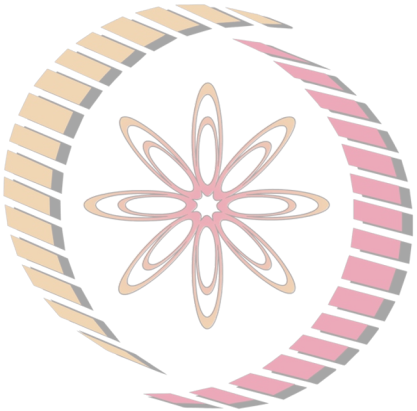
Cyber Security and Privacy
MS6880



Risk Management

Saji K Mathew, PhD
Professor, Management Studies
INDIAN INTITUTE OF TECHNOLOGY MADRAS

Do you know?

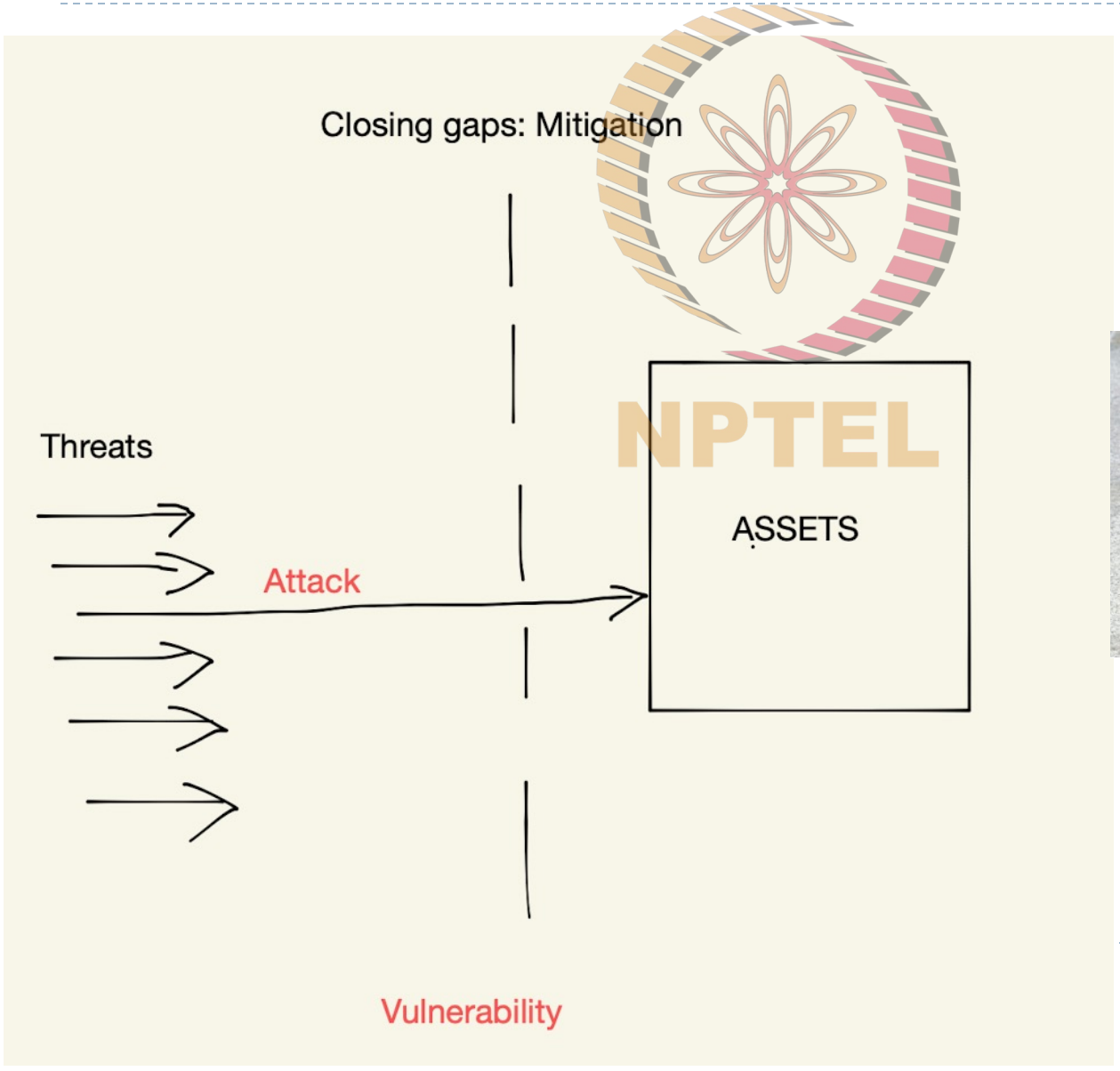
- If you know the enemy and know yourself, you need not fear the result of a hundred battles
- If you know yourself but not the enemy, for every victory gained you will also suffer a defeat
- If you know neither the enemy nor yourself, you will succumb in every battle

