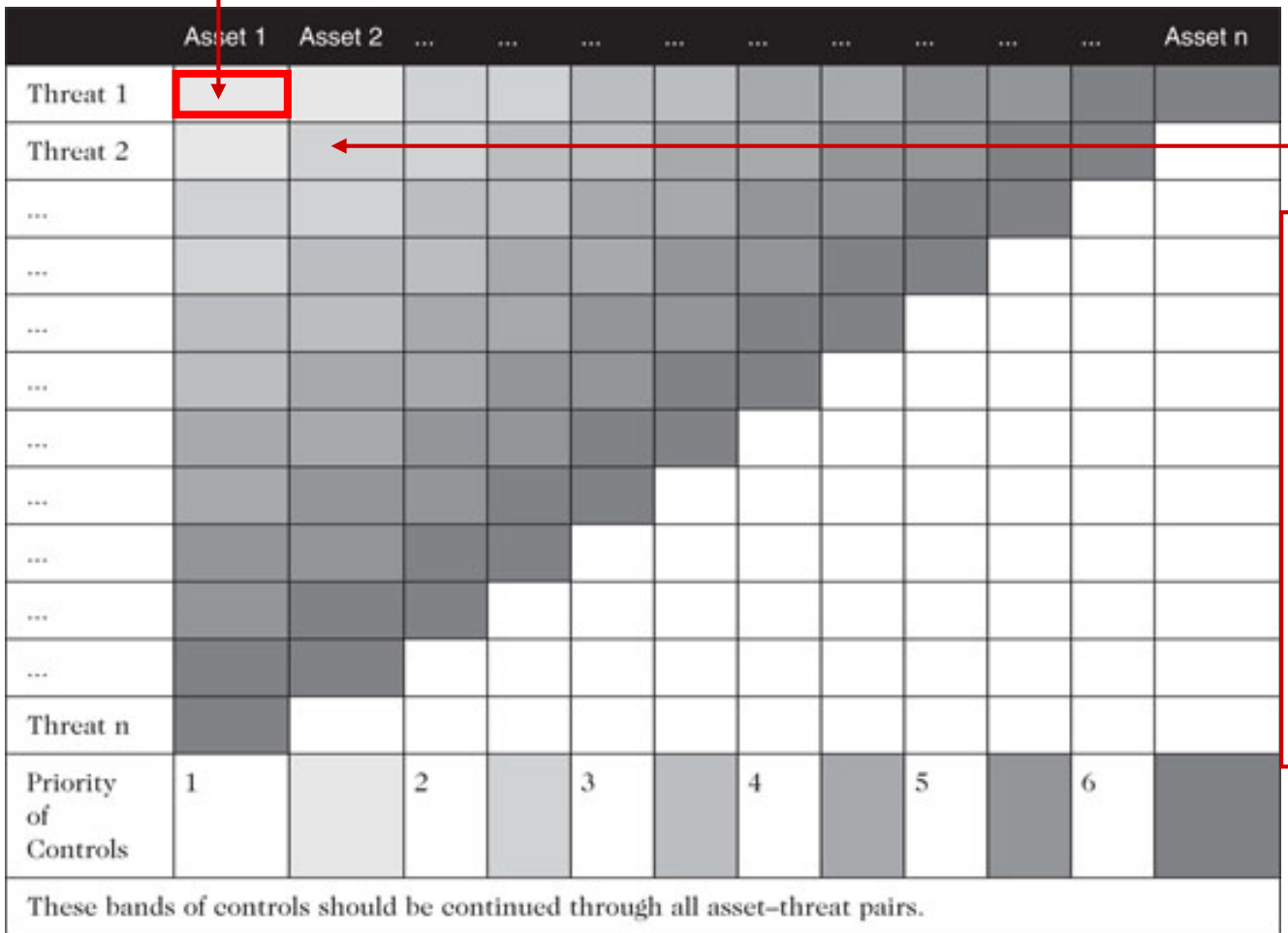


Vulnerability Analysis (cont.)

- **TVA Worksheet** – at the end of **risk identification** procedure, organization should derive **threats-vulnerabilities-assets (TVA)** worksheet
  - this worksheet is a starting point for risk assessment phase
  - TVA worksheet combines prioritized lists of assets and threats
    - prioritized list of assets is placed on x-axis, with most important assets on the left
    - prioritized list of threats is placed on y-axis, with most dangerous threats at the top
    - resulting grid enables a simplified priority-based vulnerability assessment

Vulnerability Analysis (cont.)

