CSE 4215

Chapter 1

Introduction

Md. Shahid Uz Zaman
Dept. of CSE, RUET

Course Syllabus

Introduction: Network Security Policies, Strategies and Guidelines; Network Security Assessments and Matrices.

Different Attacks: Denial of Service (Dos) Attack, Distributed Denial of Service (Ddos) Attack, Eavesdropping, IP Spoofing, Sybil Attack, Blackhole Attack, Grayhole Attack, ManIn-The-Middle Attack, Passwords-based Offline Attacks.

Network Security Threats and Attackers: Intruders, Malicious Software, Viruses and Spy-Ware; Security Standards: DES, RSA, DHA, Digital Signature Algorithm (DSA), SHA, AES; Security At Transport Layer: Secure Socket Layer (SSL) and Transport Layer Security (TLS).

Security on Network Layer: Ipsec; Network Security Applications: AAA Standards, EMail Securities, PGP, S/MIME; PKI Smart Cards; Sandboxing; Firewalls and Proxy Server;

Security for Wireless Network Protocols: WEP, WPA, TKIP, EAP, LEAP; Security Protocols for Ad-Hoc Network; Security Protocols for Sensor Network; Security for Communication Protocols; Security for Operating System and Mobile Agents; Security for E-Commerce; Security for LAN and WAN; Switching and Routing Security; other State-OfThe-Art Related Topics.

Chapter 1: Network Security Policies

What is a Policy?

- A Policy is a written document with a set of guidelines and principles that will be followed by an employee of an organization. It helps to take a decision.

Example: An employee should NOT reveal the information to 3rd party that is harmful to the company.

What is Security Policies?

- A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur.
- A security policy must identify all of a company's assets as well as all the potential threats to those assets.
- Company employees need to be kept updated on the company's security policies.
- The policies themselves should be updated regularly as well.

Types of Security Policies?

- **Acceptable Use Policy (AUP)**
- **Access Control Policy (ACP)**
- **Change Management Policy**
- **Information Security Policy**
- **Incident Response (IR) Policy**
- **Remote Access Policy**
- **Email/Communication Policy**
- **Disaster Recovery Policy**
- **Business Continuity Plan (BCP)**

Chapter 1: Network Security Policies

Acceptable Use Policy (AUP)

- An AUP stipulates the constraints and practices that an employee using organizational IT assets must agree to in order to access to the corporate network or the internet.
- It is standard on boarding policy for new employees. They are given an AUP to read and sign before being granted a network ID.

Example:

- Which site can I visit?
- Can I use my ID to use other staff
- Can I print my own doc and so on

Access Control Policy (ACP)

- The ACP outlines the access available to employees in regards to an organization's data and information systems.
- Other items covered in this policy are standards for user access, network access controls, operating system software controls and the complexity of corporate passwords.
- Additional supplementary items often outlined include methods for monitoring how corporate systems are accessed and used; how unattended workstations should be secured; and how access is removed when an employee leaves the organization.

Example:

- Only admin can enter the server room
- A faculty can access the data of students
- A student access a certain level of data access

Chapter 1: Network Security Policies

Change Management Policy (CMP)

- A change management policy refers to a formal process for making changes to IT, software development and security services/operations.
- The goal of a change management program is to increase the awareness and understanding of proposed changes across an organization, and to ensure that all changes are conducted methodically to minimize any adverse impact on services and customers.

Example:
- Who can change what?
- Who is responsible for upgrading the software?

Information Security Policy (ISP)

An information security policy is a set of rules and guidelines that dictate how information technology (IT) assets and resources should be used, managed, and protected.

Incident Response Policy (IRP)

- The incident response policy is an organized approach to how the company will manage an incident and remediate the impact to operations.
- The goal of this policy is to describe the process of handling an incident with respect to limiting the damage to business operations, customers and reducing recovery time and costs.

Example:
- Handle Cyber Attack

Chapter 1: Network Security Policies

Remote Access Policy (RAP)

- The remote access policy is a document which outlines and defines acceptable methods of remotely connecting to an organization's internal networks.

Example:

- Who should be given remote access?
- What information can be accessed remotely?

Email/Communication Policy (ECP)

- A company's email policy is a document that is used to formally outline how employees can use the business' chosen electronic communication medium.
- The primary goal of this policy is to provide guidelines to employees on what is considered the acceptable and unacceptable use of any corporate communication technology

Disaster Recovery Policy (DRP)

- An organization's disaster recovery plan will generally include both cybersecurity and IT teams' input and will be developed as part of the larger business continuity plan.
- The CISO and teams will manage an incident through the incident response policy. If the event has a significant business impact, the Business Continuity Plan will be activated

Example:

- Continue the business if one branch goes down due to disaster using other branch

Chapter 1: Network Security Policies

Business Continuity Policy (BCP)

The BCP will coordinate efforts across the organization and will use the disaster recovery plan to restore hardware, applications and data deemed essential for business continuity.