-- Sun Tzu

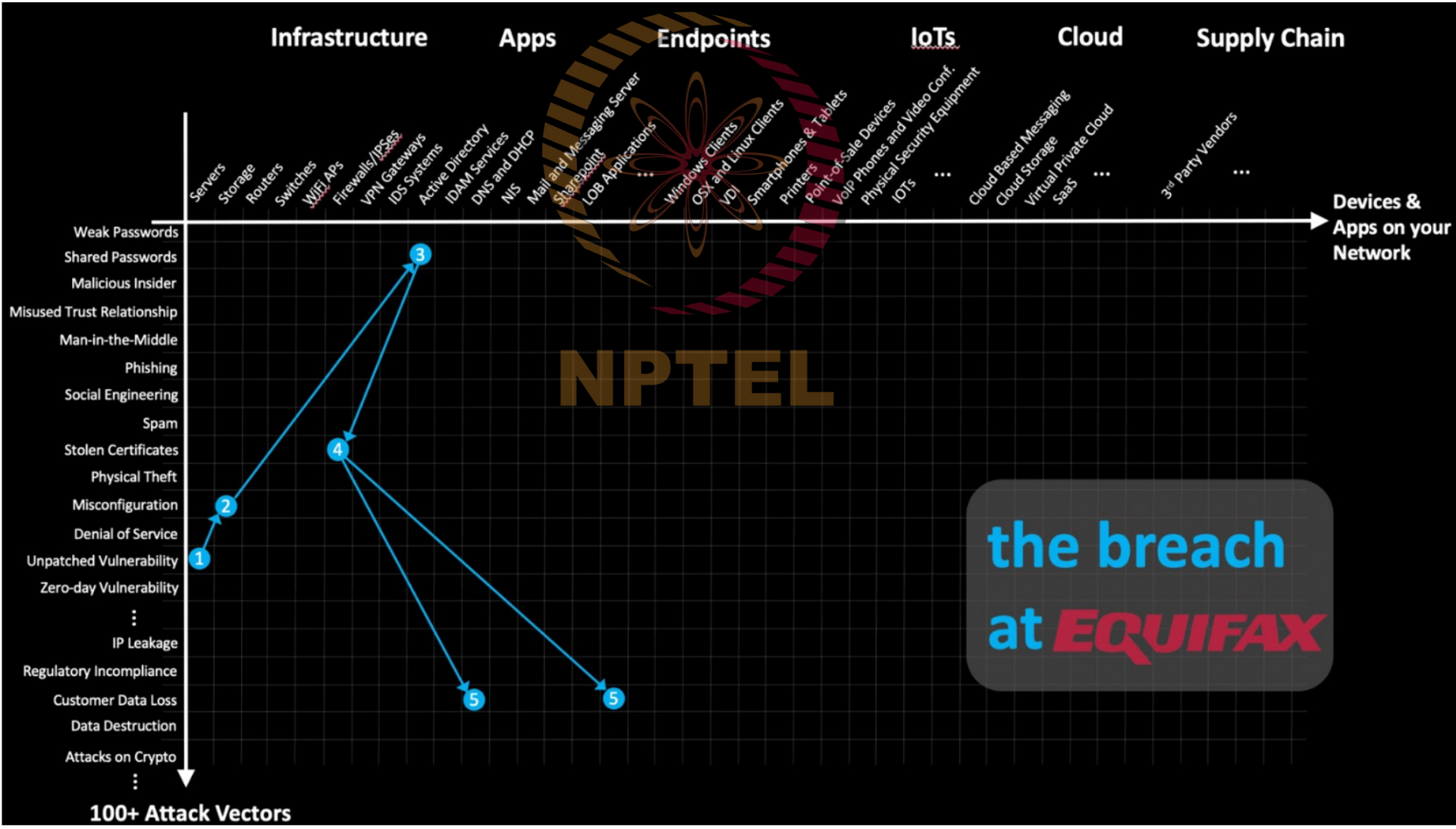
Risk management

- Knowing yourself: Identifying, examining, and understanding the information and how it is processed, stored, and transmitted
- Knowing the enemy: Identifying, examining, and understanding the threats facing the organization's information assets
- Risk management: The process of identifying, assessing, and reducing risks facing an organization