If multiple vulnerabilities exist between T1 & A1, they can be categorized:
T1V1A1 – Vulnerability 1 that exists between Threat 1 and Asset 1
T1V2A1 – Vulnerability 2 that exists between Threat 1 and Asset 1, …

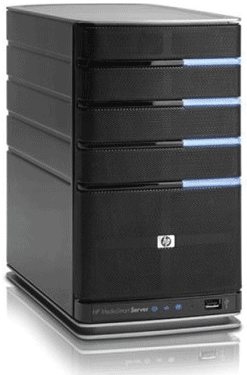


If intersection between T2 and A2 has no vulnerability, the risk assessment team simply crosses out that box.

Vulnerability Analysis (cont.)

design, implementation or security procedure

Example: Vulnerability assessment of critical files



desktop (files) on a particular computer/workstation

Asset

people open suspicious e-mail attachments and/or copy files off USBs

[procedural weakness]

certain services/ports left open

[design/implementation weakness]

Vulnerability

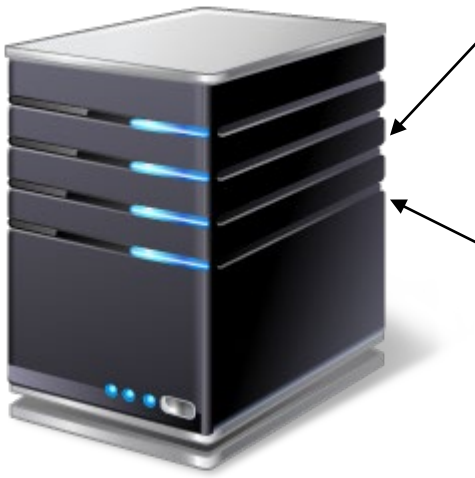
Deliberate Software Attack – Malware Attack (Virus or Worm)

Threat

Vulnerability Analysis (cont.)

design, implementation or security procedure

Example: Vulnerability assessment of critical files



Web Server

NIC can support data-rates of up to 50 Mbps

[design weakness]

CPU 'freezes' at 10,000 packets/sec

[design/implementation flaw]

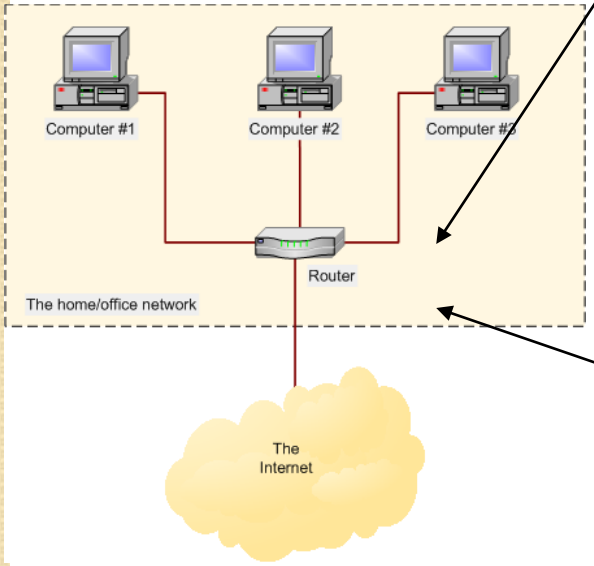
DDoS Attack

Asset | **Vulnerability** | **Threat**

Vulnerability Analysis (cont.)

design, implementation or security procedure

Example: Vulnerability assessment of a router



router

temperature control in router/server room is not adequate ⇒ router overheats and shuts downs

[design, implementation, procedural weakness]

net. administrator allows access to unauthor. user ⇒ unauthor. user uploads a virus, router crashes

[procedural weakness]

Act of Human Error or Failure

Asset | **Vulnerability** | **Threat**

Vulnerability Analysis (cont.)

Example: Vulnerability assessment of a DMZ router

Asset !!!