BCP's are unique to each business because they describe how the organization will operate in an emergency.

Example:

- Fire in one branch but still continue the business using other options

Chapter 1: Network Security Policies

Detail Email Policy-1

- An email security policy is an official company document that details acceptable use of your organization's email system.
- It indicates to whom and from whom emails can be sent or received and defines what constitutes appropriate content for work emails.

Detail Email Policy-2

Protect the Organization from Liabilities:

- When all employees read and sign an email policy, it proves they are aware and agree to the information contained in that policy.
- Should an email be sent that is not considered appropriate content according to the email policy, the employee, not the business, would bear the brunt of liability for any damages or suits brought as a result of their sending an inappropriate email.

Detail Email Policy-3

- **Promote a Professional Environment**: If email is used only in a professional manner in the workplace, you can be sure that embarrassing mistakes will not occur.
- For example, if staff are using work email to communicate with friends, the content in those emails are likely to be sloppy, unprofessional, and informal.
- If those emails accidentally get sent to clients or other professionals - the company image may become damaged.
- If an email policy does not allow for personal use of the work email system, your staff will remain in a professional mindset and eliminate the potential of personal emails going out to customers.

Detail Email Policy-4

- **Increase Productivity**: Email tends to be a distraction for employees who are using it for non-professional reasons.
- If an email policy prohibits the use of work email for personal use, your employees will stay on task more and avoid the distractions that come from sending and receiving personal emails during work hours.

Chapter 1: Network Security Policies

Detail Email Policy-5

- **Establish Systems for Email**: If the email policy outlines appropriate content for an email sent during work hours over the company email system, it can also help establish systems to ensure all staff members are contributing to the brand or image of the company.
- Have each staff member use a template for email responses and set up signature lines that appear in all outgoing emails to further establish the company's professionalism and image in the eyes of individuals who may receive email from your staff.
- Setting guidelines for content and use of email creates a single, comprehensive image of the company that helps keep the organization aligned with its mission.

Sample Email Security Policy

Inappropriate use of company email

- Our employees represent our company whenever they use their corporate email address. They must not:
- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a competitor's services unless authorized.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.

Appropriate use of corporate email

- Employees are allowed to use their corporate email for work-related purposes without limitations. For example, employees can use their email to:
- Communicate with current or prospective customers and partners.
- Log in to purchased software they have legitimate access to.
- Give their email address to people they meet at conferences, career fairs or other corporate events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

Chapter 1: Network Security Policies

Sample Email Security Policy-continue

Personal use

- Employees are allowed to use their corporate email for some personal reasons. For example, employees can use their corporate email to:
- Register for classes or meetups.
- Send emails to friends and family as long as they don't spam or disclose confidential information.
- Download ebooks, guides and other content for their personal use as long as it is safe and appropriate.

Email Security

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every two months.

Sample Email Security Policy-continue

Email Security

- Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:
- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If an employee isn't sure that an email they received is safe, they can ask our [*Security Specialists*.]
- We remind our employees to keep their anti-malware programs updated.

Chapter 1: Network Security Policies

Sample Email Security Policy-continue

Email signature

- We encourage employees to create an email signature that exudes professionalism and represents our company well. Salespeople and executives, who represent our company to customers and stakeholders, should pay special attention to how they close emails. Here's a template of an acceptable email signature:
- *[Employee Name]*
- *[Employee Title], [Company Name with link]*
- *[Phone number] | [Company Address]*
- Employees may also include professional images, company logos and work-related videos and links in email signatures. If they are unsure how to do so, they can ask for help from our Office Manager or their supervisor.

Sample Email Security Policy-continue

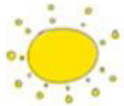
Disciplinary action

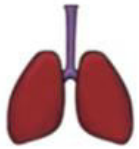
- Employees who don't adhere to the present policy **will face disciplinary action up to and including termination**. Example reasons for termination are:
- Using a corporate email address to send confidential data without authorization.
- Sending offensive or inappropriate emails to our customers, colleagues or partners.
- Using a corporate email for an illegal activity.

Chapter 1: Risk Assessment

WHAT IS RISK?

Life is full of risks!





Breathing.....

7 million deaths a year!

Eating.....

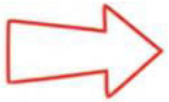
420,000 deaths a year!

Travelling.....

3,000 deaths each day!

We need to take decisions to face risk

What is the risk from certain events?