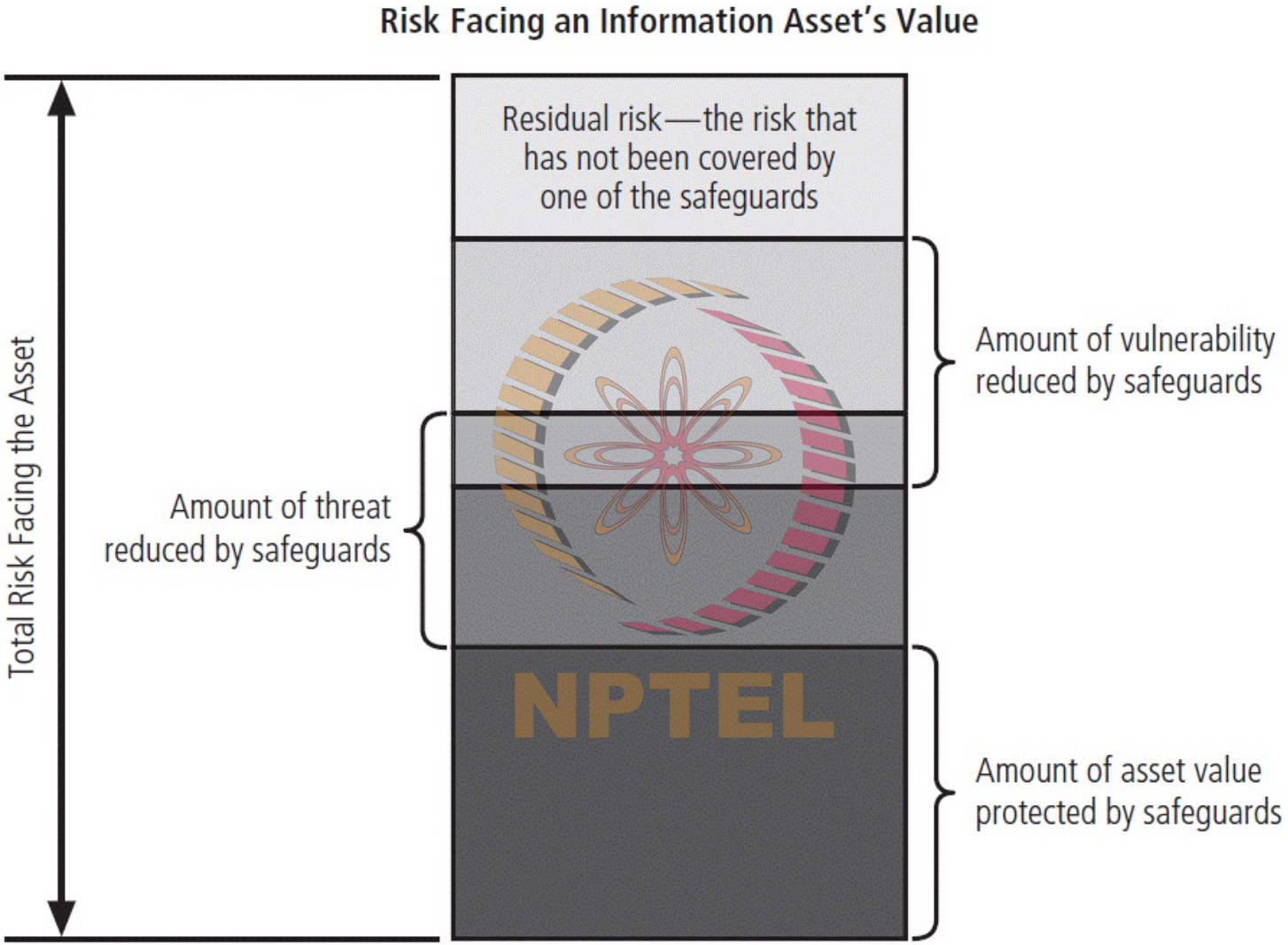
Threats, attack, vulnerability, risk

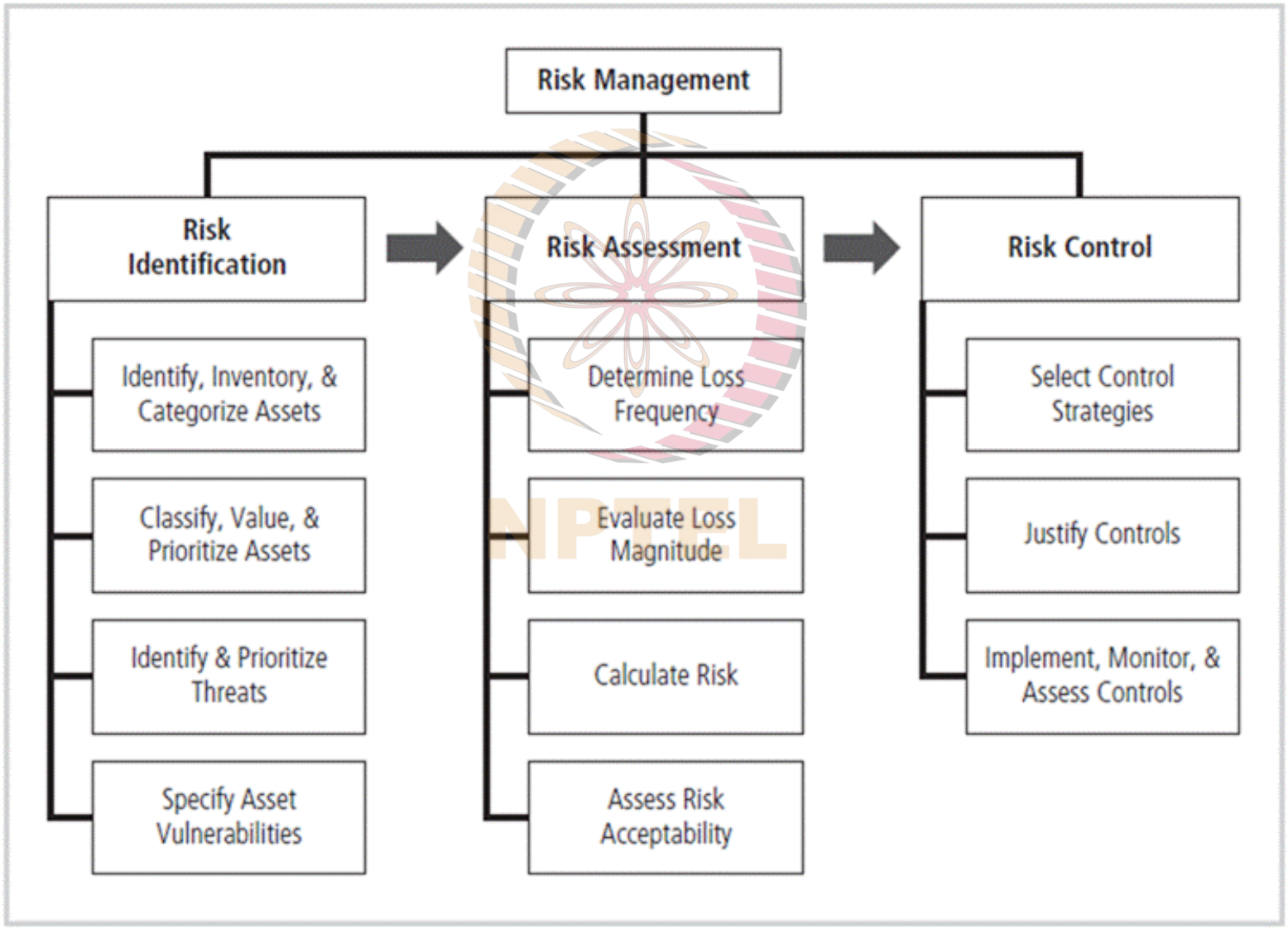


Attack surface



Residual risk




Risk Management
Risk Identification
Identify, Inventory, & Categorize Assets
Classify, Value, & Prioritize Assets
Identify & Prioritize Threats
Specify Asset Vulnerabilities
Risk Assessment
Determine Loss Frequency
Evaluate Loss Magnitude
Calculate Risk
Assess Risk Acceptability
Risk Control
Select Control Strategies
Justify Controls
Implement, Monitor, & Assess Controls

Risk identification

- Risk identification begins with the process of self-examination
- Managers identify the organization's information assets, classify them into useful groups, and prioritize them by their overall importance
- Identify information assets, including people, procedures, data and information, software, hardware, and networking elements
- This step should be done without pre-judging the value of each asset; values will be assigned later in the process

Organizational assets used in systems

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

Identifying hardware, software, and network assets

- Whether automated or manual, the inventory process requires a certain amount of planning
- Determine which attributes of each of these information assets should be tracked