Threat	Possible Vulnerabilities
Acts of human error or failure	Employees or contractors may cause an outage if configuration errors are made
Compromises to intellectual property	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of espionage or trespass	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of information extortion	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate acts of sabotage or vandalism	IP is vulnerable to denial-of-service attacks Device may be subject to defacement or cache poisoning
Deliberate acts of theft	Router has little intrinsic value, but other assets protected by this device could be attacked if it is compromised
Deliberate software attacks	Internet Protocol (IP) is vulnerable to denial-of-service attack; Outsider IP fingerprinting activities can reveal sensitive information unless suitable controls are implemented
Forces of nature	All information assets in the organization are subject to forces of nature unless suitable controls are provided
Quality-of-service deviations from service providers	Unless suitable electrical power conditioning is provided, failure is probable over time
Technical hardware failures or errors	Hardware could fail and cause an outage Power system failures are always possible
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage
Technological obsolescence	If it is not reviewed and periodically updated, a device may fall too far behind its vendor support model to be kept in service

EECS 3482

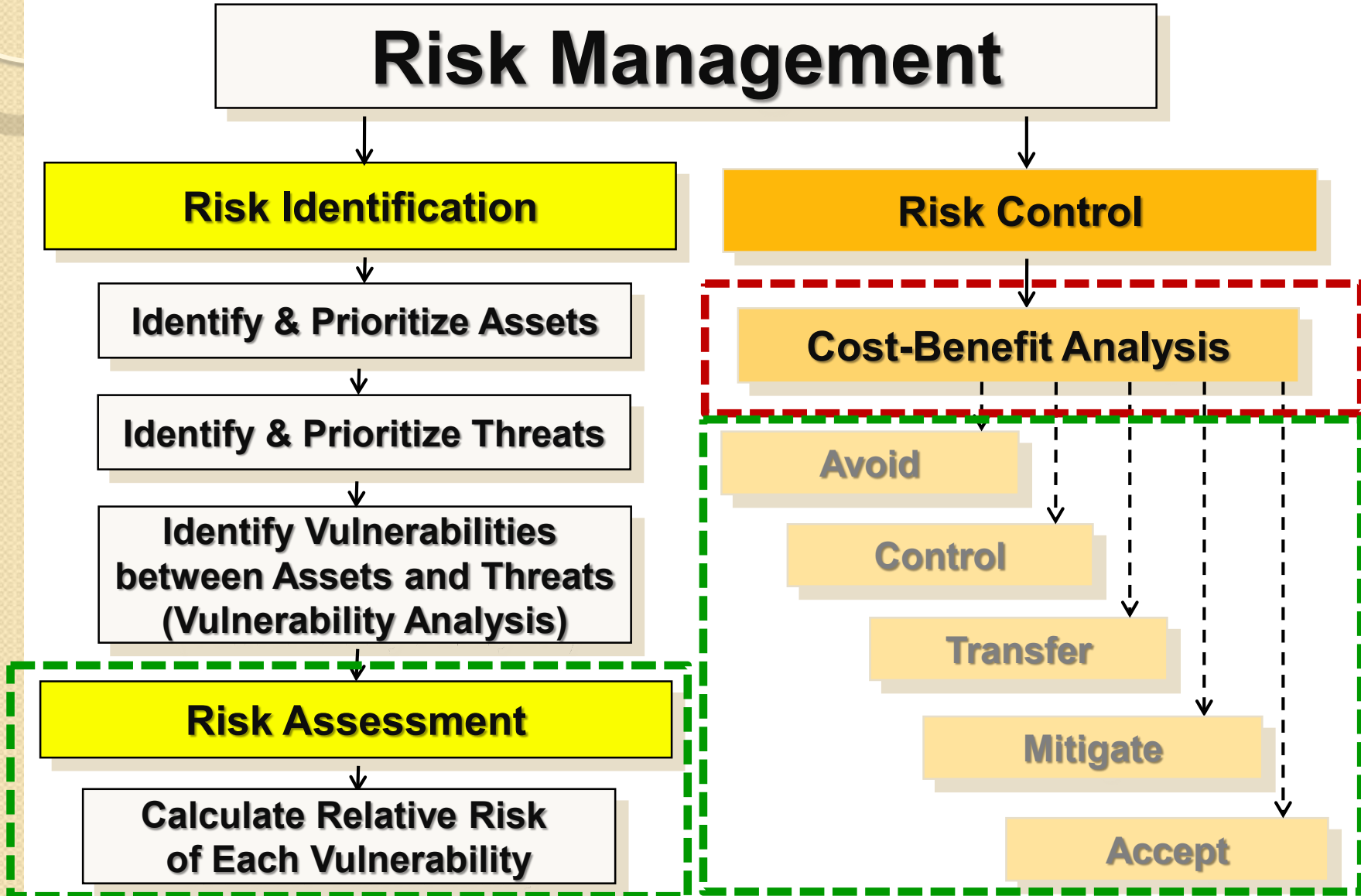
Introduction to Computer Security

Security Risk Management

Cost-Benefit Analysis

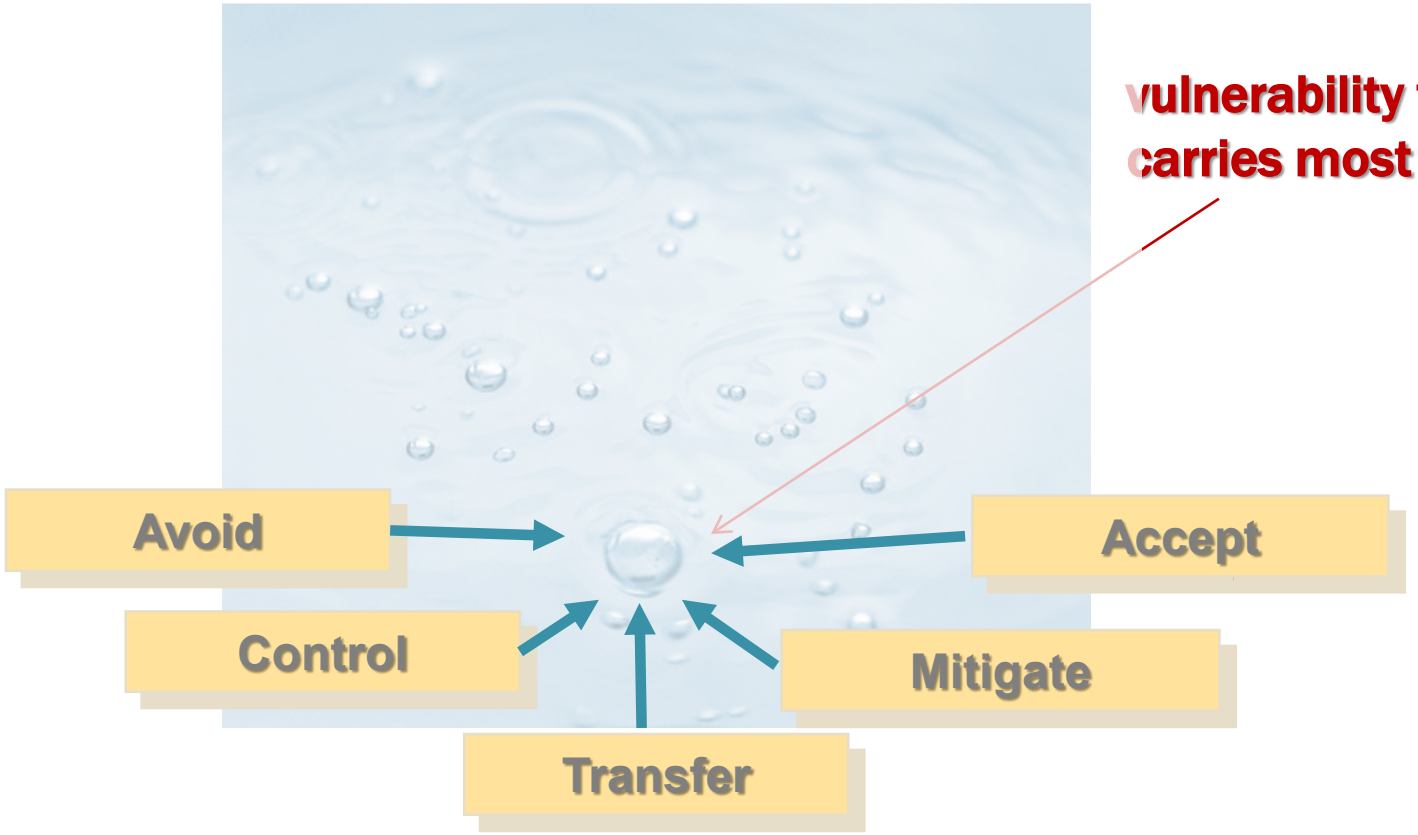
Instrutor: N. Vlajic, Fall 2021

Security Risk Management



Risk Analysis

Risk Assessment: 'Spotting' the most significant vulnerabilities in the sea of potential vulnerabilities.



Cost-Benefit Analysis: Is a sec. risk worth a sec. control?!

