Unit-2: Incident Management

Incident Prioritization

- What is incident ?
- How to manage a incident?
- Need of incident prioritization
- Incident Prioritization matrix

An incident is an event or occurrence, often unexpected, that may have a significant impact or consequences. Incidents can be positive or negative and can take place in various contexts, such as in the workplace, in public spaces, or in personal life. In some cases, incidents may require immediate attention and response to mitigate their effects, while in other cases they may simply be recorded for future reference or analysis. Examples of incidents include accidents, emergencies, security breaches, or violations of laws or regulations.

CASE-1 – held on 3-3-2023, presented/discussed in class on 5-3-2023

How to manage an incident ?

GlobalSign by GMO

Even in the early days of 2023, we have already seen Royal Mail become the victim of a severe cyber attack which has resulted in exceptional delays to its overseas operations. In a bitter twist of irony, towards the end of 2022, hackers had stolen sensitive information from the secure online password management provider, LastPass. It's believed that this LastPass hack affected 30 million users, whose IP addresses, email addresses, phone numbers and usernames were compromised.

If these organisations can be hacked, what does that mean for businesses that don't have as well-defined or structured cybersecurity procedures in place?

Case -2

Case- 3

15 hrs ·

Friends! Thanks for giving me courage. 3 hour ago I cut the vain of left hand, fortunately not so much bleeding. It is true that I lost fighting spirit but regained. Thanks Kunal sir and Indrani for boosting my morale. Please don't worry. I am OK. It is true that Samsung, Banglore harrashing me to that extent which I cannot accept.

Like · Comment · Share

3 people like this.

Incident Prioritization

Incident prioritization is the process of assigning a priority level to incidents based on their impact and urgency. Incident prioritization is crucial because it helps organizations determine the order in which incidents should be addressed and resolved.

Here are some key reasons why incident prioritization is important:

- **Focus resources on high-priority incidents**: Incident prioritization helps organizations focus their limited resources on resolving high-priority incidents that have the greatest impact on the business.

- **Improve response time**: By prioritizing incidents, organizations can ensure that the most critical incidents are addressed and resolved quickly, reducing downtime and minimizing the impact on customers, users, and the business.

- **Align with business objectives**: Incident prioritization allows organizations to align their incident response efforts with their business objectives, ensuring that they are addressing incidents that have the greatest impact on the business.

- **Optimize resource allocation**: Incident prioritization helps organizations optimize their resource allocation by identifying the incidents that require the most attention and resources.

- **Ensure consistency**: By using a standardized prioritization process, organizations can ensure consistency in their incident response efforts and avoid confusion or miscommunication among incident responders.

Incident prioritization matrix

Incident Priority Matrix					
	Impact				
Urgency		Organization	Department	Small Group or VIP	Individual
	Core Business Services	1	1	3	4
	Support Services	2	2	3	4
	Non-Urgent Services	2	3	4	5
	Inconvenienced	3	4	4	5

Eg:

