Introduction to Cybersecurity

Course Incharge: **Yahya Batla**

Course Instructor: **Instructor_Name**

What is Risk?

A risk is the **potential for loss** when the threat happens.

This measure is the combination of the likelihood that a threat exploits a vulnerability and the scale of harmful consequences.

What is Risk?

Risk = Probability that a threat occur x Cost to the asset owner

	COST TO THE ASSET OWNER		
	LOW	MEDIUM	HIGH
HIGH	MEDIUM RISK	HIGH RISK	HIGHEST RISK
MEDIUM	LOW RISK	MEDIUM RISK	HIGH RISK
LOW	LOWEST RISK	LOW RISK	MEDIUM RISK

What is Risk?


Threat
A new incident with potential to harm a system
Vulnerability
Known weakness that hackers could exploit
Risk
The potential for damage when a threat exploits a vulnerability

What is Risk?

Threats

- Angry Employees
- Dishonest Employees
- Criminals
- Governments
- Terrorists
- The Press
- Competitors
- Hackers
- Nature

Vulnerabilities

- Software Bugs
- Broken Processes
- Ineffective Controls
- Hardware Flaws
- Business Change
- Legacy Systems
- Inadequate BCP
- Human Error

Risk

- Business Disruption
- Financial Loss
- Loss of Privacy
- Damage to Reputation
- Loss of Confidence
- Legal Penalties
- Impaired Growth
- Loss of Life

Risk Management Stages

Identifying risk – evaluating the organization's environment to identify current or potential risks that could affect business operations

Assess risk – analyzing identified risks to see how likely they are to impact the organization, and what the impact could be

Control risk – define methods, procedures, technologies, or other measures that can help the organization mitigate the risks.

Review controls – evaluating, on an ongoing basis, how effective controls are at mitigating risks, and adding or adjusting controls as needed.

For further study:
https://hyperproof.io/resource/cybersecurity-risk-management-process/

Risk Identification

Gartner defines IT risk as "**the potential for an unplanned, negative business outcome involving the failure or misuse of IT.**"

Risk identification is the first step in the management process.

When you're looking to identify risk, you **must start by understanding threats, vulnerabilities, and the consequences of their convergence.**

Threats are circumstances or events with the potential to negatively affect an organization's operations or assets through unauthorized access of information systems.

Vulnerabilities can be defined as weaknesses in an information system, security procedure, internal control, or implementation that can be exploited by a threat source.

Consequences can best be defined as the adverse results that occur when threats exploit vulnerabilities.

Risk Assessment

1. Assessment is the all-important step when the answer becomes clear for “What is your organization’s level of risk?”
2. Start by naming all assets and prioritizing their importance.
3. Next, identify all possible threats and vulnerabilities in your environment. At this point, address all known vulnerabilities with appropriate controls.
4. Next, attempt to determine the likelihood of a threat event occurring and conduct an “impact analysis” to estimate its potential consequences and cost impact.

Control Risk

The all-important third step of response starts by understanding all your options for risk mitigation — you can employ either technological or best practice methods, ideally a combination of both

Review Controls

Your organization will want to monitor:

Regulatory Change - Staying abreast of all regulations and their shifts will ensure your internal controls align with outside expectations.

Vendor Risk - Be sure to assess and document security and compliance controls as new vendors are on board.

Internal IT Usage - Know what technology your internal teams use and how they it to stay ahead of potential gaps.

Monitor Security Controls – Be aware of the functionality of different types of security controls the organization has implemented and their efficiency against the emerging risks.

Business Continuity Plan

The intent of a business continuity plan is to sustain business operations while recovering from a significant disruption. An event has created a disturbance in the environment, and now you need to know how to maintain the business.

Business Continuity Plan

A key part of the plan is communication, including multiple contact methodologies and backup numbers in case of a disruption of power or communications. Many organizations will establish a phone tree, so that if one person is not available, they know who else to call. Organizations will go through their procedures and checklists to make sure they know exactly who is responsible for which action. No matter how many times they have flown, without fail, pilots go through a checklist before take-off. Similarly, there must be established procedures and a thorough checklist, so that no vital element of business continuity will be missed.

Read: https://www.qmsuk.com/news/what-are-the-5-key-components-of-a-business-continuity-plan

Components of BCP

Here are some common components of a comprehensive business continuity plan:

1. List of the BCP team members, including multiple contact methods and backup members
2. Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)
3. Notification systems and call trees for alerting personnel that the BCP is being enacted
4. Guidance for management, including designation of authority for specific managers
5. How/when to enact the plan
6. Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

Disaster Recovery

A Disaster Recovery Plan (DR or DRP) is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber attacks and any other disruptive events.

Phases of Disaster Recovery

Phases of Disaster Recovery

Prevention: Prevention focuses on preventing hazards from occurring, whether they are natural, technological or caused by humans. Not all hazards are preventable, but the risk of loss of life and injury can be limited with good evacuation plans, environmental planning and design standards.

