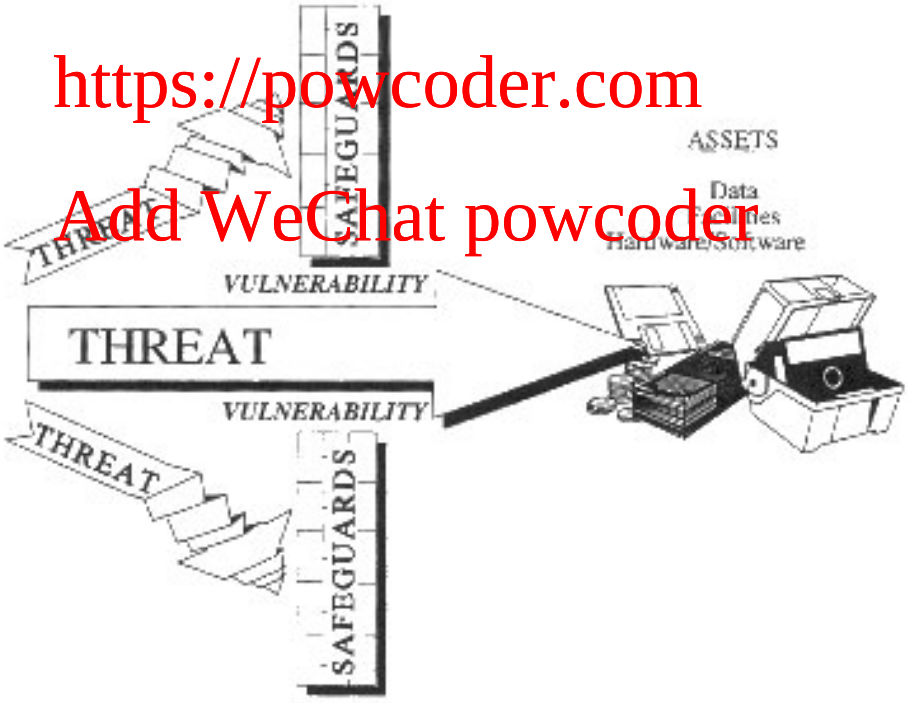
Risk in Information Security

- **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.)

documents stored on a server

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

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

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

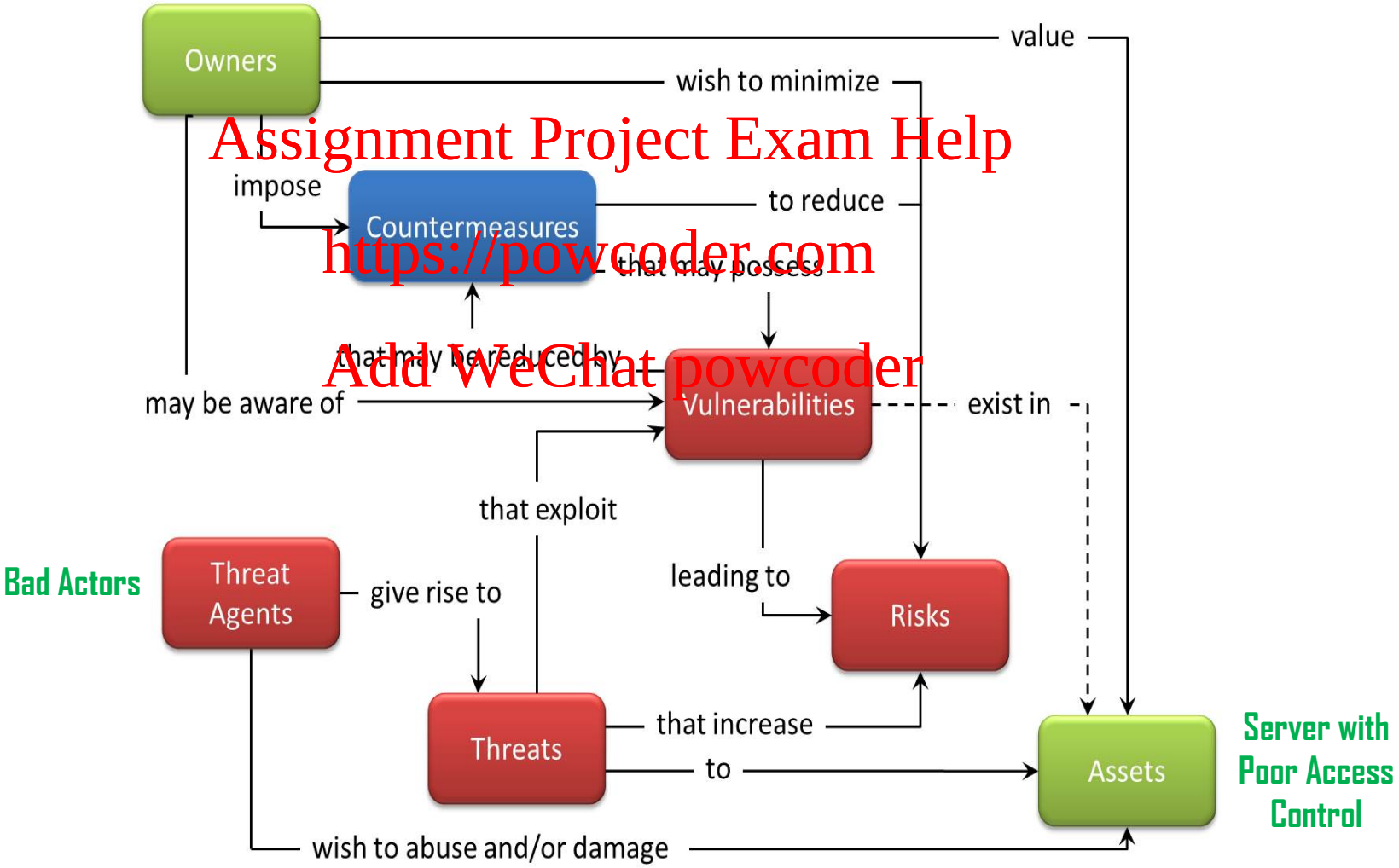
poor access control on the server

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

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

Risk in Information Security (cont.)