Risk Analysis (cont.)

risk ($) vs. cost ($)

https://nigesecurityguy.files.wordpress.com/2013/06/balancing-security.jpg

Quantitative Risk Analysis (cont.)

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

	A	B	C	D	E	F
1		Amount		Amount		Amount
2		$100.00		$0.00		$0.00
3		$100,000.00		$375.00		$375.00
4		$1.00		$694,390.00		$694,390.00
5		$1,000.00		$1,000.00		$1,000.00
6		$100.00		$10,133.00		$10,133.00
7		$100.00		$1,000,000.00		$1,000,000.00
8		$101,301.00		$1,705,898.00		$1,705,898.00

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

- **Challenges of Quantitative Analysis** – define likelihood & impact values in a manner that would allow the same scale to be used across multiple risk assessments

Quantitative Risk Analysis (cont.)

"**Quantitative risk analysis** is the standard way of measuring risk in many fields, such as finance and insurance, but it is not commonly used to measure risk in information systems.

Two of the reasons claimed for this are:

1) the difficulties in identifying and assigning a value to assets, and
2) **the lack of statistical information that would make it possible to determine frequency**.

Thus, many of the risk assessment tools that are used today for information systems are measurements of qualitative risk."

http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204

Qualitative Risk Analysis

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

Example: threat likelihood/frequency (i.e., vulnerability exploitation) categories

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may be deemed as "unlucky" or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Example: 'threat impact/consequences' categories

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify. Usually does not result in any tangible detriment to the organization.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources. Again, does not result in any tangible detriment to the organization, but may, in hindsight, show previous lost opportunities or lack of efficiency.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and will generally require management intervention, though should still be able to be dealt with at the project or team level. Will require some ongoing compliance costs to overcome. Customers or the public may be indirectly aware or have limited information about this event.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome. Senior management will be required to sustain ongoing direct management for the duration of the incident and compliance costs are expected to be substantial. Customers or the public will be aware of the occurrence of such an event and will be in possession of a range of important facts. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. A loss of customer business or other significant harm to the organization is expected. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action against personnel involved is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable. Compliance costs are likely to result in annual losses for some years, with liquidation of the organization likely.

DDoS attack on an E-commerce company

user/patient files erased due to virus infection

compromised user/patient records in a bank/hospital

Each threat/vulnerability gets a label in terms of its 'likelihood' and 'consequences', which determines its category and required action …

Example: 'risk determination' categories

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Qualitative 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 - enables credible **cost/benefit analysis**.
cons		

Quantitative Risk Analysis

- **Cost-Benefit Analysis** – aka **economic feasibility** study - quantitative decision-making process in which for each high-risk vulnerability:

  - determine the loss in value if the asset (with this vulnerability) remained unprotected
  - determine the cost(s) of protecting the asset using various approaches
  - compare available alternatives and arrive at a decision with best financial outcome …

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
  - as well as the 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

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 <u>$150,000 a year</u>?

Quantitative Risk Analysis (cont.)

- **Annualized Rate of Occurrence (ARO)** – indicates how often an attack is expected to successfully occur in a year (e.g., 2x a year => ARO=2)
  - if an attack occurs once every 2 years $\Rightarrow$ 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	~~Risk~~ Threat	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.

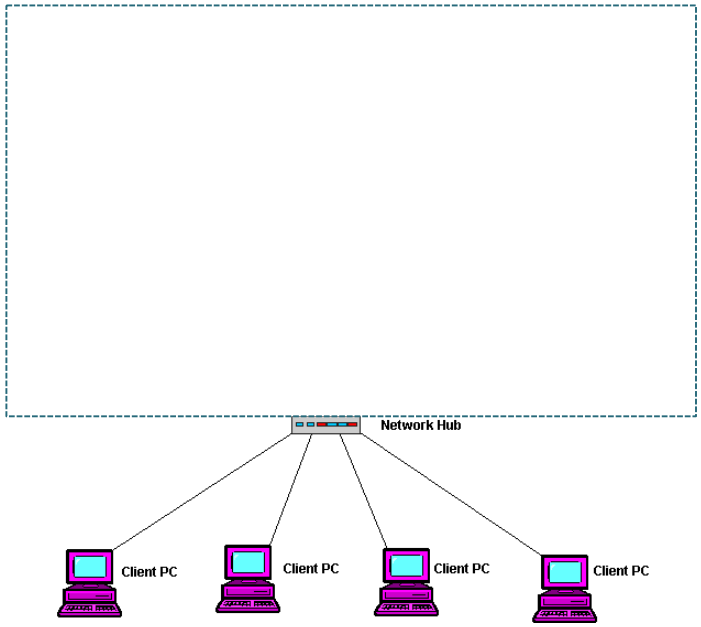
Previously, none of the workstations involved in the network had an anti-virus software installed on the machines. This was because there was no connection to the Internet and the workstations did not have USB/disk drives or Internet connectivity, so the risk of viruses was deemed minimal.