Mitigation: This phase includes actions taken to prevent or reduce the cause, impact, and consequences of disasters. Examples of hazard mitigation include:

1. Tying down homes or barns with ground anchors to withstand wind damage
2. Digging water channels to redirect water and planting vegetation to absorb water
3. Reinforcing fencing to prevent animal escapes
4. Buying insurance policies

Phases of Disaster Recovery

Preparedness: This phase includes planning, training, and educational activities for events that cannot be mitigated. Examples include:

1. Developing disaster preparedness plans for what to do, where to go, or who to call for help in a disaster
2. Exercising plans through drills, tabletop exercises, and full-scale exercises
3. Creating a supply list of items that are useful in a disaster
4. Walking around and identifying possible vulnerabilities.

Phases of Disaster Recovery

Response: The response phase occurs in the immediate aftermath of a disaster. During the response phase, business and other operations do not function normally. Personal safety and wellbeing in an emergency and the duration of the response phase depend on the level of preparedness. Examples of response activities include:

Implementing disaster response plans

Conducting search and rescue missions

Taking actions to protect yourself, your colleagues and others

Addressing public perceptions about food safety

Phases of Disaster Recovery

Recovery: During the recovery period, restoration efforts occur concurrently with regular operations and activities. The recovery period from a disaster can be prolonged. Examples of recovery activities include:

Rebuilding damaged structures based on advanced knowledge obtained from the preceding disaster

Preventing or reducing stress-related illnesses and excessive financial burdens

Reducing vulnerability to future disasters

Principal Causes of Disasters

Natural Disasters

- Rain & Windstorm
- Floods
- Biological Agents (insect or vermin infestation)
- Earthquakes
- Volcanic Eruptions

Man-Made Disasters

- Acts of War or Terrorism
- Fires
- Water (Leaking Roofs or Broken Pipes)
- Explosions
- Liquid Chemical Spills
- Building Deficiencies
- Power Failures

Benefits of Disaster Recovery Plan

Stronger business continuity

Every second counts when your business goes offline, impacting productivity, customer experience, and your company's reputation. Disaster recovery helps safeguard critical business operations by ensuring they can recover with minimal or no interruption.

Enhanced security

DR plans use data backup and other procedures that strengthen your security posture and limit the impact of attacks and other security risks. For example, cloud-based disaster recovery solutions offer built-in security capabilities, such as advanced encryption, identity and access management, and organizational policy.

Faster recovery

Disaster recovery solutions make restoring your data and workloads easier so you can get business operations back online quickly after a catastrophic event. DR plans leverage data replication and often rely on automated recovery to minimize downtime and data loss.

Benefits of Disaster Recovery Plan

Reduced recovery costs

The monetary impacts of a disaster event can be significant, ranging from loss of business and productivity to data privacy penalties to ransoms. With disaster recovery, you can avoid, or at least minimize, some of these costs. Cloud DR processes can also reduce the operating costs of running and maintaining a secondary location.

High availability

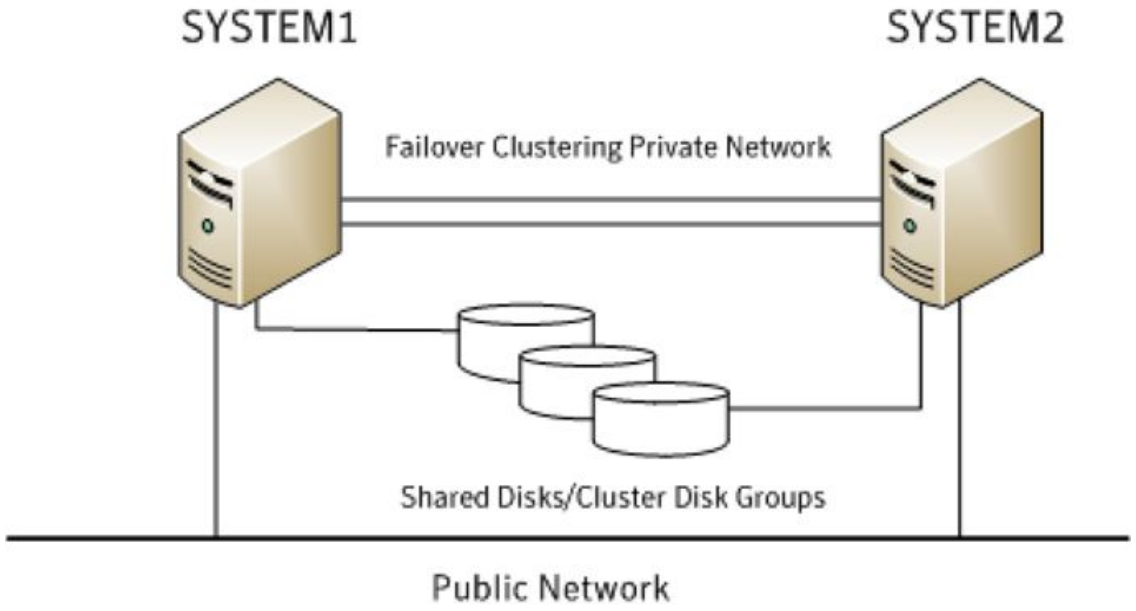
HA capabilities help ensure an agreed level of performance and offer built-in redundancy and automatic failover, protecting data against equipment failure and other smaller-scale events that may impact data availability.