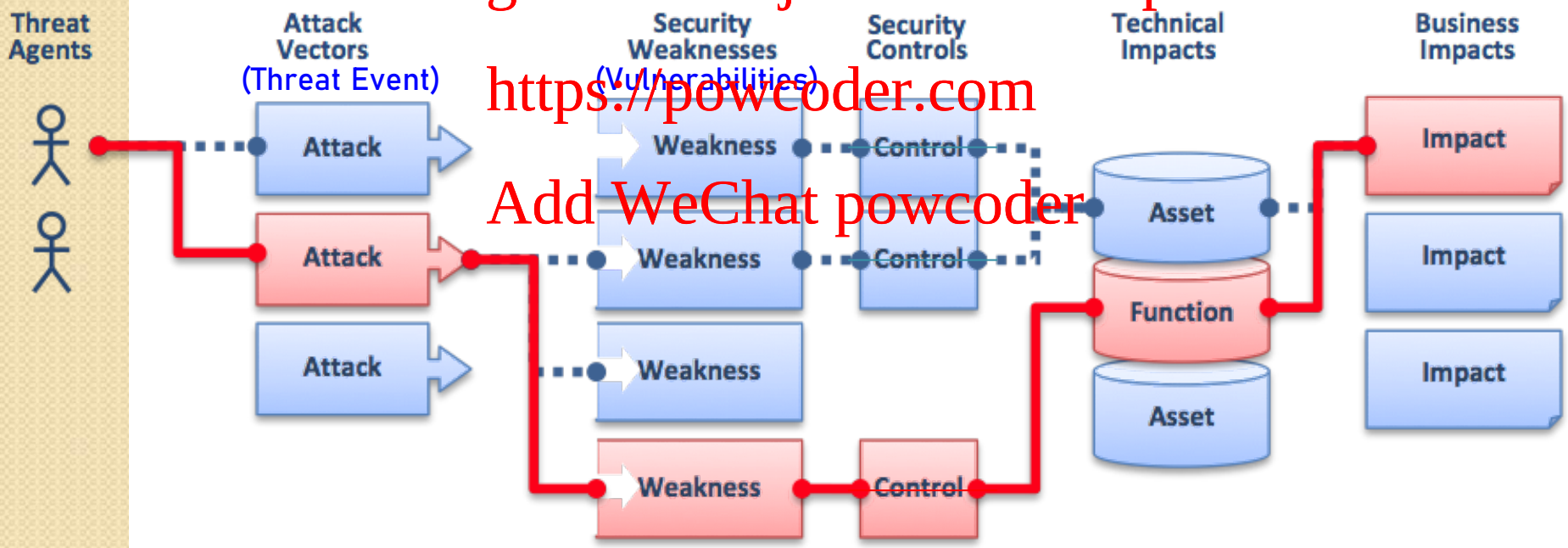
- **Interplay between Risk & other Info. Sec. Concepts**
  http://blog.patriot-tech.com/



Risk in Information Security (cont.)

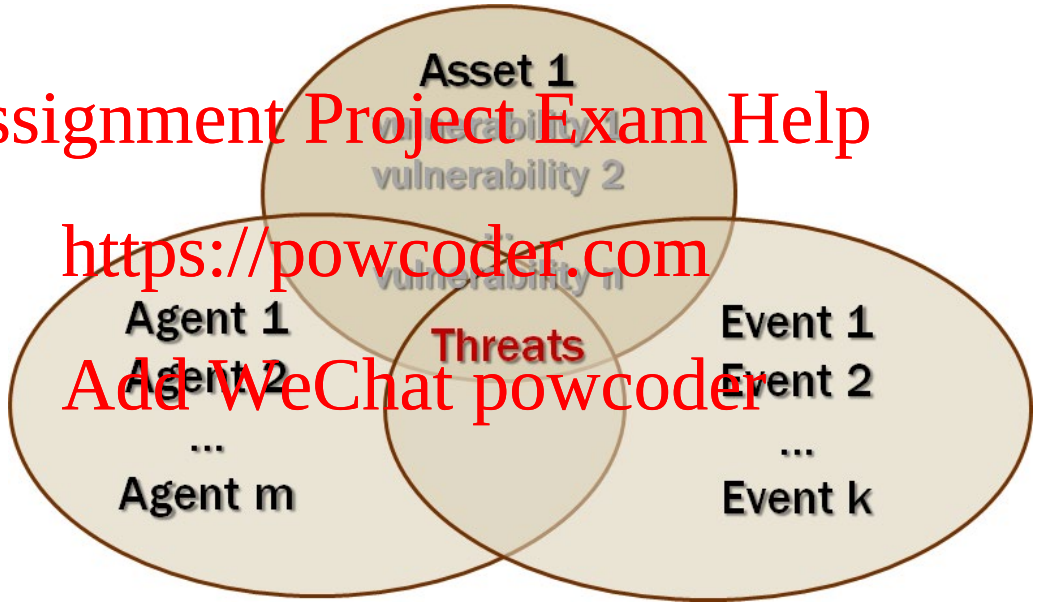
- **Asset, Threat, Vulnerability & Risk in Info. Sec.**