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.

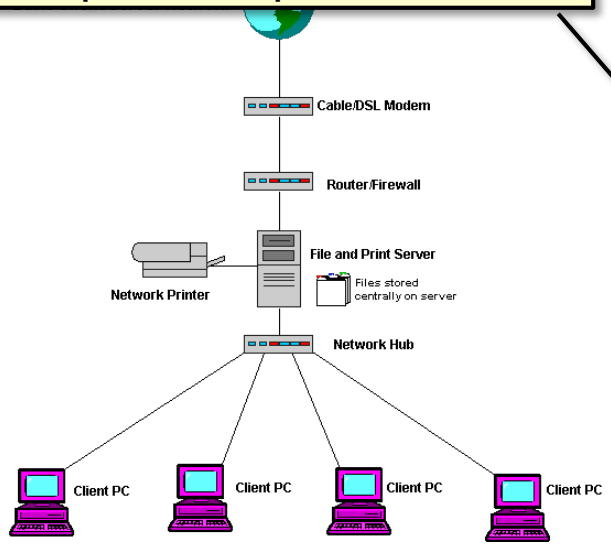
A vendor will sell licensed copies of antivirus for all servers and the 200 workstations at a cost of $4,700 per year.

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.)

Very simplistic scenario. Other losses could be: erased (IP) documents, lost emails, impact on reputation, etc.



Based on the provided data:

ARO = 0.75

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

ALE = ARO * SLE = **$ 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

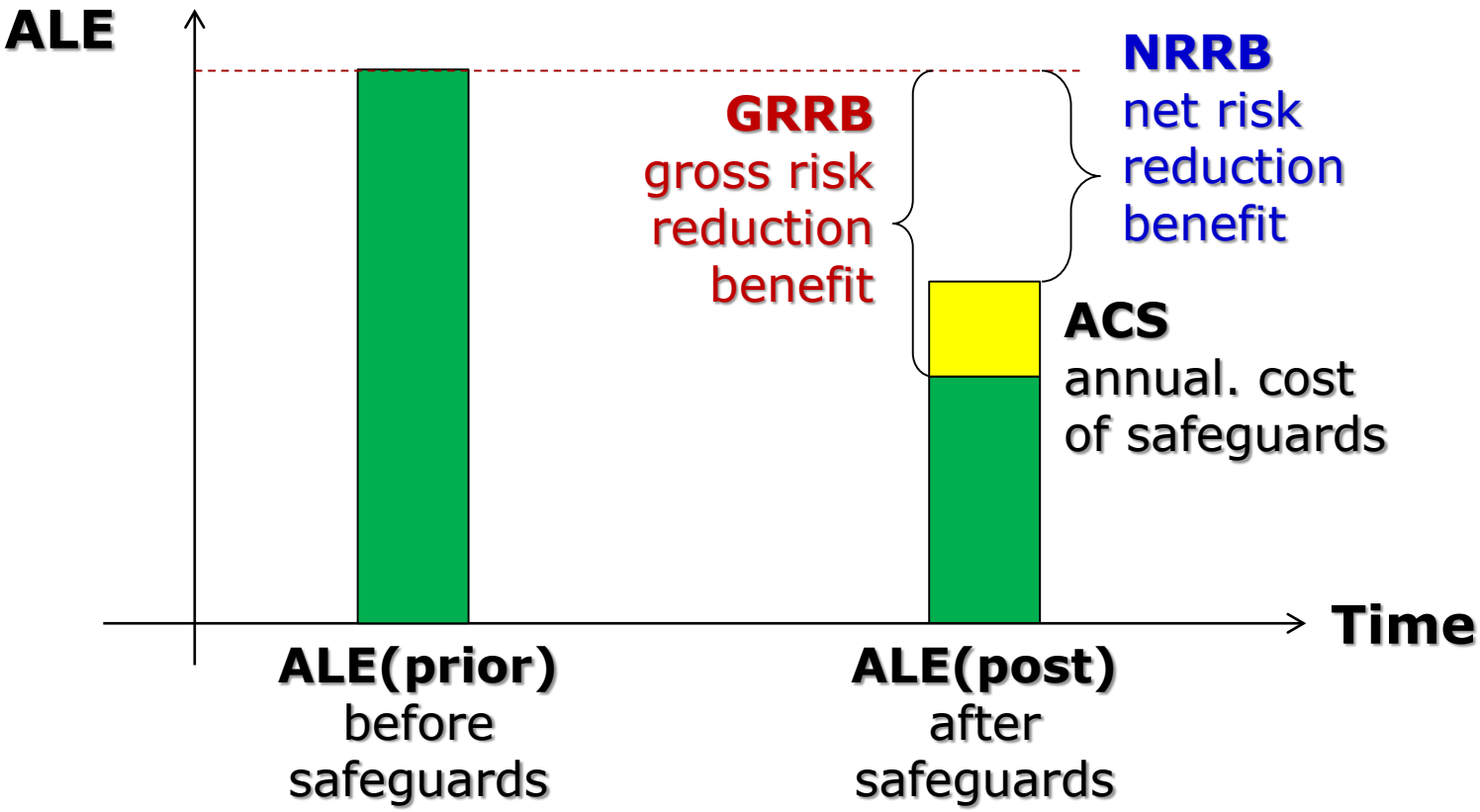
$$\mathbf{NRRB} = [\mathbf{ALE}(\text{prior}) - \mathbf{ALE}(\text{post})] - \mathbf{ACS}$$

