RISK MANAGEMENT

Information Assurance and Security

Risk Management

- Elements and Categories of Risk
- Risk Monitoring and Response
- Incident Handling and Documentation
- Backup and Recovery

RECITATION

Choose one and explain why

PS5

iPhone 13 Pro Max

HEALTH CARD

ELEMENTS AND CATEGORIES OF RISKS

What is Risk Management?

What is Cybersecurity Risk Management?

RISK MANAGEMENT

It refers to the practice of identifying potential risks in advance, analyzing them and taking precautionary steps to reduce the risk


INSURANCE


LIFE INSURANCE


1 2 3
4 5 6
7 8 9
* 0 #

CYBERSECURITY RISK MANAGEMENT

It rely on the strategies, technologies, and user education to protect an enterprise against cybersecurity attacks

ELEMENTS AND CATEGORIES OF RISKS

Basic Steps of Risk Assessment

http://www.nits.ac.in/tnp/placement-procedure

Characterize the System

Identify Threats

Determine Inherent Risk & Impact

Analyze the Control Environment

Determine a Likelihood Rating

Calculate the Risk Rating

CHARACTERIZE THE SYSTEM

(Process, Function, Application)

WHAT IS IT?

WHAT KIND OF DATA DOES IT USED?

WHAT IS THE DATA FLOW?

WHO IS THE VENDOR

WHO USES THE SYSTEM

WHERE DOES THE INFORMATION GO?

IDENTIFY THE THREATS

UNAUTHORIZED ACCESS

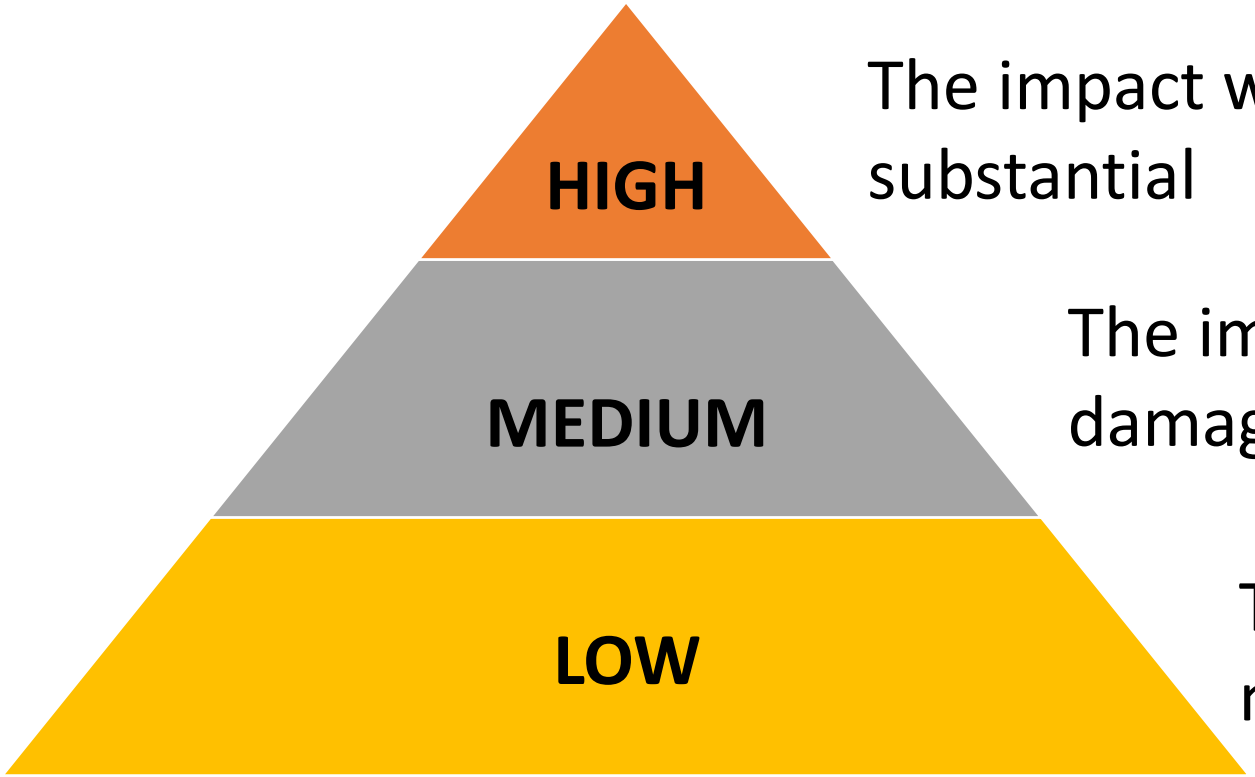
MISUSE OF INFORMATION

DATA LEAKAGE

LOSS OF DATA

DISRUPTION OF SERVICE OR PRODUCTIVITY

DETERMINE INHERENT RISK AND IMPACT



The impact would be substantial

The impact would be damaging but recoverable

The impact would be minimal or non-existent

ANALYZE THE CONTROL ENVIRONMENT

A comprehensive set of actions taken by management that set the tone for how employees engage in their day-to-day activities

USER PROVISION CONTROL

It ensures that user accounts are created, given permissions, changed, disabled and deleted

RISK MANAGEMENT CONTROL

Set of methods by which firm evaluate potential losses and take action to reduce or eliminate such threats

ADMINISTRATION CONTROLS

It establishes policies and procedure to lower the risk.