Getting a Job, having salary>80,000 pm

Process management using centralized portal

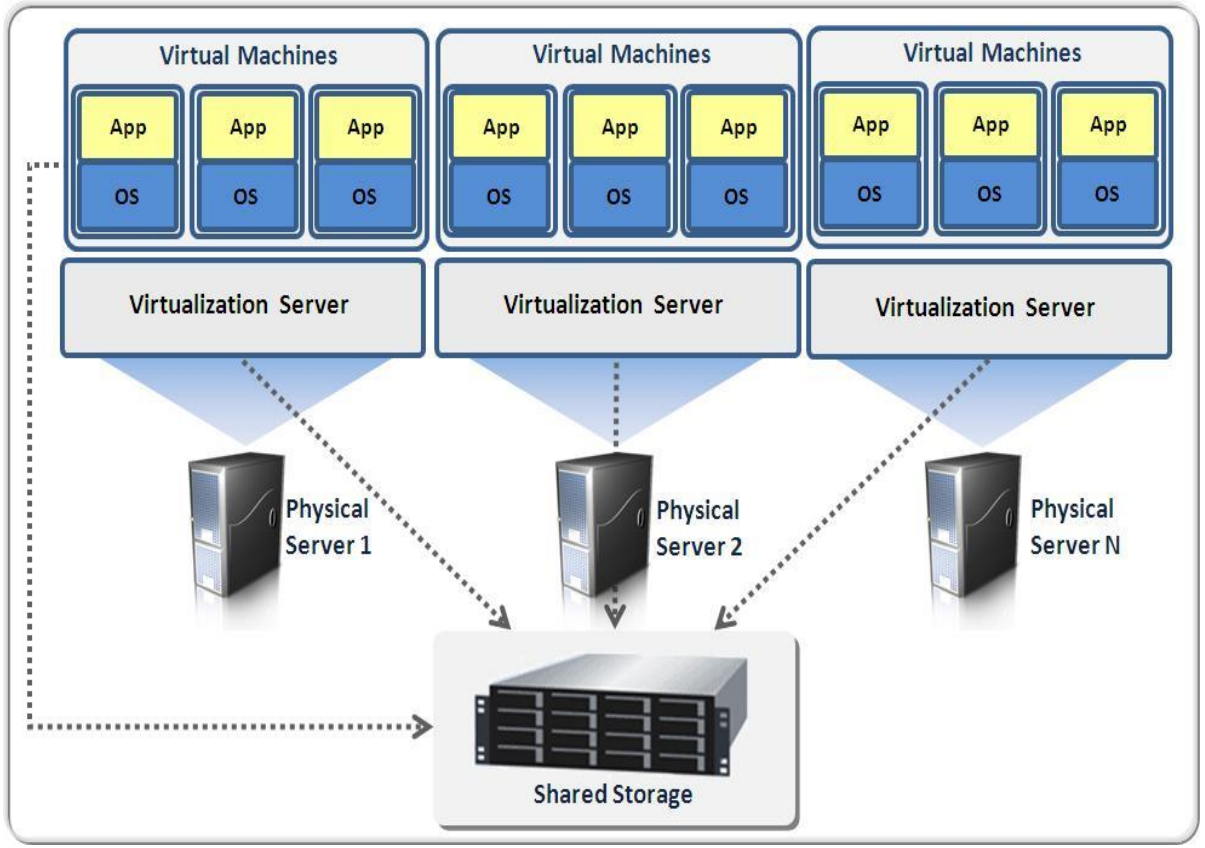
		Impact		
		HIGH	MID	LOW
Urgency	HIGH	1	2	3
	MID	2	3	4
	LOW	3	4	5

