

Introduction to Information Security

Prof. Dilip H. Ayyar

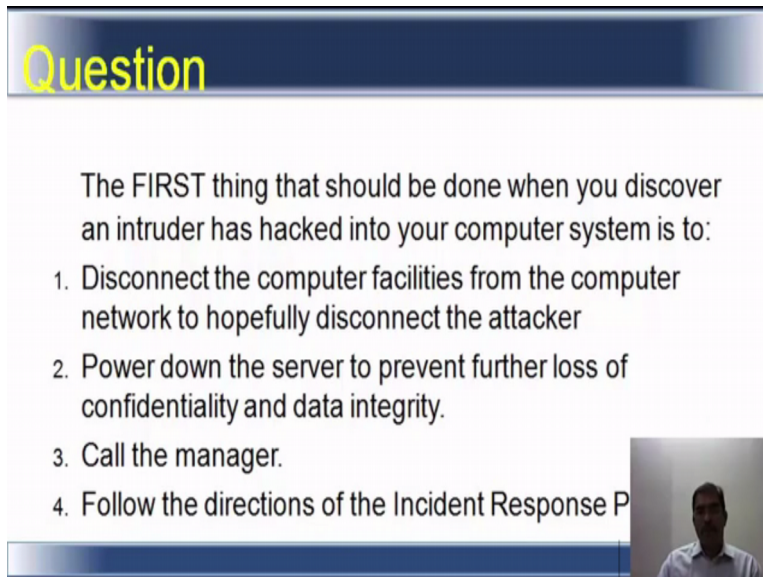
Department of Computer Science and Engineering

Indian Institute of Technology, Madras

Lecture – 40

Incident Management

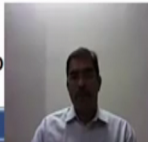
(Refer Slide Time: 00:11)



Question

The FIRST thing that should be done when you discover an intruder has hacked into your computer system is to:

1. Disconnect the computer facilities from the computer network to hopefully disconnect the attacker
2. Power down the server to prevent further loss of confidentiality and data integrity.
3. Call the manager.
4. Follow the directions of the Incident Response P




Let us see some question on what we have done. The first question is, the first thing that should be done when you discover that an intruder has hacked into your system is, number one disconnect the computer facilities from the computer network to hopefully disconnect the attacker. Two power down the server to prevent further loss of confidentiality and data integrity. Three call the manager and four follow the directions of the incident response plan. The correct answer here is 4.

(Refer Slide Time: 00:48)

Question

During an audit of the business continuity plan, the finding of MOST concern is:

1. The phone tree has not been double-checked in 6 months
2. The Business Impact Analysis has not been updated this year
3. A test of the backup-recovery system is not performed regularly
4. The backup library site lacks a UPS




During the audit of business continuity plan, the finding of most concern is, the phone tree or the phone book which has not been double checked in 6 months. The business impact analysis has not been updated this year. Test of backup recovery is not performed regularly, but the backup library site lacks an UPS. Now, what could be the possible answers here? It is three that is the most critical asset for the company is its data. The backup and restoration must be tested to ensure that this critical data is always available.

(Refer Slide Time: 01:33)

Question

The first and most important BCP test is the:

1. Fully operational test
2. Preparedness test
3. Security test
4. Desk-based paper test




The next question, the first and the most important B C P test is, the fully operational test preparedness test, security test or desk based paper test. Fourth one is the correct answer here. Desk based paper test is the first of the three test and is considered to be the most critical to perform.

(Refer Slide Time: 01:57)

Question

When a disaster occurs, the highest priority is:

1. Ensuring everyone is safe
2. Minimizing data loss by saving important data
3. Recovery of backup tapes
4. Calling a manager




When a disaster occurs, the highest priority is, number one ensuring everyone is safe. Two minimizing data loss by saving important data. Three recovery of backup tapes and four calling a manager. So, when we talk about people, process, technology, we put people first. So, even here when the disaster occurs the highest priority is one, ensuring everyone is safe that is the correct answer.

(Refer Slide Time: 02:26)

Question

A documented process where one determines the most crucial IT operations from the business perspective

1. Business Continuity Plan
2. Disaster Recovery Plan
3. Restoration Plan
4. Business Impact Analysis




A documented process where one determines the most crucial IT operations from the business perspective is the business continuity plan, the disaster recovery plan, the restoration plan or the business impact analysis. The answer here is business impact analysis.