  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)?**

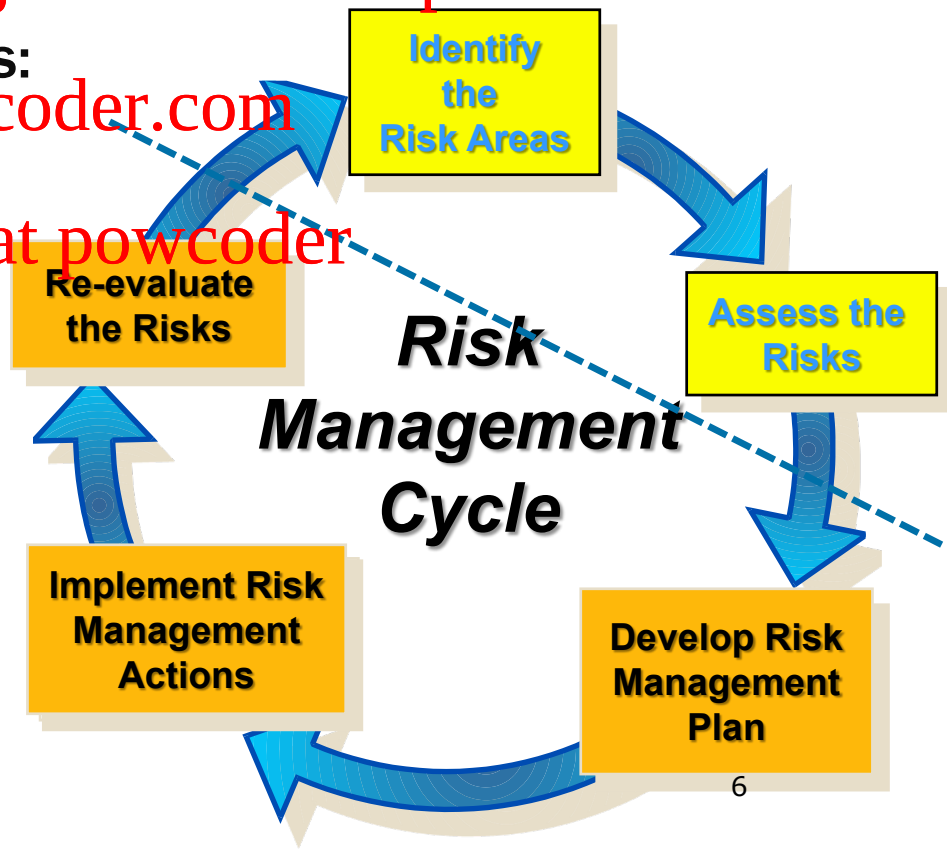


each company has many assets …
each asset may have many vulnerabilities …
each vulnerability may be associated with multiple threats …

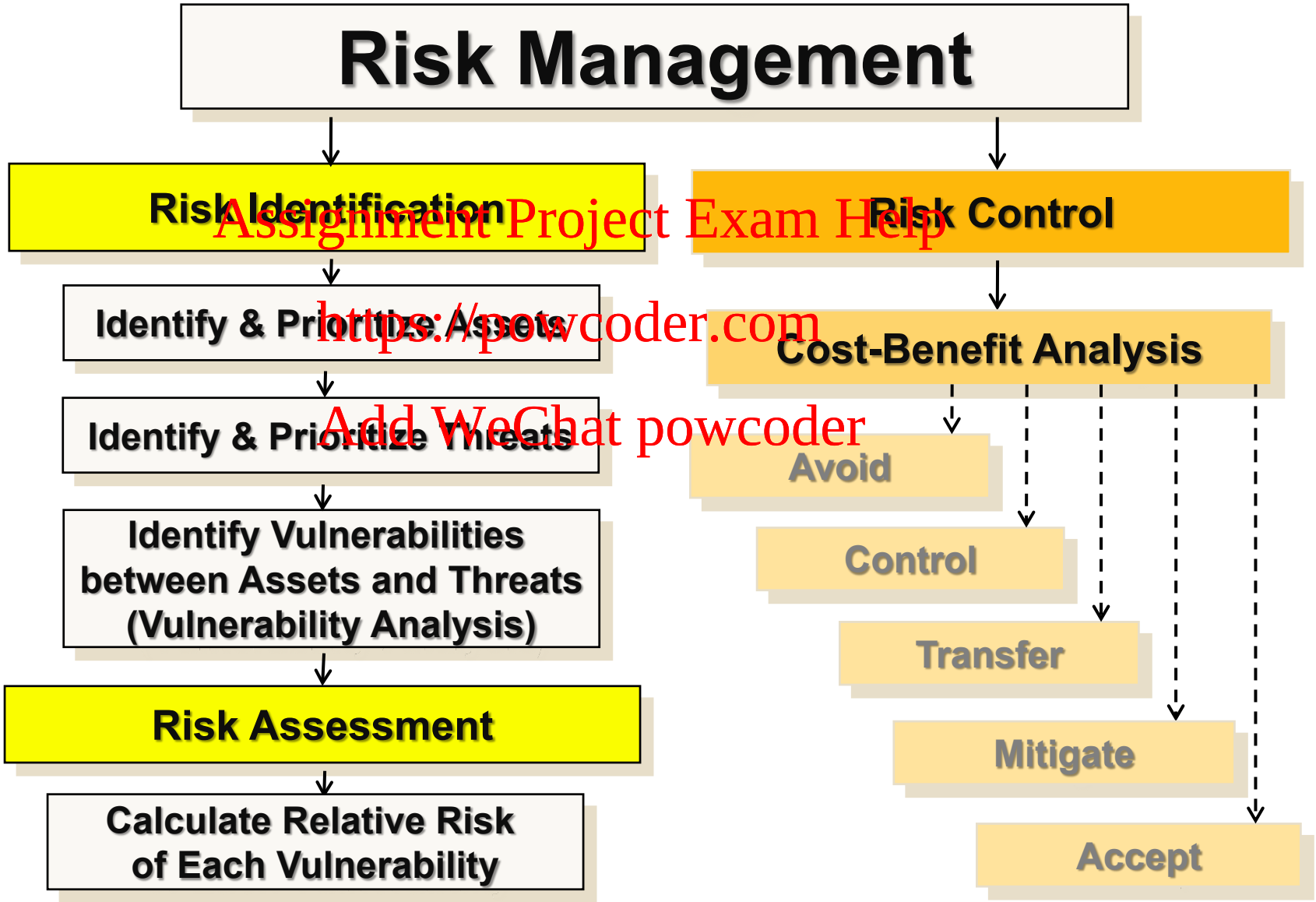
Where do we start dealing with Info. Sec. Risk ?!

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.)



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 !!

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 outside emails?

2) Backup procedure.