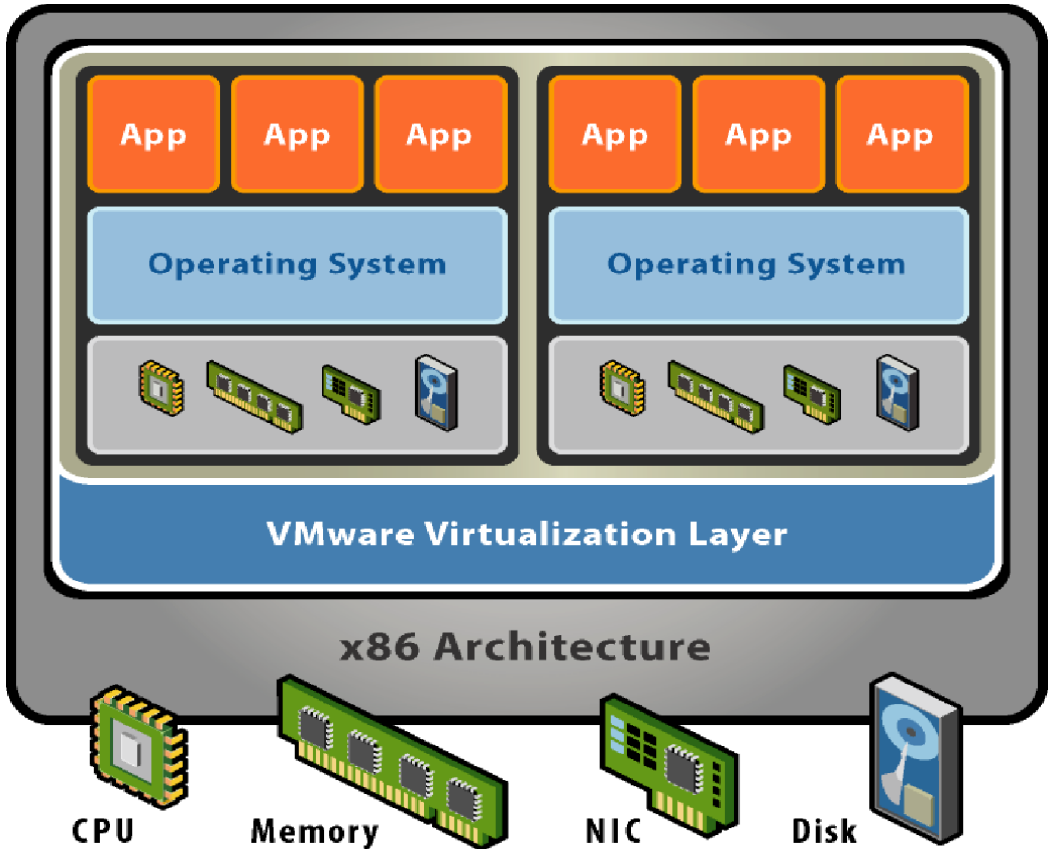
Disaster Recovery Technologies

Disaster recovery technologies are systems and tools that are designed to help organizations recover their critical IT systems and data after a disruptive event such as a natural disaster, cyber-attack, or hardware failure. Disaster recovery technologies can include a range of different tools and strategies, including:

- **Data backup and recovery**: This involves regularly backing up data to an off-site location and being able to restore that data quickly in the event of a disaster.
- **Replication**: This involves replicating critical systems and data to a secondary location so that they can be quickly activated in the event of a disaster.
- **Virtualization**: This involves creating virtualized copies of critical systems and data, which can be rapidly deployed in the event of a disaster.
- **Cloud-based disaster recovery**: This involves leveraging cloud infrastructure to replicate critical systems and data to a secondary location for rapid recovery.
- **High availability**: This involves designing systems with redundant components to minimize the risk of downtime in the event of a failure.
- **Disaster recovery testing**: This involves regularly testing disaster recovery plans and technologies to ensure they are effective and can be implemented quickly in the event of a disaster.

Impact of Virtualization on Incident Response and Handling





Impact of Virtualization on Incident Response and Handling

Virtualization can have a significant impact on incident response and handling in several ways:

- **Rapid provisioning**: Virtualization allows for the rapid provisioning of virtual machines, which can be used for testing, development, and backup purposes. This can help incident response teams quickly set up test environments to investigate and analyze incidents.
- **Isolation**: Virtualization enables the creation of isolated virtual environments, which can be used to contain and isolate incidents from spreading to other parts of the system. This allows incident response teams to isolate and investigate incidents without affecting other parts of the system.
- **Snapshots**: Virtualization allows for the creation of snapshots, which are point-in-time copies of a virtual machine. Snapshots can be used for backup and recovery purposes or to quickly revert to a known-good state in the event of an incident.
- **Centralized management**: Virtualization allows for the centralized management of virtual machines, making it easier for incident response teams to manage and monitor their systems.
- **Agility**: Virtualization provides agility and flexibility to incident response teams, allowing them to quickly spin up virtual machines, test environments, and other resources as needed to respond to incidents.

Estimating Cost of an Incident

Type of Incident	Description [computer incidents]
Malware	Software that is designed to harm or exploit a computer system or network. Includes viruses, trojans, worms, and ransomware.
Phishing	Attempting to deceive users into providing sensitive information, such as login credentials or financial information, by impersonating a trustworthy entity.
Denial of Service (DoS)	Overloading a system or network with traffic or requests to prevent legitimate users from accessing it.
Data Breach	Unauthorized access to sensitive or confidential information, such as personal or financial data.
Insider Threat	Malicious or unintentional actions by an authorized user that result in harm to the system or network.
Social Engineering	Manipulating users into divulging sensitive information or performing actions that compromise security.
Password Attack	Attempting to guess or steal passwords to gain unauthorized access to a system or network.
Physical Security	Unauthorized access to a physical device, such as stealing a laptop or breaking into a server room.
Software Vulnerabilities	Exploiting weaknesses or flaws in software to gain unauthorized access or execute malicious code.
Misconfiguration	Misconfigured settings or security controls that leave a system or network vulnerable to attack.