Appropriate action!

Risk

depends on viewpoint and context

New virus

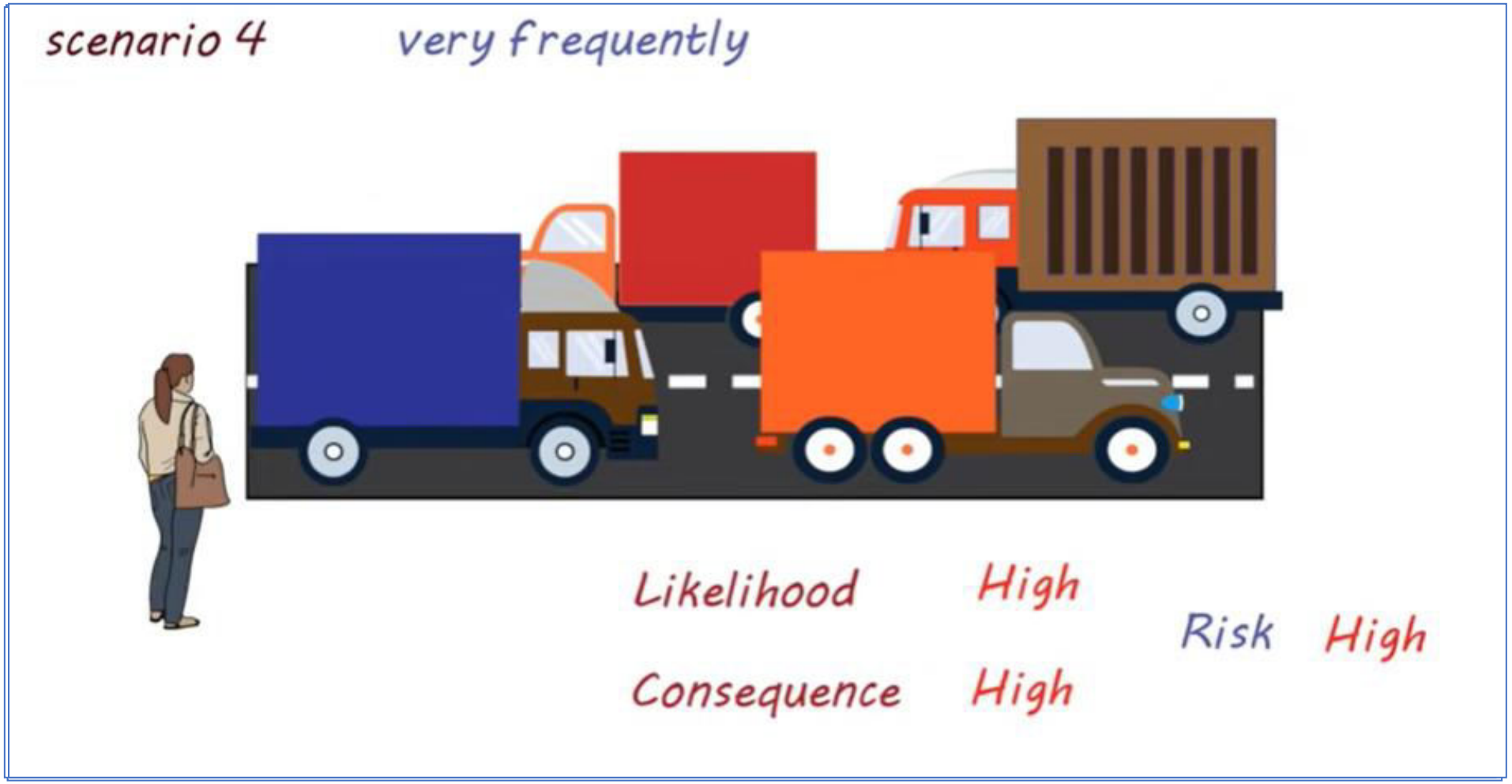
Industrial accident

Bushfire

Risk = Likelihood X Consequence

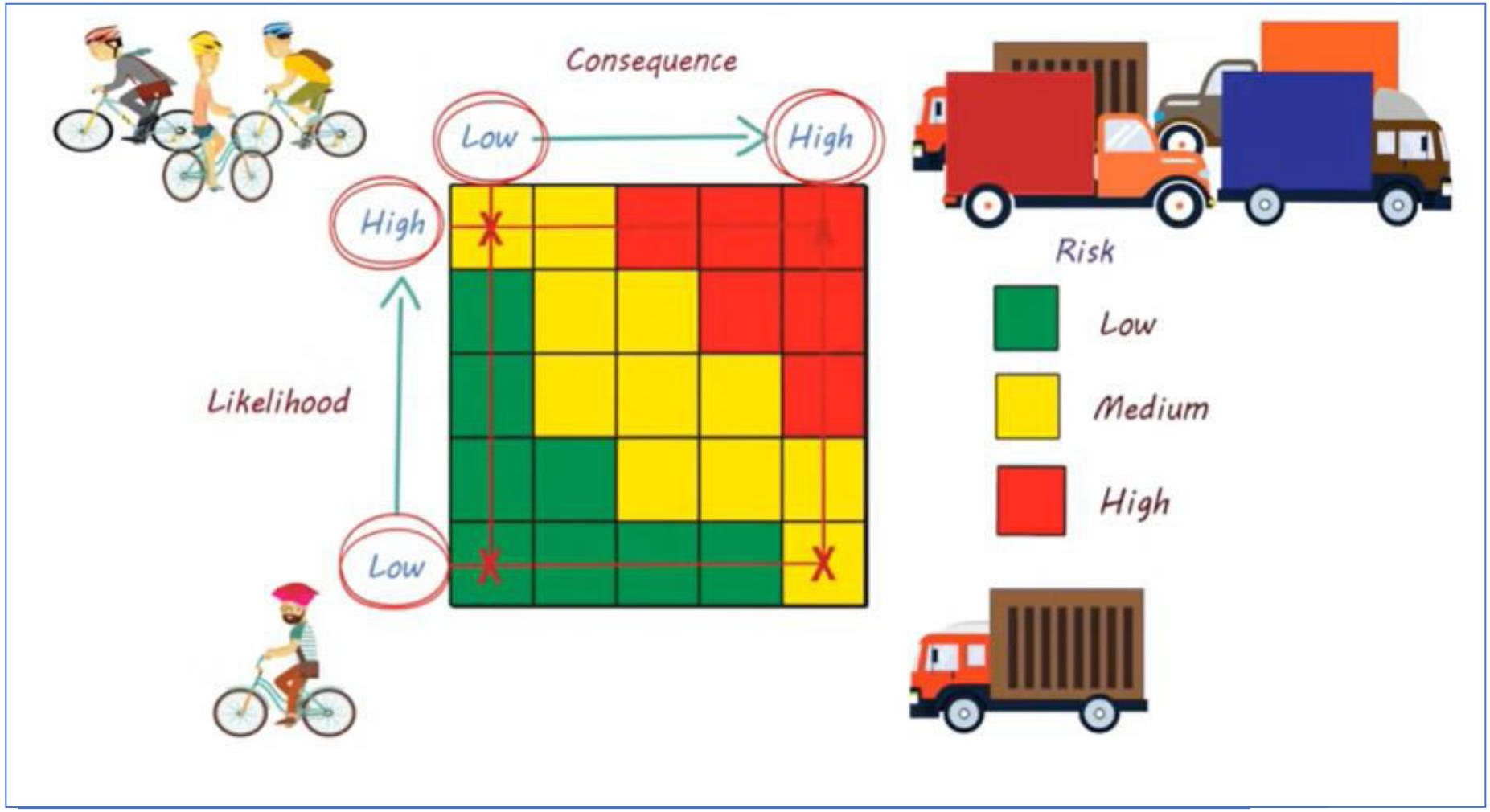
Risk=Probability x Severability

Chapter 1: Risk Assessment



Chapter 1: Risk Assessment Matrix

A simple way to measure risk using risk matrix



Chapter 1: Risk Assessment Matrix

Likelihood	Consequence: Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Risk=Likelihood x Consequence

Chapter 1: Risk Assessment

Definition of Some Key Terms

- **Vulnerability**: A weakness that can be exploited
- **Threat**: One who exploits a vulnerability
- **Risk**: Damage caused by exploiting
- **Asset**: Which needs to be accessed
- **Bug**: Error, fault or flaw in a compute
- **Hacker**: Gains access with or without
- **Cracker**: Gains access to damage

Chapter 1: Risk Assessments Elements

1) Risk Identify

To identify Risk we need the know the following

a) Assets (ex: Hardware, software, peoples…)

b) Threats (virus, experts leaving job, disaster, fire.. etc)

c) Vulnerability (No anit-virus, No fire extinguisher

2) Risk Owner

Who is responsible for what risk. Ex> The software risk owner might be the admin.

3) Risk Assessment

i) Determine the impact of risk

ii) Determine likelihood of risk

Data for Risk Assessment Table

Asset	Owner	Threat	Vulnerability	Impact	Likelihood	Risk
Server	Admin	Electricity failure	No UPS/IPS	4	1	4
Contract	MD	Unauthorized access	It is in table	4	4	16

End Chapter 1