- That will depend on the needs of the organization and its risk management efforts

Attributes for assets

- When deciding which attributes to track for each information asset, consider the following list of potential attributes:
  - Name
  - IP address
  - MAC address
  - Asset type
  - Serial number
  - Manufacturer name
  - Manufacturer's model or part number
  - Software version, update revision, or FCO number
  - Physical location
  - Logical location
  - Controlling entity

Identifying people, procedures, and data assets

- Responsibility for identifying, describing, and evaluating these information assets should be assigned to managers who possess the necessary knowledge, experience, and judgment
- As these assets are identified, they should be recorded via a reliable data-handling process like the one used for hardware and software

Suggested attributes for people, procedures, and data assets

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

Data classification model

- Example
  - Public
  - For official use only
  - Sensitive
  - Classified

FIGURE 7-3 Military Data Classification Cover Sheets

- The U.S. military classification scheme (Executive Order 12958)
  - Unclassified data
  - Sensitive but unclassified (SBU) data
  - Confidential data
  - Secret data
  - Top Secret data

Assessing values for information assets

- As each information asset is identified, categorized, and classified, assign a relative value
- Relative values are comparative judgments made to ensure that the most valuable information assets are given the highest priority, for example:
  - Which information asset is the most critical to the success of the organization?
  - Which information asset generates the most revenue?
  - Which information asset generates the highest profitability?
  - Which information asset is the most expensive to replace?
  - Which information asset is the most expensive to protect?
  - Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?

Knowing the enemy:
Identify and prioritize threats and threat agents

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

Threats

- Back doors
- Brute force
- Dictionary
- Man-in-the –middle
- Password crack
- Social engineering
- Phishing
  - Spear phishing
  - Vishing

Threat categories

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Deviations in quality of service from service providers	Power and WAN service issues
9. Forces of nature	Fire, flood, earthquake, lightning
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Weighted ranks of threats to information security