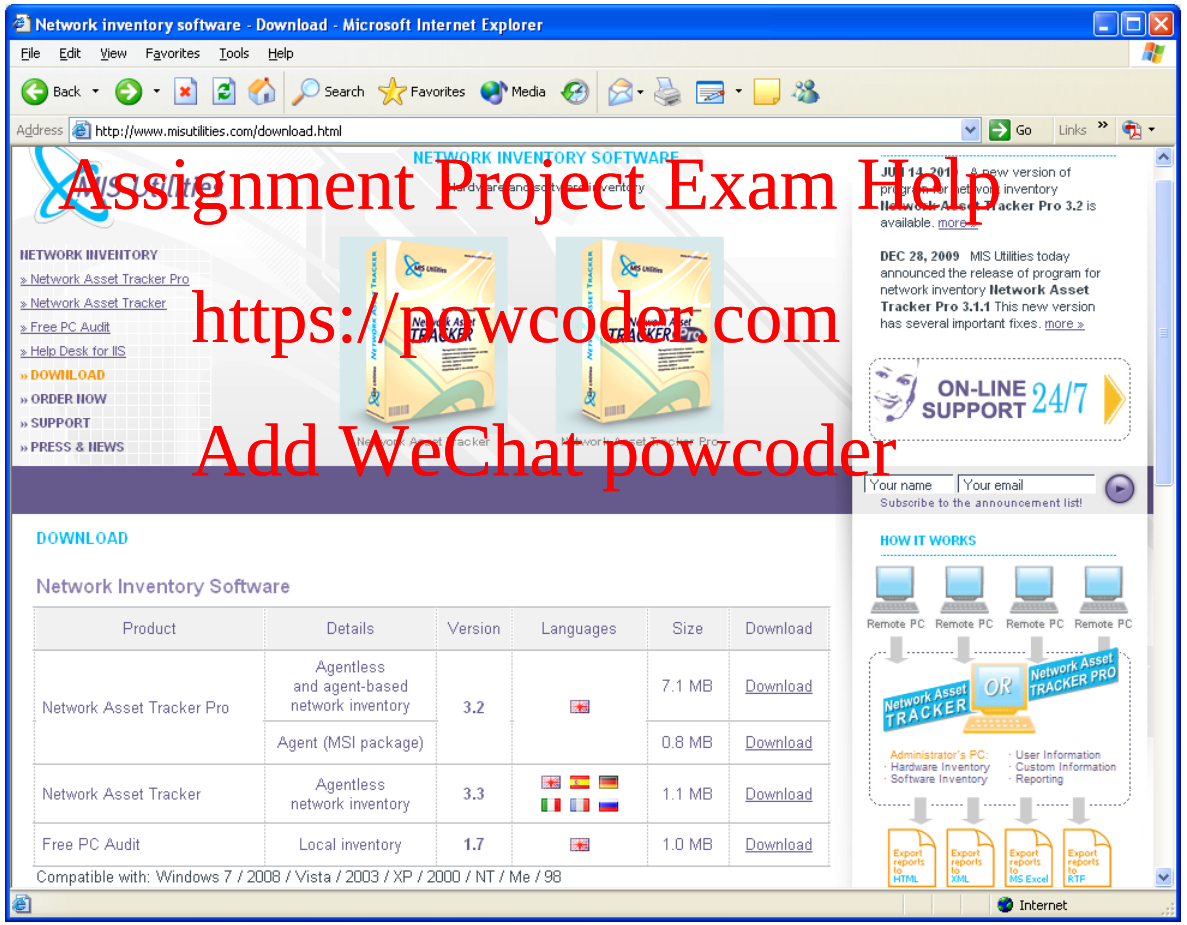
- No prejudging of asset values should be done at this stage – values are assigned later!

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



http://www.misutilities.com/
http://www.misutilities.com/network-asset-tracker/howtouse.html

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 profitability?

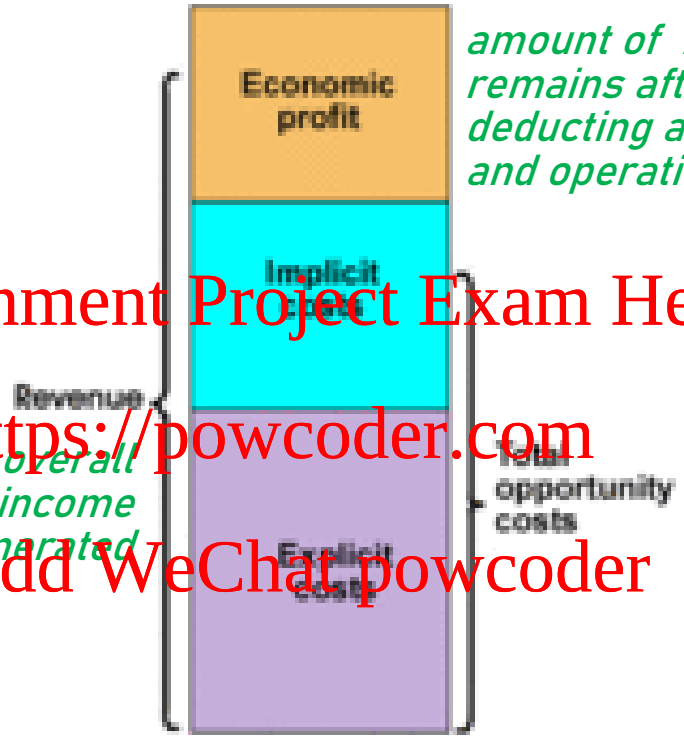
Example: Amazon's ranking assets

At Amazon.com, some servers support book sales (resulting in highest revenue), while others 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.)