Type of Incident	Description (general incidents)
Physical Security	An incident that involves unauthorized access or theft of physical assets, such as computers, servers, or other hardware.
Cybersecurity	An incident that involves the unauthorized access or theft of digital assets, such as sensitive data, login credentials, or financial information.
Human Error	An incident caused by human mistakes or oversight, such as accidentally deleting important data or misconfiguring a system.
Natural Disaster	An incident caused by natural events, such as earthquakes, floods, or hurricanes, that disrupts normal business operations.
Technical Failure	An incident caused by hardware or software failure, such as a server crash or software malfunction.
Malicious Activity	An incident caused by intentional and malicious actions, such as hacking, cyber espionage, or cyber terrorism.
Supply Chain	An incident that occurs when a supplier or vendor's product or service is compromised, potentially impacting an organization's own security.
Compliance	An incident that arises from non-compliance with regulatory or legal requirements, such as failure to adhere to data protection laws or industry-specific regulations.
Service Interruption	An incident that causes a disruption or outage to a service, such as a website or application, resulting in loss of access or revenue.
Physical Safety	An incident that involves the physical safety or well-being of individuals, such as workplace accidents or violent incidents.

Estimating Cost of an Incident

general steps you can follow to estimate the cost of an incident:

- **Identify the scope of the incident**: The first step is to determine the extent of the incident and its impact on your organization. This will help you understand the potential areas of financial loss.
- **Identify the direct costs**: Direct costs are the expenses that can be attributed directly to the incident, such as lost productivity, equipment damage, legal fees, and medical expenses. These costs are relatively easy to identify and quantify.
- **Identify the indirect costs**: Indirect costs are the expenses that are not directly related to the incident but are still affected by it. These costs may include loss of business reputation, customer dissatisfaction, and employee turnover.
- **Estimate the total cost**: Once you have identified the direct and indirect costs, you can estimate the total cost of the incident by adding them together.
- **Consider the potential future costs**: Depending on the nature of the incident, there may be additional costs to consider in the future. For example, if the incident results in a lawsuit, there may be ongoing legal fees to consider.
- **Update your incident response plan**: After estimating the cost of the incident, you can update your incident response plan to help mitigate the risk of future incidents and reduce the potential cost of any future incidents.

Let's consider **an example of a cyber attack** on a company's computer network.

Direct costs:

IT Forensic investigation to identify the cause and extent of the attack: $10,000
IT repair and recovery costs to restore the network: $50,000
Legal and regulatory compliance costs: $20,000
Notification and credit monitoring for affected customers: $30,000

Indirect costs:

Loss of productivity due to network downtime: $100,000
Reputation damage and loss of customer trust: $50,000
Ongoing security upgrades to prevent future attacks: $25,000
Total cost:
Direct costs: $110,000
Indirect costs: $175,000
Total cost: $285,000

In this example, the total cost of the incident is estimated to be $285,000. It is important to note that this is only an estimate, and the actual cost could be higher or lower depending on the specific circumstances of the incident.

let's consider **another example of a physical security breach** at a retail store.

Direct costs:

Replacement of damaged security equipment: $5,000
Replacement of stolen merchandise: $15,000
Hiring additional security personnel: $10,000
Investigation costs: $8,000
Indirect costs:

Loss of revenue due to store closure for investigation and repairs: $20,000
Customer dissatisfaction due to security breach: $5,000
Damage to brand reputation: $15,000

Total cost:
Direct costs: $38,000
Indirect costs: $40,000
Total cost: $78,000

In this example, the total cost of the incident is estimated to be $78,000. Again, this is only an estimate and the actual cost could be higher or lower depending on the specific circumstances of the incident.

consider **another example of an employee accident** in a manufacturing facility.