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_{prior}) is $145,000. The cost of this anti-virus countermeasure Is estimated to $24,000/year, and it will lower the ALE_{post} 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

Quantitative Risk Analysis (cont.)

Example: Cert. Info. Sys. Sec. Prof. (CISSP) Exam

3. As an information systems security professional, what is the highest amount would you recommend to a corporation to invest annually on a countermeasure for protecting their assets valued at $1 million from a potential threat that has an annualized rate of occurrence (ARO) of once every five years and an exposure factor (EF) of 10% :

   A. $100,000.

   B. $20,000.

   C. $200,000.

   D. $40,000.

ALE (prior) = AV*EF*ARO = 10^6 *0.1*0.2 **= $20,000**

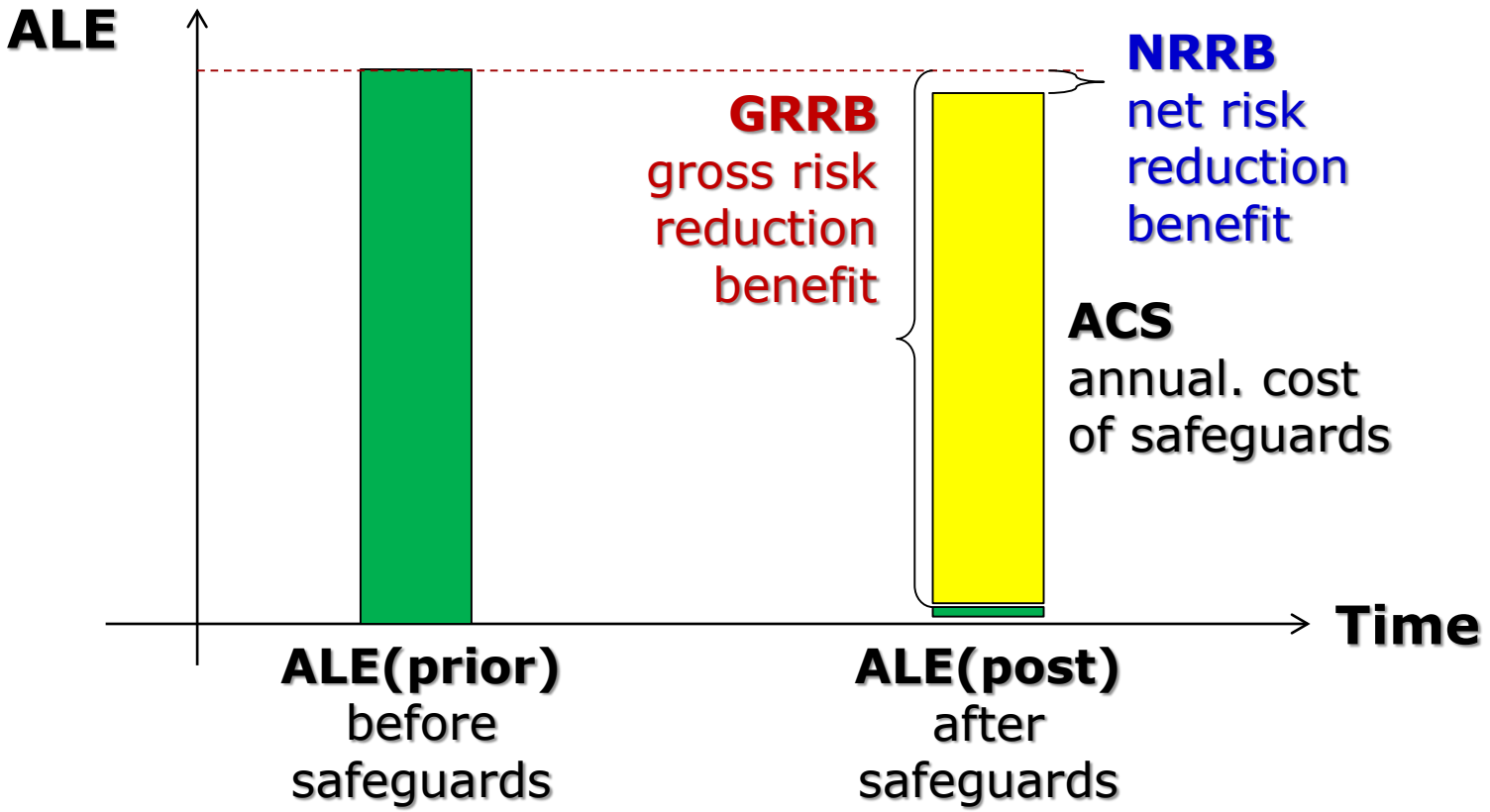
ALE (post) = $0 (best case scenario - safeguard 100% eff.)