(Refer Slide Time: 02:49)

Question

The PRIMARY goal of the Post-Test is:

1. Write a report for audit purposes
2. Return to normal processing
3. Evaluate test effectiveness and update the response plan
4. Report on test to management




The primary goal of a post is, is one write a report for audit purposes, return to normal processing, evaluate the effectiveness of the test and update the response plan, report the test on management. The correct answer here is three, evaluate test effectiveness and update the response plan.

(Refer Slide Time: 03:11)

Question

A test that verifies that the alternate site successfully can process transactions is known as:

1. Structured walkthrough
2. Parallel test
3. Simulation test
4. Preparedness test



A test that verifies that the alternate site successfully can process transaction is known as, a, structural walkthrough, parallel test, simulation test or preparedness test. The correct answer is the parallel test. Now, the reason why we are giving you so much questions here is, for you to get an understanding of what exactly it is. And if you have registered for taking the exam it will help you a long way.

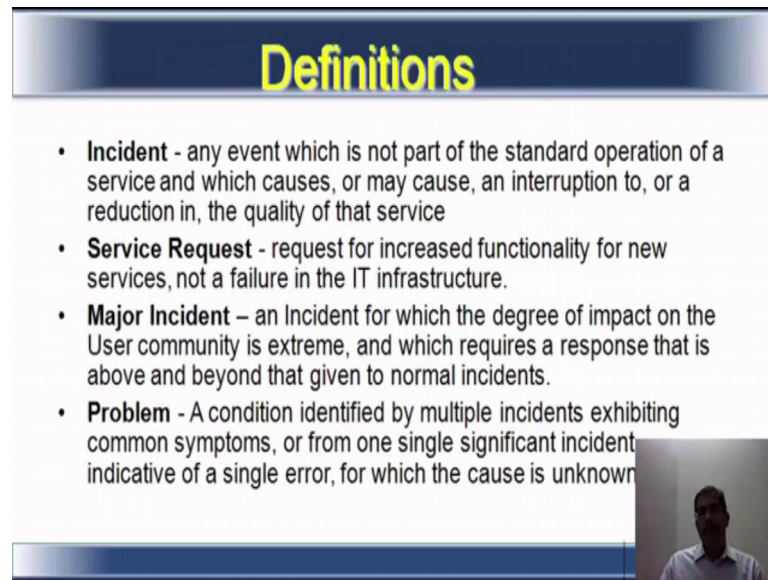
(Refer Slide Time: 03:44)

Incident Management



Let us talk about incident management. Now, we have already discussed what are incident is. An incident is an event which has an undesirable effect on the business process or the business itself, in simple terms that is incident. So, how you will manage this incident.

(Refer Slide Time: 04:04)



Definitions

- **Incident** - any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service
- **Service Request** - request for increased functionality for new services, not a failure in the IT infrastructure.
- **Major Incident** – an Incident for which the degree of impact on the User community is extreme, and which requires a response that is above and beyond that given to normal incidents.
- **Problem** - A condition identified by multiple incidents exhibiting common symptoms, or from one single significant incident indicative of a single error, for which the cause is unknown

Video inset showing a person speaking.

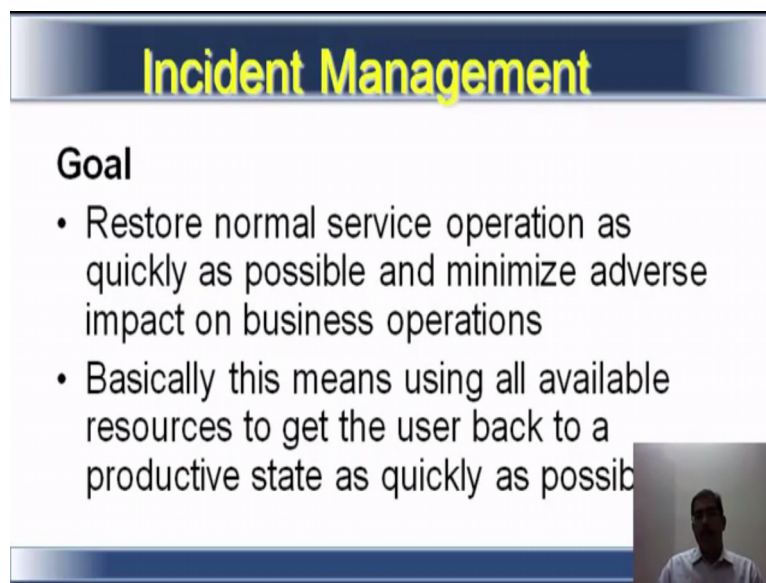
Now, you will see look at the definition of incident of various terminologies. Incident is any event which is not a part of the standard operation of a service and which causes or may cause an interruption to or the reduction in the quality of that service. So, it is basically a undesirable event, which is not a part of your standard operation. That means which is something that you do not do in your day to day operation of a service. And which can cause an interruption or reduction in quality of the service that we have asked for can be classified it as an incident.