Direct costs:

Medical expenses for injured employee: $20,000
Repair or replacement of damaged equipment: $10,000
OSHA fines and penalties: $15,000
Indirect costs:

Lost productivity due to downtime and investigation: $25,000
Increased workers' compensation insurance premiums: $7,000
Cost of hiring and training a replacement employee: $10,000

Total cost:
Direct costs: $45,000
Indirect costs: $42,000
Total cost: $87,000

In this example, the total cost of the incident is estimated to be $87,000. As with the previous examples, this is only an estimate, and the actual cost could be higher or lower depending on the specific circumstances of the incident.

Incident Reporting

Incident reporting is a critical aspect of incident management, which involves reporting any adverse event or security incident that has occurred in an organization. Incident reporting is necessary to ensure that the organization can take appropriate measures to prevent similar incidents from happening again in the future.

Here are **some key steps for effective incident reporting**:

- **Define incident reporting procedures**: Establish a clear and concise set of incident reporting procedures, including who should report incidents, how they should be reported, and the timeline for reporting.

- **Train employees**: Provide training to all employees on incident reporting procedures, including how to identify potential incidents, how to report them, and what information needs to be included in the report.

- **Use a standardized incident reporting form**: Use a standardized incident reporting form to ensure that all relevant information is captured consistently across different incidents. The form should include details such as the date and time of the incident, a description of what happened, the location of the incident, and any witnesses or other involved parties.

Incident Reporting

- **Ensure confidentiality**: Ensure that all incident reports are kept confidential to prevent retaliation or discrimination against the employee reporting the incident.

- **Evaluate incidents**: Once an incident is reported, evaluate it to determine the severity, potential impact, and necessary response. This will help to identify areas where improvements can be made to prevent future incidents.

- **Learn from incidents**: Use incident reports as an opportunity to learn from mistakes and improve incident response procedures, training programs, and risk management strategies.

- **Keep records**: Maintain a centralized incident reporting database or system to track incidents, monitor trends, and support data analysis and reporting.

By following these steps, organizations can ensure that they have a comprehensive and effective incident reporting process in place, which will help them to respond to incidents quickly and efficiently, minimize the impact of incidents, and prevent similar incidents from happening again in the future.

Incident Reporting organizations

Here are some incident reporting organizations:

- National Highway Traffic Safety Administration (NHTSA) - responsible for reporting incidents related to motor vehicles and traffic safety.
- Consumer Product Safety Commission (CPSC) - responsible for reporting incidents related to consumer products such as toys, electronics, and household appliances.
- Food and Drug Administration (FDA) - responsible for reporting incidents related to food and drug safety.
- Occupational Safety and Health Administration (OSHA) - responsible for reporting incidents related to workplace safety.
- Federal Aviation Administration (FAA) - responsible for reporting incidents related to aviation safety.

- National Transportation Safety Board (NTSB) - responsible for reporting incidents related to transportation safety, including aviation, railroad, and marine incidents.
- Environmental Protection Agency (EPA) - responsible for reporting incidents related to environmental safety and pollution.
- Cybersecurity and Infrastructure Security Agency (CISA) - responsible for reporting incidents related to cybersecurity threats and infrastructure safety.
- Federal Emergency Management Agency (FEMA) - responsible for reporting incidents related to natural disasters and emergency management.
- United States Coast Guard (USCG) - responsible for reporting incidents related to maritime safety and security.

Vulnerability Resources

Here are some useful resources for vulnerability information:

- National Vulnerability Database (NVD) - The NVD is a U.S. government repository of standards-based vulnerability management data, including information on vulnerabilities and patches.
- Common Vulnerabilities and Exposures (CVE) - CVE is a dictionary of publicly disclosed cybersecurity vulnerabilities and exposures.
- Open Web Application Security Project (OWASP) - OWASP is a nonprofit organization dedicated to improving software security. Its website includes information on web application vulnerabilities and mitigation techniques.
- National Institute of Standards and Technology (NIST) - NIST provides cybersecurity guidance and best practices, including the Cybersecurity Framework and publications on vulnerability management.
- SecurityFocus - SecurityFocus is a comprehensive database of vulnerabilities and exploits, with additional resources such as security news and forums.