ACS = ?

For NRRB ≥ 0, safeguard of up to $20,000 acceptable.

Quantitative Risk Analysis (cont.)

Example: Cost-benefit analysis in case of 100% effective safeguard



Other Feasibility Measures

- **Quantitative cost-benefit analysis determines whether a security control measure is feasible economically.**
- **Other factors and 'measures of feasibility', when evaluating a security control, should be considered:**

$$\mathbf{NRRB} = [\mathbf{ALE}(\text{prior}) - \mathbf{ALE}(\text{post})] - \mathbf{ACS}$$

$$= ARO_{post} * AV_{post} * EF_{post}$$

- **Organizational Feasibility** – **examines how well a proposed security control will contribute to organization's strategic objectives**
  - e.g. a firewall might be a good security safeguard, but may prevent effective flow of multimedia data

Other Feasibility Measures (cont.)

- **Behavioral Feasibility** – examines user's and management's acceptance and support of a proposed security control
  - e.g. if users do not accept a new policy/ technology/program, it will inevitably fail
  - most common methods for obtaining user acceptance are:
    - communication – affected parties must know the purpose and benefits of the proposed change
    - education – affected parties must be educated on how to work under the new constraints
    - involvement – affected parties must be given a chance to express what they want and what they will tolerate from the system

Other Feasibility Measures (cont.)

- **Technical Feasibility** – **determine whether organization has or can acquire technology and/or necessary technical expertise to implement and support a control**
  - e.g. use of VPN may require special software hardware support / installation on all computers
- **Political Feasibility** – **determines what can and cannot be done based on consensus and relationship between different departments …**
  - IT and Info. Sec. department might have to compete for same resources

Relative Risk Analysis

- **Rather than using quantitative or qualitative risk analysis an organization may resort to relative risk analysis of a control, including:**

- **Benchmarking** – **study practices used in other organizations that obtain results you would like to duplicate**

- **Due Care or Due Diligence** – **implement a minimum level of security**
  - failure to maintain a standard of due care can open an organization to legal liability – especially important if dealing with customer data

Relative Risk Analysis (cont.)

- **Best Practices** – implement entire set of security controls as recommended for your industry / general public
  - 'best practices' according to Microsoft:
    - use antivirus software
    - use strong passwords
    - verify your software security setting
    - update product security
    - build personal firewalls
    - back up early and often
    - protect against power surges and losses
- **Gold Standard** – implement controls beyond best practices – for those that strive to be 'the best of the best'