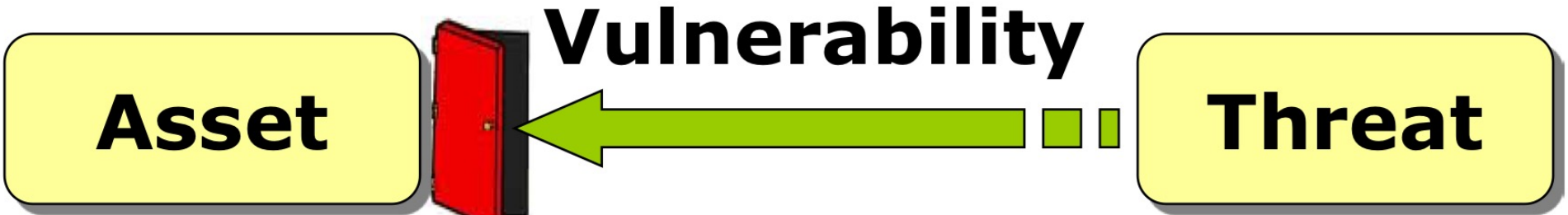
Weighted Ranks of Threats to Information Security

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

Source: Adapted from M. E. Whitman. Enemy at the gates: Threats to information security. *Communications of the ACM*, August 2003 reprinted with permission.

Vulnerability assessment

- Once you have identified the information assets of the organization and documented some threat assessment criteria, you can begin to review every information asset for each threat
- This review leads to the creation of a list of vulnerabilities that remain potential risks to the organization
- Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset
- *At the end of the risk identification process, a list of assets and their vulnerabilities has been developed*
- This list serves as the starting point for the next step in the risk management process: risk assessment



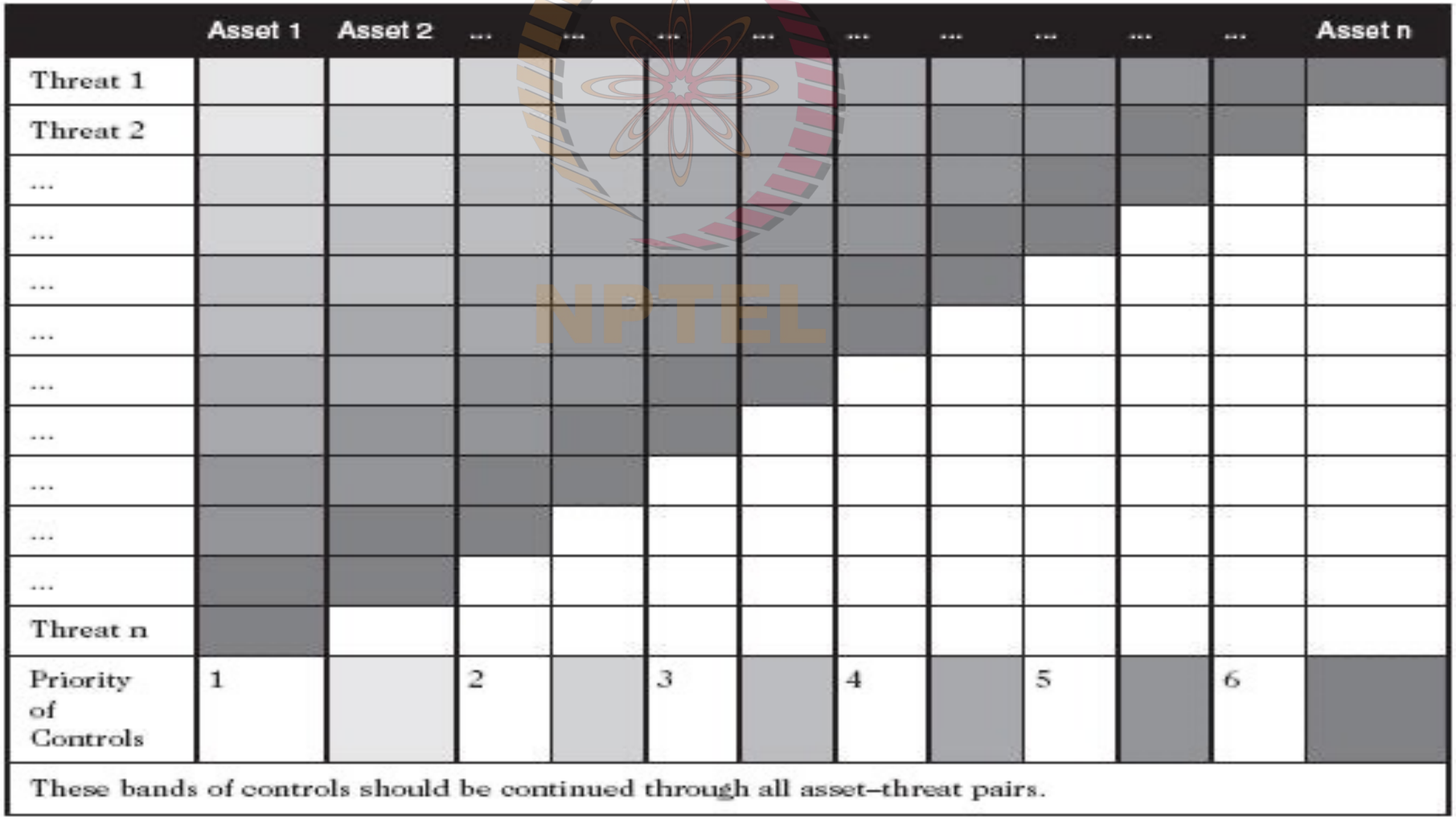
Vulnerability assessment of a DMZ router