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

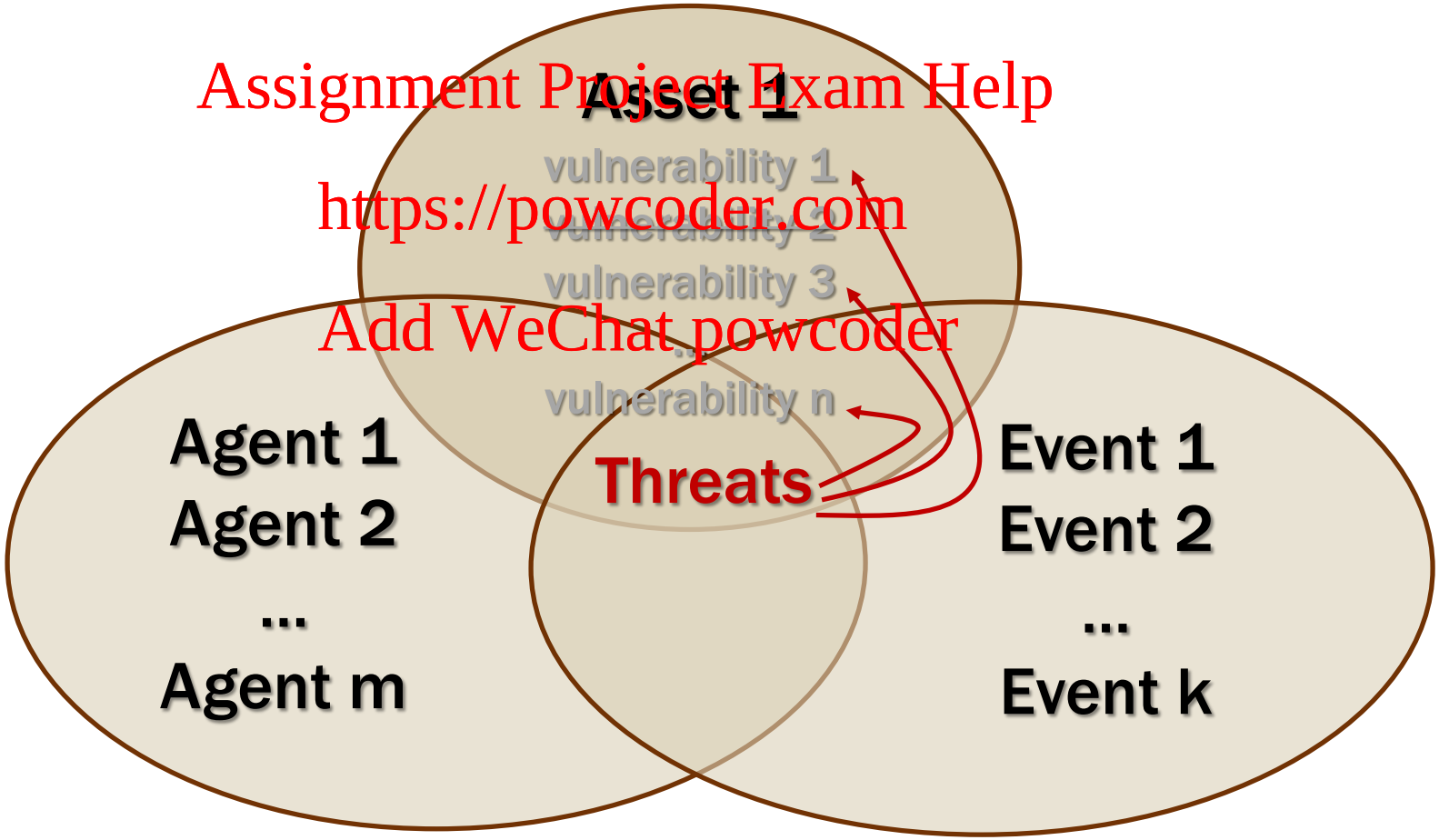
Data asset / information transmitted:

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 threats to those assets exist ...



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: CSI/FBI survey of types of threats/attacks

Computer Security Institute

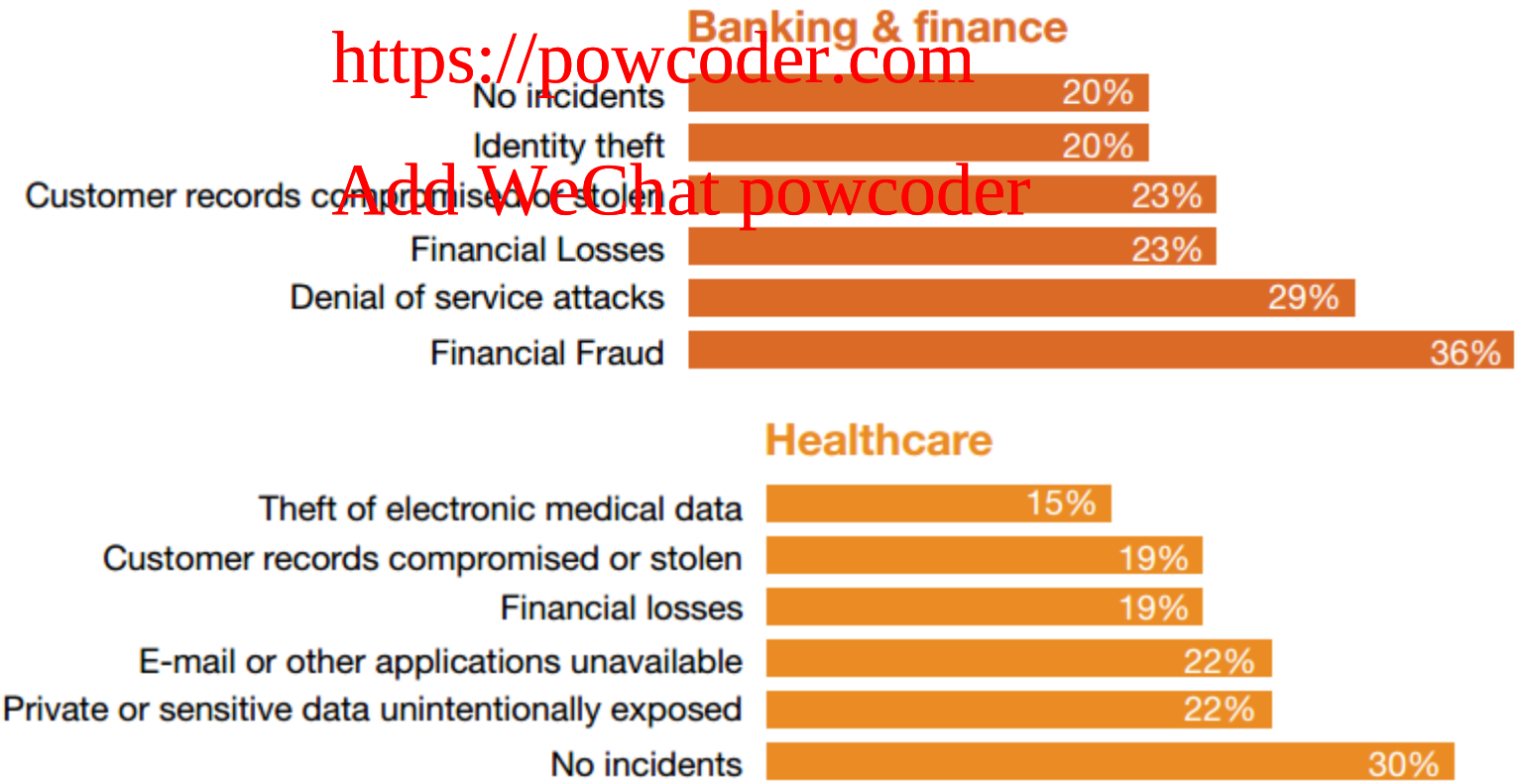
Type of Attack	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots / zombies within the organization	added in 2007		21%	20%	23%	29%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%	39%
Password sniffing	added in 2007		10%	9%	17%	12%
Financial fraud	7%	9%	12%	12%	20%	9%
Denial of service	32%	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%	1%
Web site defacement	5%	6%	10%	6%	14%	7%
Other exploit of public-facing Web site	option altered in 2009				6%	7%
Exploit of wireless network	16%	14%	17%	14%	8%	7%
Exploit of DNS server	added in 2007		6%	8%	7%	2%
Exploit of client Web browser	option added in 2009				11%	10%
Exploit of user's social network profile	option added in 2009				7%	5%
Instant messaging abuse	added in 2007		25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%	13%