- Exploit Database - The Exploit Database is a repository of exploits and vulnerabilities for various platforms, including web applications, operating systems, and software.

- Vulnerability Lab - The Vulnerability Lab is a German-based research organization that focuses on discovering and reporting software vulnerabilities and exploits.

- Secunia Research - Secunia Research is a provider of vulnerability intelligence and security advisories, with a focus on software patching and vulnerability management.

- Zero Day Initiative (ZDI) - ZDI is a program run by Trend Micro that incentivizes researchers to discover and report zero-day vulnerabilities.

- Microsoft Security Updates - Microsoft releases regular security updates to address vulnerabilities in its software products. The Microsoft Security Bulletin website provides information on these updates and their associated vulnerabilities.

Incident Management - Process

Incident management is the process of identifying, analyzing, and resolving incidents that disrupt normal business operations. Here are the steps involved in incident management:

- **Preparation** - This step involves creating an incident response plan that outlines the roles and responsibilities of incident response team members, procedures for identifying and reporting incidents, and steps for mitigating the impact of an incident.

- **Identification** - Incidents are identified through various means, such as alerts from security monitoring systems, reports from employees or customers, or through routine system maintenance checks.

- **Categorization** - Once an incident is identified, it is categorized based on its severity and impact on business operations. This helps determine the priority level for response and the appropriate response team members to be involved.

- **Prioritization** - Prioritizing incidents involves evaluating the potential impact of an incident on business operations and assigning a priority level based on that evaluation.

- **Investigation** - During this step, incident response team members gather information about the incident, such as how it occurred and its potential impact on business operations.

- **Resolution** - The incident response team works to resolve the incident, typically by following pre-defined procedures in the incident response plan. This may involve implementing temporary workarounds to restore business operations, investigating the root cause of the incident, and implementing long-term fixes to prevent similar incidents from occurring in the future.

- **Reporting** - After the incident is resolved, a report is generated to document the incident and the steps taken to resolve it. This report is used to inform incident response planning and improve incident response processes.

- **Review and Improvement** - The incident response process is continually reviewed and improved based on lessons learned from past incidents, changes in business operations, and new threats or vulnerabilities. This helps ensure that incident response plans remain effective and up-to-date.

Incident Response Team Roles

Here are the typical roles in an incident response team and their responsibilities:

- Incident Response Manager - The incident response manager is responsible for overseeing the entire incident response process, including coordinating the activities of the incident response team, communicating with stakeholders, and providing regular updates on the incident.

- IT Security Analyst - The IT security analyst is responsible for identifying and analyzing incidents, determining the scope of the incident, and providing recommendations for mitigating the impact of the incident.

- Forensic Analyst - The forensic analyst is responsible for conducting a forensic investigation of the incident, including collecting and analyzing evidence, determining the cause of the incident, and providing recommendations for preventing future incidents.

- Network Security Engineer - The network security engineer is responsible for analyzing network traffic and logs to identify and analyze security incidents, and implementing network security controls to prevent future incidents.

- Systems Administrator - The systems administrator is responsible for managing and maintaining IT systems, identifying and remediating vulnerabilities, and restoring services following an incident.

- Communications Coordinator - The communications coordinator is responsible for communicating with stakeholders during the incident response process, including providing regular updates on the status of the incident and coordinating communications with external organizations, such as law enforcement or regulatory agencies.

- Legal Counsel - The legal counsel is responsible for providing legal guidance and support during the incident response process, including ensuring compliance with legal and regulatory requirements and managing any legal implications of the incident.

- Public Relations Specialist - The public relations specialist is responsible for managing the public image and reputation of the organization during and after an incident, including communicating with the media and managing social media accounts.

Note that the specific roles and responsibilities of an incident response team may vary depending on the size and complexity of the organization, the nature of the incident, and the industry in which the organization operates.

Incident Response Team Responsibilities

The incident response team is responsible for responding to incidents that threaten the security and availability of an organization's information systems and data. Here are the main responsibilities of an incident response team:

- **Preparation** - The incident response team is responsible for developing and maintaining an incident response plan that outlines the steps to be taken in the event of a security incident. This plan should include procedures for identifying, analyzing, containing, and mitigating security incidents.