What is service request? Request for increased functionality for new services, not a failure in the IT infrastructure. So, it is a service request. We give a service request and say that we need more functionality in this application or we need more processing power in this particular server. So, that is a service request, then major incident is an incident for which the degree of impact on the user community is extreme. And which requires the response that is above and beyond that given to the normal circumstances. So, we have seen that major incident what has to be done and all that. So, major incident is an incident for which the impact is very high. And it requires a response also that is equally fast and different and

effective, when compared to the normal incidents. A problem is a condition identified by multiple incidents exhibiting normal symptoms or from one single significant incident.

It could be a hack, it could be a failure of a hard disk, it could be the crash of the network anything. Indicative of a single error for which the cause is unknown. So, something happens in the organization where the cause is unknown, but it has caused a significant problem.

(Refer Slide Time: 06:05)



Incident Management

Goal

- Restore normal service operation as quickly as possible and minimize adverse impact on business operations
- Basically this means using all available resources to get the user back to a productive state as quickly as possible

The slide features a blue gradient header with the title 'Incident Management' in yellow. Below the header, the word 'Goal' is written in bold black text. Two bullet points follow, describing the objective of incident management. A small inset video of a man is visible in the bottom right corner of the slide.

What is the goal of incident management? It is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations. Basically this means using all available resources to get the user back to productive state as quickly as possible. Now, productive state as quickly as possible means receive normal operations as quickly as possible.

(Refer Slide Time: 06:32)

Incident Management

Benefits

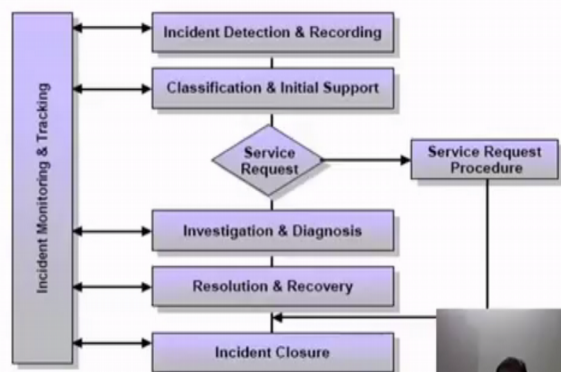
- Minimize the disruption and downtime for our users
- Maintain a record during the entire Incident life-cycle.
(This allows any member of the service team to obtain or provide an up-to-date progress report)
- Building knowledgebase of known issues to allow quicker resolution of frequent Incidents



What are the benefits of having a good incident management? It minimizes the disruption and downtime for our users that is the organizations users. It maintains the record during the entire incident lifecycle. So, it helps you to maintain a record during the entire incident lifecycle, receive, manage it properly the documentation should be good. This allows any member of the service team to obtain or provide an up to date progress report. Then you also build a knowledge base of known issues to allow quicker resolution of frequent incidents. These are the benefits of having good incident management processes.

(Refer Slide Time: 07:11)