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

Threat-Vulnerability-Asset (TVA) worksheet

- At the end of the risk identification process, a list of assets and their vulnerabilities has been developed
- Another list prioritizes threats facing the organization based on the weighted table discussed earlier
- These lists can be combined into a single worksheet

Sample TVA Spreadsheet



Determining the loss frequency

- Describes an assessment of the likelihood of an attack combined with expected probability of success
- Use external references for values that have been reviewed/adjusted for your circumstances.
- Assign numeric value to likelihood, typically annual value.
  - Eg.: Targeted by hackers once every five years: 1/5, 20 percent
- Determining an attack's success probability by estimating quantitative value (e.g., 10 percent) for the likelihood of a successful attack; value subject to uncertainty

Evaluating loss magnitude

- The next step is to determine how much of an information asset could be lost in a successful attack.
  - Also known as loss magnitude or asset exposure
- Combines the value of information asset with the percentage of asset lost in event of a successful attack
- Difficulties involve:
  - Valuating an information asset
  - Estimating percentage of information asset lost during best-case, worst-case, and most likely scenarios

Calculating residual risk

- For the purpose of relative risk assessment, risk equals:

Loss frequency TIMES loss magnitude MINUS *the percentage of risk mitigated by current controls* PLUS *measurement uncertainty*

Problem

Q: An ecommerce database has 10% chance of an attack this year based on industry reports (one attack in ten years). InfoSec dept reports if the infrastructure is attacked there is 50% chance of success based on current asset vulnerabilities and protection. The asset is valued at 50 in a 0-100 scale, and InfoSec informs that 80% asset will be compromised by a successful attack. Measurements are 75% accurate. Estimate risk

Example

Q: An ecommerce database has 10% chance of an attack this year based on industry reports (one attack in ten years). InfoSec dept reports if the infrastructure is attacked there is 50% chance of success based on current asset vulnerabilities and protection. The asset is values at 50 in a 0-100 scale, and InfoSec informs that 80% asset will be compromised by a successful attack. Measurements are 75% accurate. Estimate risk

A: Likelihood: 0.1; Attack success probability: 0.5

Loss frequency: 0.1*0.5=0.05

Loss magnitude= 0.8*50=40

Risk=0.05*40+error=2+2*0.25=2.5

Cyber Security and Practices

Case Study: Protecting the Cheddar

Group : 4
Jagvir Jaglan MS21A025
Prasad Deshmukh MS22S002
Sanjay Prasannan S MS22S010