Better compliance

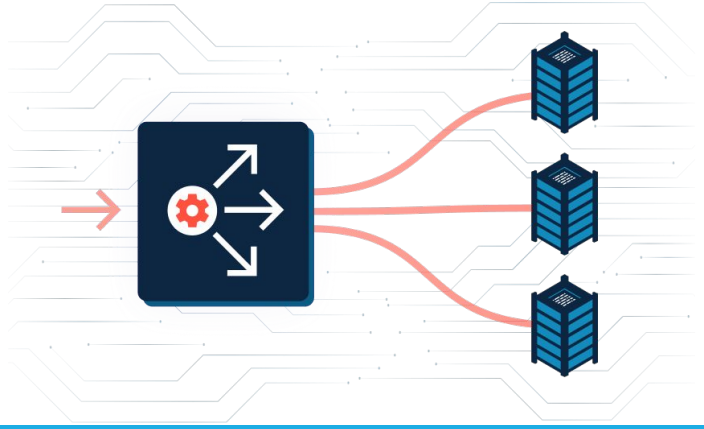
DR planning supports compliance requirements by considering potential risks and defining a set of specific procedures and protections for your data and workloads in the event of a disaster. This usually includes strong data backup practices, DR sites, and regularly testing your DR plan to ensure that your organization is prepared.

High Availability and Load Balancing

High Availability(HA) means that an IT system, component, or application can operate at a high level, continuously, without intervention, for a given time period.



Load Balancing is the method of distributing network traffic equally across a pool of resources that support an application.



Advantages of High Availability

- Protection from Downtime
- Save Lost Revenue
- Simplify Maintenance
- Maximum Flexibility
- Improve Resilience & Agility

High Availability Advantages

1. **Protection from downtime :** If one system fails (i.e. Server, LAN Switch, Router or Firewall), HA solutions allow you to seamlessly migrate operations over to another system. This way, client relations can still be maintained, employees can continue getting their work done, and downtime can't cripple critical business functioning.

2. **Saves you from lost revenue:** The faster you get your system back up and running, the faster you can get back to business as usual.

3. **Simplify maintenance:** Unplanned downtime from a disaster isn't the only type of downtime that companies face. Hardware and software updates or upgrades are other instances where companies can face costly downtime. With HA solutions, this downtime can be minimized.

High Availability Advantages

4. **Maximum flexibility:** Does your production site need to be available and secure 24/7? Only HA solutions can provide this level of flexibility. As soon as the main production site is back up and running, the failover site can be seamlessly switched off and transfer any changes that occurred back to production servers while the main site was offline.

5. **Improve resilience and agility:** While DR solutions are essential, these can take hours to coordinate. With HA solutions, it takes only seconds to switch over to the failover center and run production from there. It's all customized to your specifications. You can specify how quickly you want your data replicated, so the version that you're running at the host site is almost identical to the version of the server that went offline.

Advantages of Load Balancing

- Improved Performance
- Enhanced Availability
- Reduced Downtime
- Improved User Experience
- Increased Scalability
- Improved Security
- Enhanced Resilience
- Better Support for Microservices
- Better Resource Utilization
- Enhanced Observability

Load Balancing Advantages

1. **Improved performance:** Load balancing can distribute incoming traffic evenly across multiple resources, which can help improve a system's overall performance. This can reduce response times and improve the user experience.

2. **Enhanced availability:** Load balancing can help to ensure that a system remains available, even if individual servers or resources fail. By automatically redirecting traffic away from failed servers or resources, load balancing can help to keep a system running smoothly.

3. **Increased scalability:** Load balancing allows teams to scale their systems horizontally, by adding more servers or resources to the load balancer. This can help to ensure that a system can handle increased traffic or workloads, and it can support growth and expansion.

Load Balancing Advantages

4. **Improved security:** Load balancing can provide additional security features such as encryption, authentication, and access control, which can help to protect your systems and data.

5. **Better resource utilization:** By distributing traffic evenly across multiple resources, load balancing can help to ensure that resources are used efficiently and effectively.

6. **Reduced downtime:** By automatically redirecting traffic away from failed servers or resources, load balancing can help to reduce downtime and improve the overall availability of a system.

7. **Improved user experience:** Load balancing can improve the performance of a system, which can lead to a better user experience. This can be particularly important for applications that are used by a large number of users, or that are critical to the operation of a business.

Load Balancing Advantages

8. **Enhanced resilience:** Load balancing can help to make a system more resilient to failures and other issues, by automatically redirecting traffic away from failed servers or resources.

9. **Better support for microservices:** It is well-suited to microservices architectures, where multiple services are communicating with each other to perform a task. It can help to distribute traffic evenly across the services in a microservices architecture.

10. **Enhanced observability:** Load balancing can provide valuable insights into the performance and behavior of a system, which can help teams to improve observability and to better understand the state of their systems.

THANK YOU