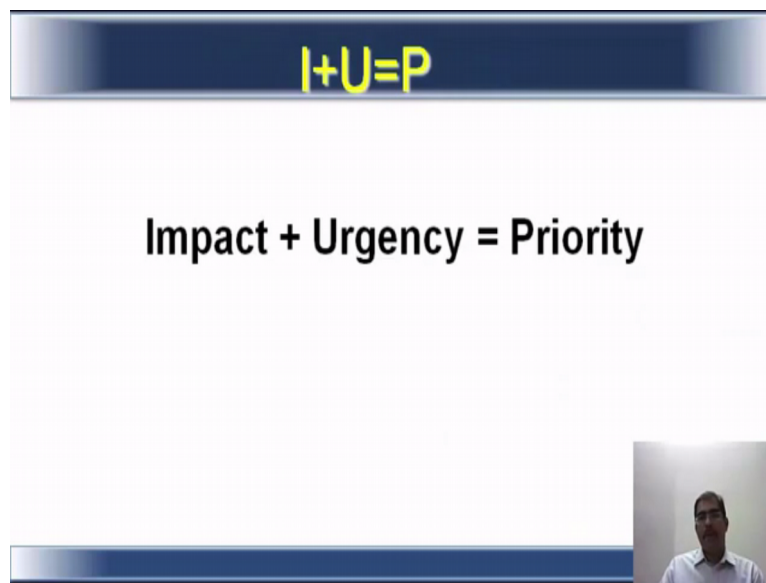
Incident Lifecycle



Now, what is an incident life cycle. There is incident detection and recording. So, first of all an incident occurs and you detect it, you record it, then you classify and see initial support.

So, it leads to a service request from the service request there is a service request procedure, from there it goes to the resolution and recovery, investigation and diagnosis. And then the incident closure, but during a life cycle of this incident there is also incident monitoring tracking at every stage of the incident life cycle.

(Refer Slide Time: 07:49)



I+U=P

Impact + Urgency = Priority

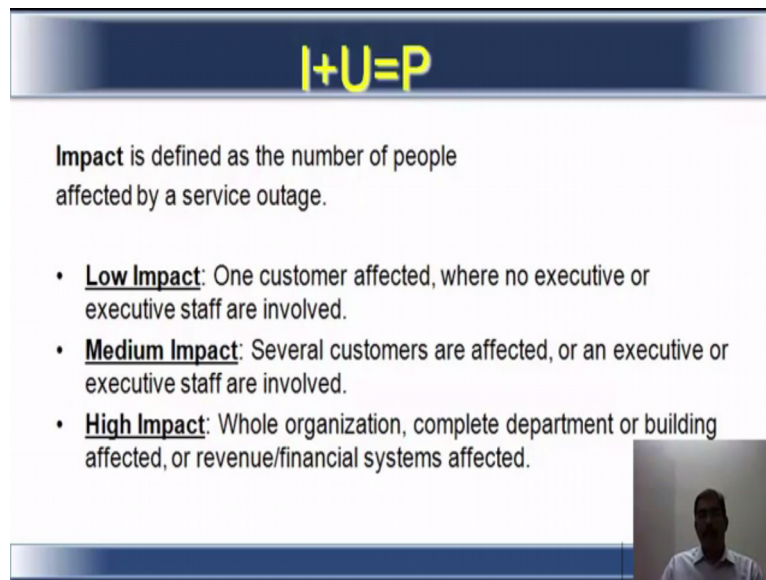
There is a formula here,

$$\text{Impact} + \text{Urgency} = \text{Priority} \quad (7:49)$$

in incident management. So,

$$I + U = P \quad (7:57)$$


(Refer Slide Time: 07:59)



I+U=P

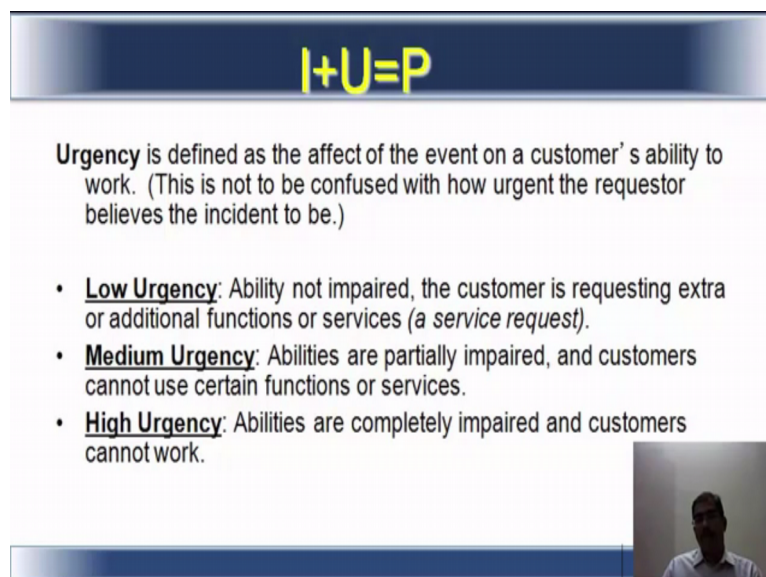
Impact is defined as the number of people affected by a service outage.