FROM WALES WITH LOVE

Cole Newhouse emigrated to Wales

1811

Became the most popular cheesemonger

Entered Supermarket with tagline

The great depression

1929-1939

Chadwick Newhouse took over

Early 2000

Fully Digital, precision-controlled factory

CHADWICK ROBERT NEWHOUSE
CEO

FRANK ARMEN
CISO

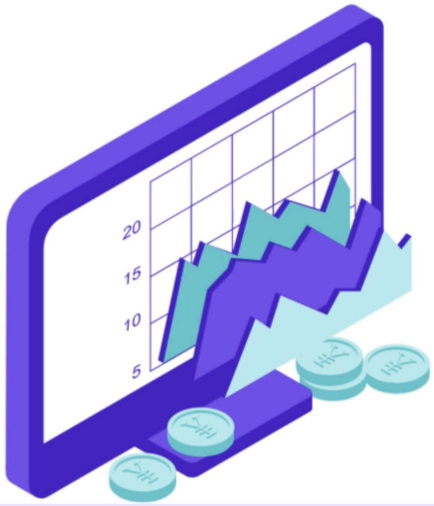
BRUCE BOYLE
COO

JENNY CRUICKSHANK
CFO

SARA WILUND
Deputy to COO

JACK PAREM
Consultant

Characters of Case Study



Begining of the case study

1. Chad had wired $49,999
2. The company suffered from "Ransomware" attack
3. Hackers gained access to the system
4. Ransom was paid on the advice from FBI and lawyers

Who invited her ??

what do we do ?

CHAD

FRANK

Review our incident response protocol, because SEC will come knocking

How much have we already spent ?

$ 6 million

Still breaches have increased

"Um, Why are our control system even online ?

Who invited her ??

Shouldn't family recipes just be locked up on paper ?
Why do we need them digitally ? and the pasteurization equipment and all ?

- Overly complicated systems are vulnerable
- Anywhere - anytime access
- Many consultants recommend humans in the process

But if someone did get access?

Sensors in the tanks send us real-time data about everything ,"
"It's saved millions of dollars"

TECH GUY

"Of course. Otherwise someone would have to be here whenever the process was happening. This way, we just get alerts if something is out of whack. That's crucial to the cost savings."

Who has access?

"And the system is networked?"

JACK PAREM

"Anyone with a login, but we only give it to, I don't know, two or three people. Mostly it's me. When I was on vacation last month, I logged in from my hotel to check on things.

Steps of the Consultant

STEP 1

Identifying the most critical information and processes.

STEP 2

Mapping digital terrrain on which those processes rested

STEP 3

Illuminating most likely path of the attack

STEP 4

Generating the options

Findings of the Consultant

3 Points of Failure

FOUR
PATHWAYS INTO
NETWORK

HACKER ACCESS
INDUSTRIAL CONTROL
SYSTEM

ONE SYSTEM
COMPROMISED BY BOT

“RANSOMWARE DOESN’T SCARE ME; LISTERIA DOES”

“The whole point of going digital was to save money. Going offline could kill the bottom line.

BRUCE

“You want us to roll the business back 20 years on a one-in-a-million chance?”

FRANK

“The goal isn’t to go back to the Stone Age; it’s to reduce the digital pathways

JACK PAREM

frankly, ransomware doesn’t scare me, Listeria does

How Ransomware Works

1. Bad guys create ransomware themselves or buy/lease it from other cybercriminals.

2. Cybercriminals use social engineering to gain access to your network or systems.

3. They use the malware to digitally encrypt all your IT systems and data possible.

4. Attackers use your encrypted sensitive data as leverage to force you to pay a ransom.

In some cases, attackers will exfiltrate your data prior to encrypting your systems.

Should Chad implement the consultant's recommendations ?

Opinions ?

Implementation of Consultant's Recommendation

Pros

1. Isolation and prevention of critical systems to ensure the least damage
2. Production won't be hindered by the cyber attacks.
3. Sensitive data is more secured in offline mode.
4. Less chances of unauthorized access

Cons

1. Security at the cost of automation & efficiency.
2. Investors might penalize for being overcautious
3. Raised costs
4. Hinderance to operations

Other security measures ?

Opinions ?

Alternative Solutions

- Multi-Factor Authentication
- VPNs
- Multiple Firewalls
- Malware Detections
- Policy
- Lock all unused ports
- For bidirectional communication use a single open port
- Limit Remote Access functionality wherever possible
- Training and Awareness

UKRAINE

POWER GRID

DECEMBER 2015

- Remote operation of breakers using remote industrial control system (ICS) client software
- Scheduled disconnects for server UPS via UPS remote management interface.
- Wiped systems by KillDisk malware to make it fully inoperative

Thank you !