- **Identification** - The incident response team is responsible for identifying security incidents through various means, such as alerts from security monitoring systems, reports from employees or customers, or through routine system maintenance checks.

- **Analysis** - The incident response team is responsible for analyzing security incidents to determine the scope of the incident, the type of attack, and the potential impact on the organization's systems and data.

- **Containment** - The incident response team is responsible for containing the incident to prevent further damage or loss. This may involve isolating affected systems, disabling network connections, or blocking access to compromised accounts.

- **Mitigation** - The incident response team is responsible for mitigating the impact of the incident and restoring normal business operations as quickly as possible. This may involve implementing temporary workarounds, applying security patches or updates, or restoring data from backups.

- **Reporting** - The incident response team is responsible for documenting the incident, including the steps taken to contain and mitigate the incident, and any lessons learned from the incident. This report is used to inform incident response planning and improve incident response processes.

- **Coordination** - The incident response team is responsible for coordinating with other teams within the organization, such as IT, legal, and public relations, as well as external organizations, such as law enforcement or regulatory agencies.

- **Training** - The incident response team is responsible for ensuring that all members of the organization are aware of the incident response plan and their roles and responsibilities in the event of a security incident. This may involve conducting regular training and awareness sessions.

Note that the specific responsibilities of an incident response team may vary depending on the size and complexity of the organization, the nature of the incident, and the industry in which the organization operates.

Dependencies

Dependencies refer to the relationships between different components or systems within an organization that are necessary for them to function properly. In the context of incident response, dependencies can have a significant impact on the ability of the incident response team to detect and respond to security incidents. Here are some examples of dependencies that may affect incident response:

- **Hardware and software dependencies** - Incident response teams rely on hardware and software systems to detect and respond to security incidents. These systems may be dependent on other systems or components within the organization, and any failure or disruption in these dependencies can hinder the incident response team's ability to effectively detect and respond to security incidents.

- **Network dependencies** - Incident response teams rely on network connectivity to detect and respond to security incidents. Network dependencies include switches, routers, firewalls, and other networking equipment. Any disruption in network connectivity can have a significant impact on the ability of the incident response team to detect and respond to security incidents.

- **Communication dependencies** - Incident response teams rely on effective communication channels to coordinate their response to security incidents. Communication dependencies include email, phone systems, chat applications, and other communication tools. Any disruption in these communication channels can hamper the ability of the incident response team to effectively communicate and coordinate their response.

- **Personnel dependencies** - Incident response teams rely on personnel to effectively detect and respond to security incidents. Personnel dependencies include the availability and skills of incident response team members, as well as the availability and skills of other employees who may be involved in the incident response process. Any disruption in personnel availability or skills can affect the incident response team's ability to effectively detect and respond to security incidents.

- **Third-party dependencies** - Incident response teams may rely on third-party service providers, such as cloud providers or managed security service providers, to detect and respond to security incidents. Any disruption in these third-party services can impact the incident response team's ability to effectively detect and respond to security incidents.

Information Technology Infrastructure Library (ITIL)?

The Information Technology Infrastructure Library (ITIL) is a set of detailed practices for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of the business. ITIL describes processes, procedures, tasks, and checklists which are neither organization-specific nor technology-specific but can be applied by an organization toward strategy, delivering value, and maintaining a minimum level of competency. It allows organizations to establish a baseline from which it can plan, implement, and measure. IBM defines ITIL as a library of best practices for managing IT services and improving IT support and service levels. One of the main goals of ITIL is to ensure that IT services align with business objectives, even as business objectives change

Top 10 questions on incident management

1. What is incident management?
2. What are some examples of commonly occurring IT incidents?
3. Can you list some incident management best practices?
4. How would you manage recurrent incidents?
5. What steps can you take to prevent incidents from happening?
6. When would you implement an incident management system?
7. What is the Information Technology Infrastructure Library (ITIL)?
8. Which document do you need to restore a failed IT system?
9. What are the roles of an incident manager?
10. Why are you interested in this role?