(Eg. Training, Restricting access, posting hazard signs)

USER AUTHENTICATION CONTROL

It determines the user identity according to credentials.

(Eg. Username and Password)

INFRASTRUCTURE DATA PROTECTION CONTROL

It is to safeguard sensitive and important information or to have a countermeasure against its unauthorized use

(Eg. Security Audit, Anti-Virus, Spam Solution)

DATA CENTER PHYSICAL AND ENVIRONMENTAL SECURITY

Measures taken to protect systems, buildings, and related supporting infrastructure against threats

(Eg. Access control, Surveillance)

Control Assessment Categories

- Satisfactory
- Satisfactory with Recommendations
- Needs Improvement
- Inadequate

DETERMINE A LIKELIHOOD RATING

The frequency or a probability value of a risk or threat

Occurrence Value (OV)		Probability of Occurrence	
Rating	**Value**	**Percent**	**Description**
Not Present	0	0%	Item/operation is not present in laboratory.
Rare	1	1–10%	Rare
Possible	2	10–50%	Possible
Likely	3	50–90%	Likely
Almost Certain to Certain	4	90–100%	Almost Certain to Certain

CALCULATE THE RISK RATING

It will determine whether or not it is safe enough to continue with the work or whether you need to adopt additional control measure to reduce or eliminate the risk

RISK RATING = IMPACT * LIKELIHOOD

Categories of Cybersecurity Risk

Strategic Risk

Reputational Risk

Operational Risk

Categories of Cybersecurity Risk

Transactional Risk

Compliance Risk

Five (5) Categories to a Cybersecurity Risk Assessment

- **Strategic risk** is related to adverse business decisions or the failure to implement appropriate business decisions in a manner that is consistent with the institution's strategic goals.
- **Reputational risk** is related to negative public opinion.
- **Operational risk** is related to loss resulting from inadequate or failed internal processes, people, and systems or external events.
- **Transactional risk** is related to problems with service or product delivery.
- **Compliance risk** is related to violations of laws, rules, or regulations, or noncompliance with internal policies or procedures or business standards.

Monitoring of

CYBER RISK MANAGEMENT

Executive and board-level is involve to set the tone and priorities around cyber risk as part of the organization’s larger business risk management program.

FUNCTIONAL AREAS FOR TRANSORMATION:

Alignment – refers to the whole organization

Data – It support business event detection

Analytics – It transform from an indicator-driven approach to a pattern-detection approach

Talent – A talent-model to enable evolution from reactive to proactive action model

ADDRESSING THE ALARMING

LEVEL OF CYBER RISK

1. Start by understanding and addressing common pitfalls

Delegating problem to IT/CISO

Throwing Resources at the Problem

Treating the problem as a compliance issue

Other reasons cybersecurity often breaks down:

- They does not have an inventory of the company's digital assets
- Does not identify who is most likely to come after its data
- Does not resolve system vulnerabilities
- No security plans
- Employees are not oriented or trained

2. Device a more proactive, collaborative approach

- Treat it as a risk management issue
- Addresses within a business context
- Calls for adaptive defenses
- Calls for collaborative governance

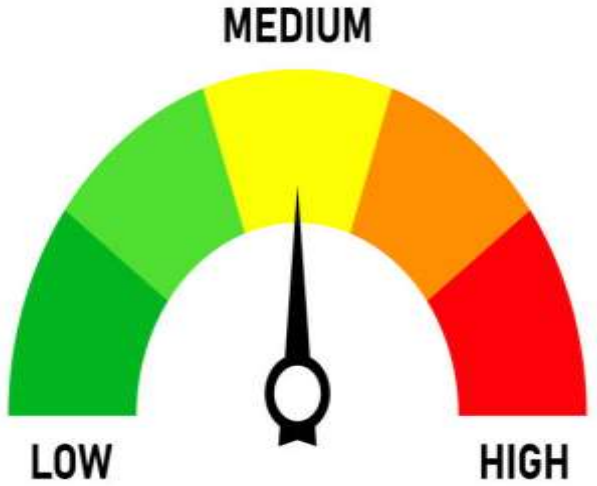
Security Incident Management

The process of identifying, managing, recording, and analyzing security threats or incident in real-time

PROCESS FOR SECURITY INCIDENT HANDLING

Prepare for handling incidents

Identify potential incidents through documents



Assess identified incidents

PROCESS FOR SECURITY INCIDENT HANDLING

Respond to the incident by containing, investigating, and resolving it

Learn and document key takeaways from every incidents

Best practices for

SECURITY INCIDENT MANAGEMENT

1. Develop a security incident management plan and supporting policies
2. Establish an incident response team
3. Develop a comprehensive training program
4. Perform a post-incident analysis to learn from your success and failures

INCIDENT DOCUMENTATION

Documenting all workplace injuries, near misses and accidents and it should be completed at the time an incident occurs.

What is considered an accident?

- It causes interference to an organization
- It causes significant risk that could affect members within organization
- It impacts on the systems and operation of workplaces
- It attracts negative media attention

Response plan includes:

- Mission
- Strategies and Goals
- Organization approach to incident response
- How will the incident response team communicate with the rest of the organization

Response plan includes:

- Metrics for measuring the incident response and its effectivity
- Roadmap for maturing the incident response capability
- How does the program fit into the overall organization