- **Low Impact:** One customer affected, where no executive or executive staff are involved.
- **Medium Impact:** Several customers are affected, or an executive or executive staff are involved.
- **High Impact:** Whole organization, complete department or building affected, or revenue/financial systems affected.



Here impact is defined as number of people affected by a service outage. There can be different levels of impact. It can be a low impact where only one customer is affected where no executive or executive staff are involved. Then it could be a medium impact where several customers are affected or an executive or executive staff are also involved in that. And then there is a high impact the whole organization is affected. Complete department or building is affected, revenue or financial system itself is affected. So, that is a high impact incident.


(Refer Slide Time: 08:34)



I+U=P

Urgency is defined as the affect of the event on a customer's ability to work. (This is not to be confused with how urgent the requestor believes the incident to be.)

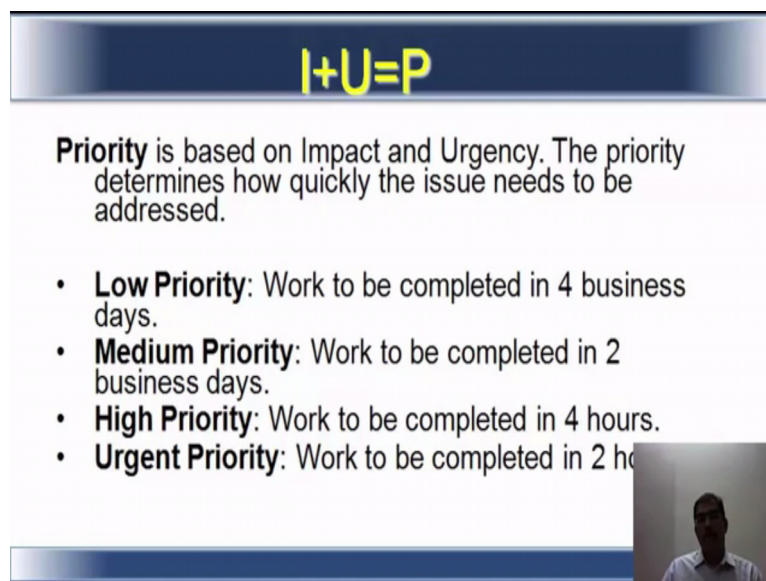
- **Low Urgency:** Ability not impaired, the customer is requesting extra or additional functions or services (*a service request*).
- **Medium Urgency:** Abilities are partially impaired, and customers cannot use certain functions or services.
- **High Urgency:** Abilities are completely impaired and customers cannot work.



Now, urgency is defined as, the effect of the event, urgency is defined as the effect of the event on a customer's ability to work. This is not to be confused with how the how urgent the requester believes the incident to be. So, it is basically defined as the effect of the event on a customer's ability to work. There again there are three classifications here, low, medium and high.

Now, under low ability is not impaired. The customer is requesting extra or additional functions or services. It could be a service request medium urgency abilities are partially impaired and customers cannot use certain functions or services. Let us say an internet banking facility. Where certain activities are not available for a specific period of time. So, the customers raise a request. High urgency abilities are completely impaired and customers cannot work, there will be internet banking site itself goes wrong then it will go for high urgency classification.


(Refer Slide Time: 09:42)



I+U=P

Priority is based on Impact and Urgency. The priority determines how quickly the issue needs to be addressed.

- **Low Priority:** Work to be completed in 4 business days.
- **Medium Priority:** Work to be completed in 2 business days.
- **High Priority:** Work to be completed in 4 hours.
- **Urgent Priority:** Work to be completed in 2 hours.



The third is the priority. Priority is based on the impact and urgency. The priority determines how quickly the issue needs to be addressed. Again here there are low, medium high and urgent priority, four categories here. An example low priority work to be completed within four business days, under medium priority work to be completed in two business days. High within four hours and urgent within two hours. So, this is how the impact urgency and priority is determined.

We come to end of module three, BCP DRP in itself is a very vast subject. We have just introduced you to the concepts of BCP/ DRP. Now, as we go on we propose to teach you in depth BCP and DRP. And about your RAID, about your network redundancies, cloud you have already seen in module 2. So, we will actually go into these subjects deeper and deeper as we progress, you are in different post level. Now, we go to CUM in module four, which is basically the network security.

Thank you all for seeing this session.