Risk Identification: Threat Identification

Example: PwC Report "US Cybercrime: Rising Risks, Reduced Readiness" (2014)

http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Significant Detected Incidents Across Industries:

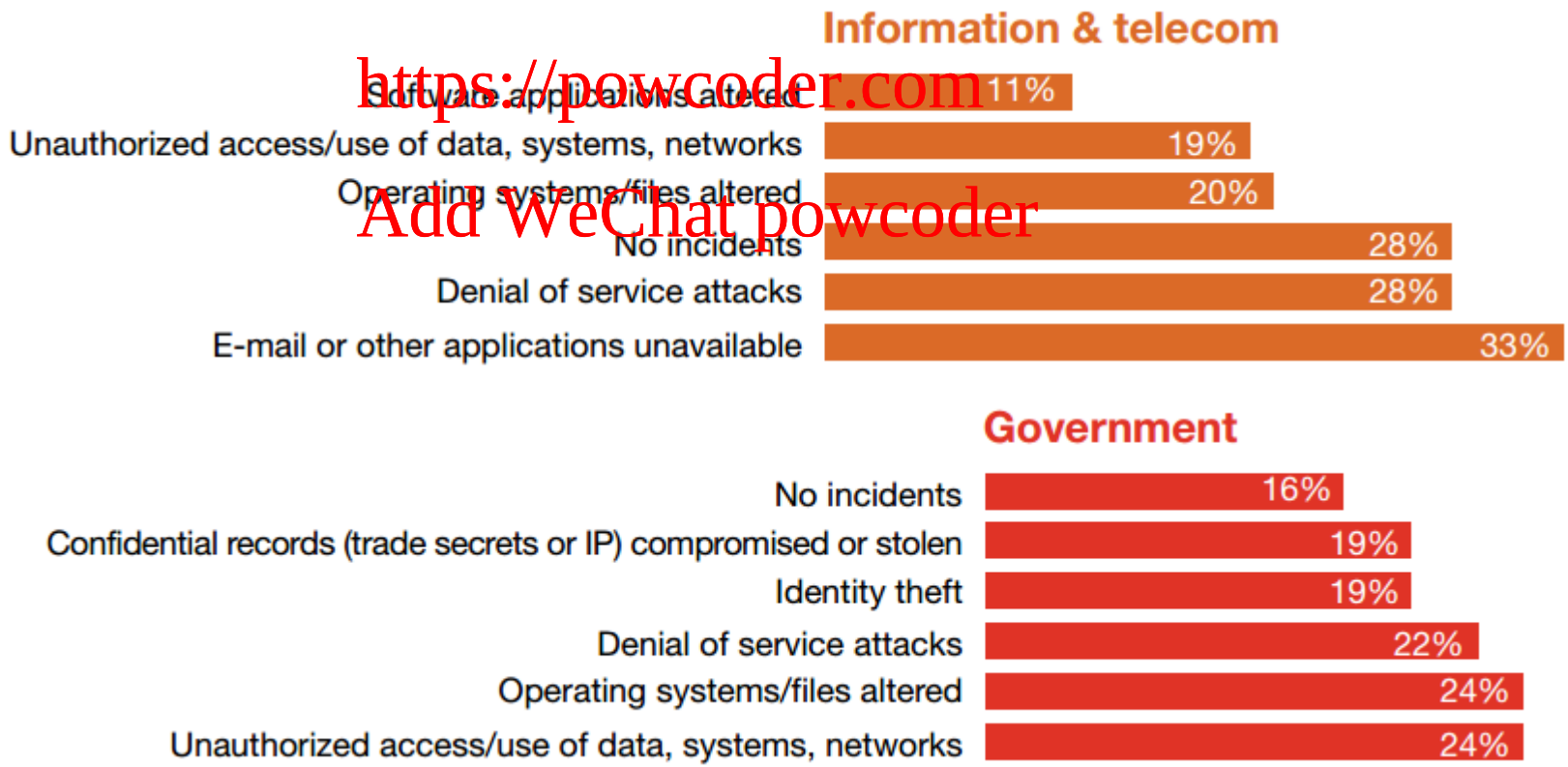


Risk Identification: Threat Identification

Example: PwC Report "US Cybercrime: Rising Risks, Reduced Readiness" (2014)

http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

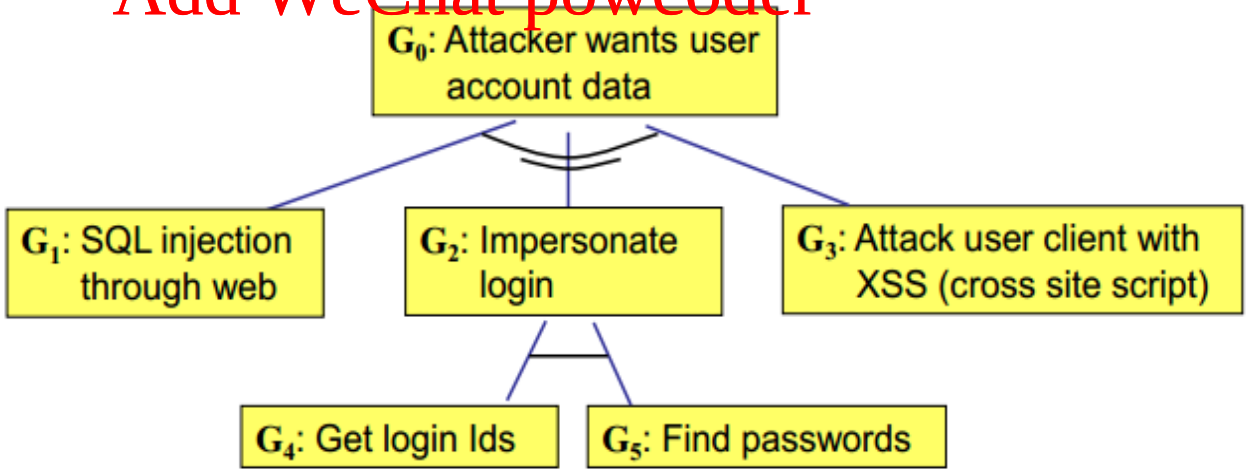
Significant Detected Incidents Across Industries:



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]

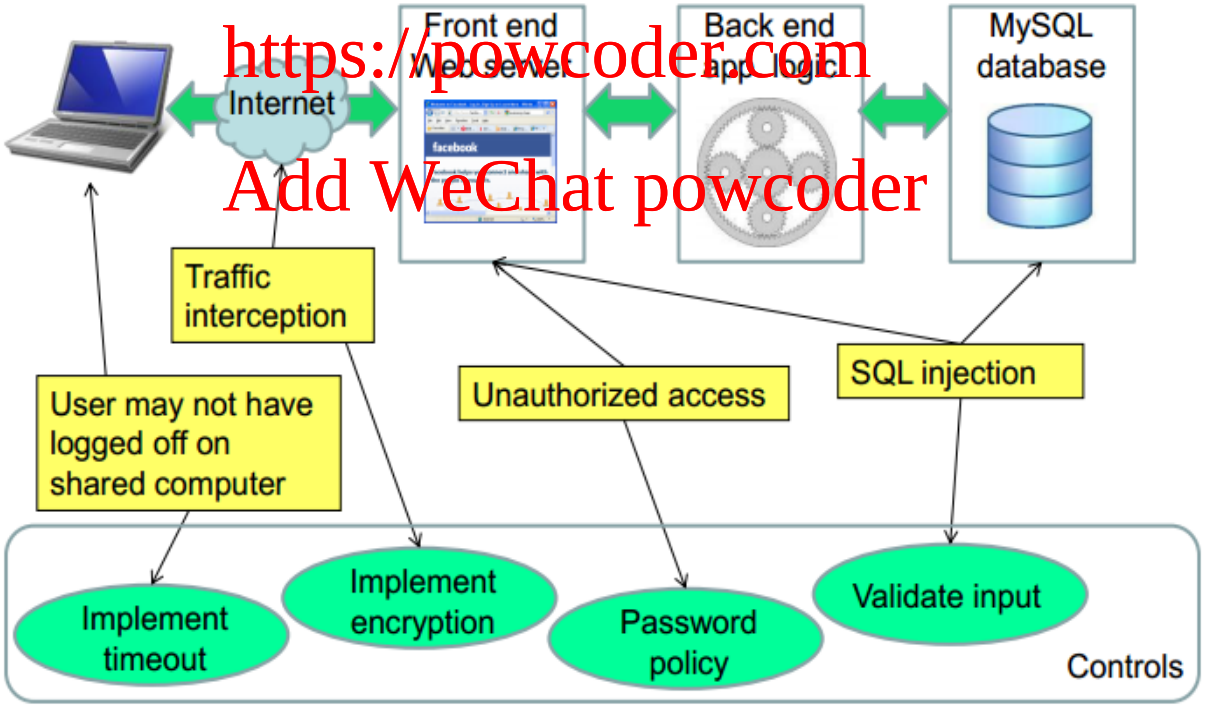
  - **Attacker-centric** – starts from attackers, evaluates their motivations and goals, and how they might achieve them through attack tree.



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

Risk Identification: Threat Identification (cont.)

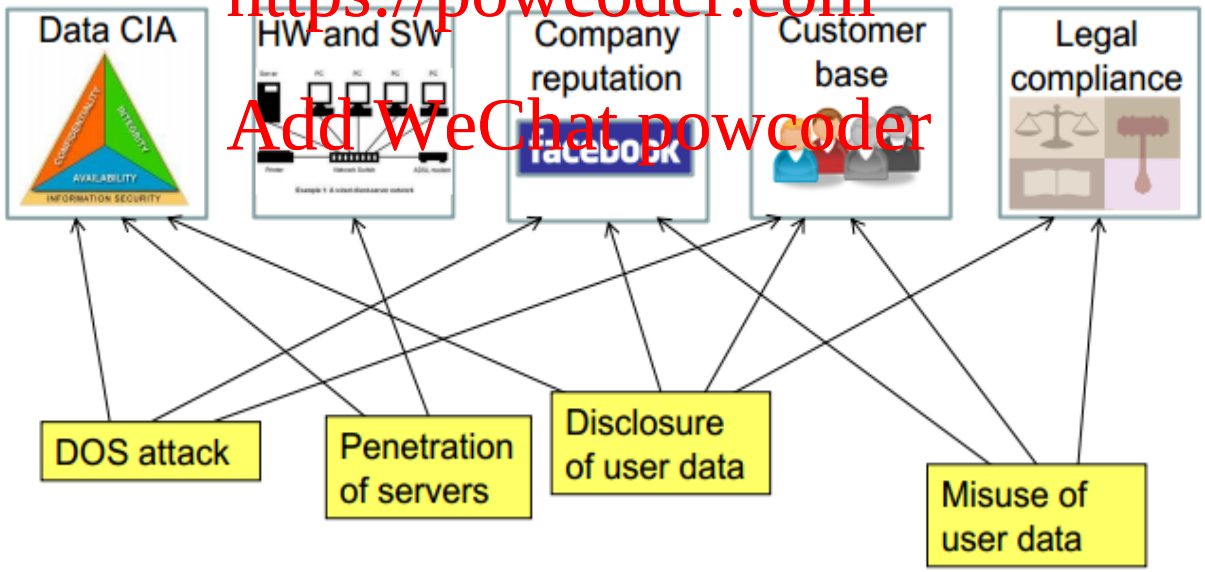
- Threat Modeling/Assessment
  - **System-centric** – starts from model of system, and attempts to follow model dynamics and logic, looking for types of attacks against each element of the model.



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

Risk Identification: Threat Prioritization

- **Questions used to <u>prioritize</u> threats:**
  - **Which threats present a 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 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?**

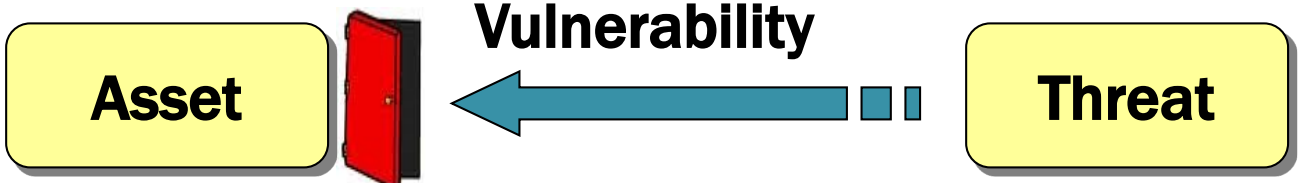
- **Threat ranking can be quantitative or qualitative.**
- **Once threats are prioritized, each asset should be reviewed against each threat to create a specific list of vulnerabilities.**

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

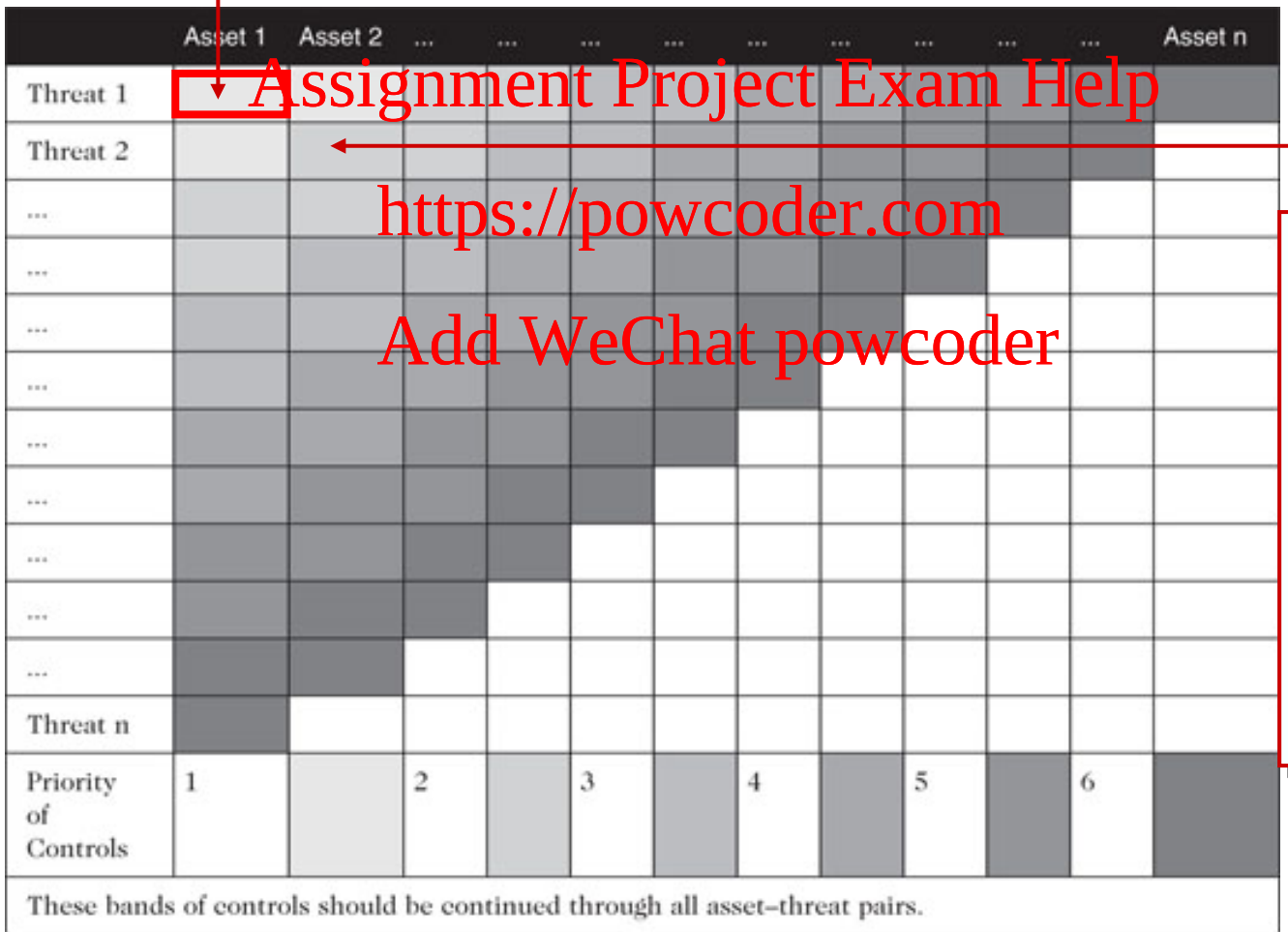


Vulnerability Analysis (cont.)

- **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, …

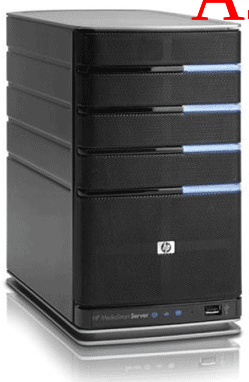


If intersection between T2 and A2 has no vulnerability, the risk assessment team simply crosses out that box.

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]

antivirus software not up-to-date

[procedural 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]

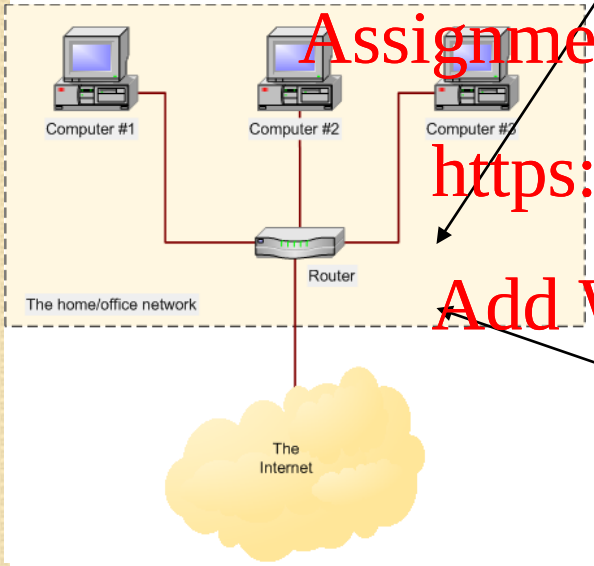
DDoS Attack

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